Landtag von Sachsen-Anhalt

Drucksache 7/3858
21.01.2019

Gesetzentwurf

Landesregierung

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung der Datenschutzvorschriften im Bereich des Justizvollzuges von Sachsen-Anhalt (Justizvollzugsdatenschutzumsetzungsgesetz Sachsen-Anhalt - JVollzDSUG LSA)

Sehr verehrte Frau Landtagspräsidentin,

als Anlage übersende ich gemäß Artikel 77 Abs. 2 der Verfassung des Landes Sachsen-Anhalt den von der Landesregierung am 15. Januar 2019 beschlossenen

> Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung der Datenschutzvorschriften im Bereich des Justizvollzuges von Sachsen-Anhalt (Justizvollzugsdatenschutzumsetzungsgesetz Sachsen-Anhalt - JVollzDSUG LSA)

nebst Begründung mit der Bitte, die Beschlussfassung des Landtages von Sachsen-Anhalt herbeizuführen.

Federführend ist das Ministerium für Justiz und Gleichstellung des Landes Sachsen-Anhalt.

Mit freundlichen Grüßen

Dr. Reiner Haseloff
Ministerpräsident

(Ausgegeben am 23.01.2019)

Vorblatt

A. Problem

Das Europäische Parlament und der Rat der Europäischen Union haben am 27. April 2016 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 4.5.2016, S. 89, L127 vom 23.5.2018, S. 9), im Folgenden: „Richtlinie (EU) 2016/680“, erlassen. Die Richtlinie (EU) 2016/680 ist zwingend in nationales Recht umzusetzen. Das betrifft auch den Bereich des Justizvollzuges in Sachsen-Anhalt.

Der Justizvollzug, einschließlich des Vollzuges der Sicherungsverwahrung, des Jugendarrestes, der Untersuchungshaft und der ihnen gleichgestellten Freiheitsentziehungen, fällt unter den Begriff der Strafvollstreckung und unter den Schutz vor und dem Abwehren von Gefahren für die öffentliche Sicherheit gemäß Artikel 1 der Richtlinie (EU) 2016/680. Das Einordnen des Justizvollzuges unter den Begriff der Strafvollstreckung ist dem deutschen Rechtssystem immanent. So wird zwischen der Strafvollstreckung im Weiteren und der Strafvollstreckung im engeren Sinne unterschieden. 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 Justizvollzug.

Das europarechtliche Betrachten führt ebenso zum Einordnen des Justizvollzuges unter den Begriff der Strafvollstreckung im Sinne der Richtlinie (EU) 2016/680. In zahlreichen europäischen Ländern werden begriffliche Unterscheidungen nicht vorgenommen, sondern beide Rechtsmaterien in einheitlichen Gesetzen geregelt. Auch das an dem Sinn und Zweck der Richtlinie (EU) 2016/680 orientierte Betrachten führt zu diesem Ergebnis. Der sensible Bereich der Strafrechtspflege soll gerade der Richtlinie (EU) 2016/680 und nicht der am 25. Mai 2016 in Kraft getretenen 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) - im Folgenden „Verordnung (EU) 2016/679“ - unterfallen.

Dies soll den Mitgliedstaaten der europäischen Union beim Umsetzen der Richtlinie (EU) 2016/680 größere Handlungs- und Gestaltungsspielräume eröffnen und gilt auch für den Justizvollzug, der, als zeitlich letzter Abschnitt eines Strafverfahrens und als Dienstleister des Gewährleistens des sicheren Durchführens eines Strafverfahrens, ein wesentlicher Teil der Strafrechtspflege ist. Davon werden auch Sanktionen wie die Sicherungsverwahrung und der Jugendarrest erfasst, die zwar keine Strafen im eigentlichen Sinne darstellen, aber Maßnahmen sind, die als staatliche Reaktion auf Verstöße gegen strafrechtliche Bestimmungen erfolgen. Der Vollzug der Untersuchungshaft und ihr gleichgestellten Haftarten knüpfen an den dringenden Verdacht eines Verstoßes gegen strafrechtliche Bestimmungen an und dienen dem

geordneten Durchführen eines Strafverfahrens oder dem Abwehren von Gefahren für die öffentliche Sicherheit und Ordnung.

Der Anwendungsbereich der Richtlinie (EU) 2016/680 ist damit für den Justizvollzug des Landes eröffnet und verdrängt den Anwendungsbereich der Verordnung (EU) 2016/679.

Das vollständige Umsetzen der Richtlinie (EU) 2016/680 im Bereich des Justizvollzuges des Landes macht das umfassende Überarbeiten des bereichsspezifischen Datenschutzes und das Anpassen aller Justizvollzugsgesetze des Landes notwendig.

Der Schutz personenbezogener Daten betroffener Personen im Justizvollzug ist gegenwärtig bereichsspezifisch in Abschnitt 23 des Justizvollzugsgesetzbuches Sachsen-Anhalt (JVollzGB LSA) geregelt. Das Sicherungsverwahrungsvollzugsgesetz von Sachsen-Anhalt (SVVollzG LSA) verweist bisher auf das JVollzGB LSA (vgl. § 72 SVVollzG LSA). Dieser Verweis muss zwingend aufgehoben werden, weil, unabhängig von der Richtlinie (EU) 2016/680, aufgrund der Verordnung (EU) 2016/679 ein vollständiges Neufassen des allgemeinen Datenschutzrechtes in Sachsen-Anhalt erfolgen wird, das auch im Anwendungsbereich der Richtlinie (EU) 2016/680 weiterhin keine eigenen Regelungen für den Justizvollzug des Landes enthalten wird.

Soweit im Justizvollzug hingegen anderweitige Rechtsmaterie zu vollziehen ist, paradigmatisch wäre insofern das beamtenrechtliche Dienstrecht, einschließlich des Personalaktenrechtes, zu nennen, vollzieht sich diese Rechtsanwendung außerhalb des sachlichen Anwendungsbereiches gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680. Das hat aus unionsrechtlicher Sicht die Folge, dass bei Vorliegen der weiteren Voraussetzungen der sachliche Anwendungsbereich der Verordnung (EU) 2016/679 eröffnet ist (vgl. Artikel 9 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 für das Weiterverarbeiten von im sachlichen Anwendungsbereich der Richtlinie (EU) 2016/680 erhobenen personenbezogenen Daten). Das Landesrecht setzt dies dahingehend um, dass sich der allgemeine datenschutzrechtliche Rahmen aus den Bestimmungen der Verordnung (EU) 2016/679, einschließlich der hierzu erlassenen landesrechtlichen Regelungen, ergibt.

B. Lösung

Es wird der Entwurf eines Gesetzes zum vollständigen Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen des bereichsspezifischen Datenschutzes im Justizvollzug und der Justizvollzugsgesetze des Landes vorgelegt (Gesetzentwurf).

Der Gesetzentwurf enthält in Artikel 1 - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (JVollzGB IV LSA) - eine Vollregelung des für den gesamten Justizvollzug (Strafvollzug, Jugendstrafvollzug, Untersuchungshaftvollzug, Jugendarrestvollzug und Vollzug der Sicherungsverwahrung) des Landes geltenden Datenschutzrechtes, die weit überwiegend ohne externe Verweisungen auskommt, unter dem Ausschöpfen der bestehenden Regelungsspielräume bewährte Strukturen erhält, die Pflichten der Verantwortlichen konkretisiert, die bisherigen datenschutzrechtlichen Standards in ein neues eigenständiges Gesetz zum Datenschutz im Justizvollzug des Landes überführt und zugleich die Vorgaben der Richtlinie (EU) 2016/680 vollständig in bereichsspezifisches Landesrecht umsetzt. Dies soll dem hohen Stellenwert des Datenschutzes im Justizvollzug und den Be-

sonderheiten des Justizvollzuges im erforderlichen Umfang Rechnung tragen, die sehr komplexe Materie „Datenschutz“ anwendungsfreundlicher gestalten und so die Rechtssicherheit beim Anwender deutlich erhöhen.

Diese Verfahrensweise entspricht auch dem beabsichtigten Vorgehen des überwiegenden Teils der Länder, die auf der Grundlage des Musterentwurfes für ein Justizvollzugsdatenschutzgesetz, ebenfalls das Einführen eigenständiger Gesetze für den Datenschutz im Justizvollzug planen.

Der Gesetzentwurf berücksichtigt die wesentlichen Inhalte des Musterentwurfes zum Umsetzen der Richtlinie (EU) 2016/680 und Entwürfe anderer Länder zum bereichsspezifischen Datenschutz im Justizvollzug. Er orientiert sich zudem an den Novellierungen des Datenschutzrechtes außerhalb des Justizvollzuges des Landes [vgl. Entwurf des Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (Drs. 7/3207)].

Artikel 1 des Gesetzentwurfes - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (JVollzGB IV LSA) - enthält u. a. Vorschriften über die allgemeinen Grundsätze des Verarbeitens personenbezogener Daten, die Rechtsgrundlagen einzelner Formen des Verarbeitens personenbezogener Daten, die Rechte betroffener Personen, die Pflichten der Justizvollzugsbehörden und etwaiger Auftragsverarbeiter, das Bestellen behördlicher Datenschutzbeauftragter bei den Justizvollzugsbehörden und Regelungen über Schadensersatz und Sanktionen beim rechtswidrigen Verarbeiten personenbezogener Daten.

Neu aufgenommen wurden einige für die Vollzugspraxis erforderliche Regelungen, unter anderem Vorschriften zum Durchführen einer Sicherheitsanfrage über Gefangene und anstaltsfremde Personen, deren Ziel es ist, extremistische Einstellungen der betroffenen Personen zu erkennen, die zunächst nicht erkennbar sind. Eine Sicherheitsanfrage kann dabei durch eine auch technikgestützte Anfrage der Justizvollzugsbehörden beispielsweise beim Landeskriminalamt und dem Verfassungsschutz des Landes erfolgen. Die bislang in den einzelnen Justizvollzugsgesetzen des Landes Sachsen-Anhalt enthaltenen Abschnitte mit Vorschriften zum Datenschutz werden aufgehoben.

Artikel 2 und 3 des Gesetzentwurfes nehmen hierzu die erforderlichen Änderungen und korrespondierenden Anpassungen in den Justizvollzugsgesetzen vor. Damit werden alle von der Richtlinie (EU) 2016/680 geforderten Regelungen entsprechend deren inhaltlicher Vorgaben erlassen. Weil ein vollständiges bereichsspezifisches Umsetzen der Richtlinie (EU) 2016/680 im Justizvollzug erfolgt, sind Verweisungen in allgemeines Datenschutzrecht des Landes nicht erforderlich.

Artikel 4 des Gesetzentwurfes sieht das Inkrafttreten des Gesetzes vor. Mit Blick auf das erforderliche umfassende Umstellen und Anpassen der im Justizvollzug bereits verwendeten automatisierten Verarbeitungssysteme wurde von der in Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 zu den Protokollierungspflichten eröffneten Option Gebrauch gemacht. Das in § 16 des Gesetzentwurfes enthaltene verpflichtende Protokollieren einzelner Vorgänge des Verarbeitens personenbezogener Daten gilt

erst frühestens ab dem 6. Mai 2023 und tritt demzufolge auch erst zu diesem Zeitpunkt in Kraft.

Der Gesetzentwurf stellt zugleich einen weiteren Schritt dar, um alle Justizvollzugsgesetze des Landes Sachsen-Anhalt zu ordnen und formell in die neue Gesamtsystematik von insgesamt vier Büchern des Justizvollzugsgesetzbuches Sachsen-Anhalt zu überführen: Erstes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Vollzug der Freiheitsstrafe, der Jugendstrafe, der Untersuchungshaft und des Strafarrestes - (JVollzGB I LSA), Zweites Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Vollzug der Sicherungsverwahrung - (JVollzGB II LSA), Drittes Buch Justizvollzugsgesetzbuch Sachsen - Anhalt - Vollzug des Jugendarrestes - (JVollzGB III LSA) und Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (JVollzGB IV LSA). Alle vier Bücher stellen materiell-rechtlich (weiterhin) eigenständige Regelungswerke dar, wodurch alle rechtlich erforderlichen Abgrenzungen und Spezifika, die im Vollzug der unterschiedlichen Freiheitsentziehungen zu beachten und umzusetzen sind, uneingeschränkt erhalten bleiben.

C. Alternativen

Das Umsetzen der Richtlinie (EU) 2016/680 im Justizvollzug des Landes ist zwingend. Vor diesem Hintergrund bestehen hierzu keine Alternativen.

D. Kosten

Das Umsetzen der EU-Bestimmungen führt aber, insbesondere hinsichtlich der vom EU-Gesetzgeber vorgegebenen erweiterten Dokumentations-, Mitteilungs- und Auskunftspflichten der Justizvollzugsbehörden, zu erhöhten Anforderungen. Gleiches gilt für das Beantworten von Sicherheitsanfragen bei Behörden mit Sicherheitsaufgaben, insbesondere den Polizeibehörden des Bundes und der Länder sowie dem Verfassungsschutz des Bundes und der Länder.

Zudem stellt der EU-Gesetzgeber höhere Anforderungen an das Protokollieren automatisierter Vorgänge des Verarbeitens personenbezogener Daten. Für das Anpassen des im Justizvollzug dafür bisher verwendeten Fachverfahrens BASIS-WEB sieht der Gesetzentwurf eine Übergangsfrist bis 6. Mai 2023 vor. Ergänzend werden für das Anpassen des Fachverfahrens BASIS-WEB voraussichtlich im Haushaltsjahr 2024 Kosten in Höhe von 10.000 Euro anfallen.

E. Anhörung

Der Präsident des Oberlandesgerichtes, der Generalstaatsanwalt, der Deutsche Beamtenbund und Tarifunion Sachsen-Anhalt, der Deutsche Gewerkschaftsbund Bezirk Niedersachsen-Bremen-Sachsen-Anhalt (DGB), der Landesverband des Bundes der Strafvollzugsbediensteten und der Landesbeauftragte für den Datenschutz (LfD) hatten Gelegenheit, zu dem Gesetzentwurf Stellung zu nehmen. Der DGB und der LfD haben inhaltlich Stellung genommen.

Grundsätzliche Bedenken wurden gegen den Gesetzentwurf nicht erhoben. Anregungen zu Einzelfragen des Gesetzentwurfes wurden sorgfältig geprüft und dieser, soweit erforderlich, überarbeitet. Darüber hinaus wurden vereinzelt weitere redaktio-

nelle Änderungen vorgenommen. Das wichtigste Vorbringen und dessen Bewerten werden im Folgenden dargestellt.

Allgemein

Der LfD merkt Bedenken hinsichtlich der neuen Systematik von vier Büchern des Justizvollzugsgesetzbuches Sachsen-Anhalt (JVollzGB I bis IV LSA) dahingehend an, dass der Gesetzentwurf mit dem Ersten Buch beginnen und mit dem Vierten Buch enden müsse. Zudem gehe der Gesetzentwurf über ein einfaches Umsetzen der Richtlinie (EU) 2016/680 hinaus. Die Bedenken des LfD sind unbegründet. Der Gesetzentwurf wurde rechtsförmlich geprüft und entspricht den Grundsätzen der Rechtsförmlichkeit (vgl. Anlage zur GGO.LSA II). Das Umsetzen der Richtlinie (EU) 2016/680 im Justizvollzug des Landes erfordert das umfassende Überarbeiten des bereichsspezifischen Datenschutzes und das Anpassen der Justizvollzugsgesetze des Landes. In diesem Kontext wurden auch notwendige Änderungen, die sich aus Rechtsprechung und Praxis ergeben haben, aufgenommen. Dazu gehören die Entscheidungen des Bundesverfassungsgerichtes (BVerfG) zur Antiterrordatei und zum Bundeskriminalamtgesetz ebenso wie das Verbessern des Austausches personenbezogener Daten zwischen den Justizvollzugsbehörden und den Behörden mit Sicherheitsaufgaben.

Der LfD regt an, in der Begründung klarzustellen, um welche vier Bücher es sich nach dem Ordnen und Überführen der Justizvollzugsgesetze des Landes in die neue Systematik konkret handele und ob das Vierte Buch für die vorhergehenden drei Bücher gelten solle. Die Anregung des LfD wurde aufgegriffen und der Gesetzentwurf in der Begründung überarbeitet.

Der LfD ist der Ansicht, dass der Vollzug der Sicherungsverwahrung kein Strafvollzug sei. Der Gesetzentwurf regele aber auch den Datenschutz im Vollzug der Sicherungsverwahrung. Er gebe so den Unterschied zwischen Strafvollzug und dem Vollzug der Sicherungsverwahrung auf. Untergebrachte würden ein Sonderopfer erbringen, das es rechtfertige, sie auch datenschutz-rechtlich besser zu stellen als Strafgefangene. Es sei unklar, ob im Vollzug der Sicherungsverwahrung die Richtlinie (EU) 2016/680 oder die Verordnung (EU) 2016/679 gelte und ob der Gesetzentwurf nur Gefangene oder auch Untergebrachte erfasse. Der Justizvollzug, einschließlich des Vollzuges der Sicherungsverwahrung, des Jugendarrestes, der Untersuchungshaft und der ihnen gleichgestellten Freiheitsentziehungen, fällt unter den Begriff der Strafvollstreckung und unter den Schutz vor und dem Abwehren von Gefahren für die öffentliche Sicherheit gemäß Art. 1 der Richtlinie (EU) 2016/680. Das Einordnen des Justizvollzuges unter den Begriff der Strafvollstreckung ist dem deutschen Rechtssystem immanent. So wird zwischen der Strafvollstreckung im Weiteren und der Strafvollstreckung im engeren Sinne unterschieden 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 Justizvollzug. Das europarechtliche Betrachten führt ebenso zum Einordnen des Justizvollzuges unter den Begriff der Strafvollstreckung im Sinne der Richtlinie (EU) 2016/680. In vielen europäischen Ländern wird begrifflich nicht unterschieden, sondern beide Rechtsmaterien in einheitlichen Gesetzen geregelt. Auch das an dem Sinn und Zweck der Richtlinie (EU) 2016/680 orientierte Betrachten führt zu diesem Ergebnis. Der sensible Bereich der Strafrechtspflege soll gerade der Richtlinie (EU) 2016/680 und nicht der Verordnung (EU) 2016/679 unterfallen. Dies gilt auch für den

Justizvollzug, der als Dienstleister des Gewährleistens des sicheren Durchführens eines Strafverfahrens, ein wesentlicher Teil der Strafrechtspflege ist. Die strafrichterlichen Sanktionen Sicherungsverwahrung und Jugendarrest werden hiervon erfasst. Sie stellen zwar keine Strafen im eigentlichen Sinne darstellen, sind aber Maßnahmen, 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 dem geordneten Durchführen eines Strafverfahrens oder dem Abwehren von Gefahren für die öffentliche Sicherheit und Ordnung. Im Justizvollzug des Landes, einschließlich des Vollzuges der Sicherungsverwahrung und des Jugendarrestes ist damit der Anwendungsbereich der Richtlinie (EU) 2016/680 eröffnet und verdrängt die Verordnung (EU) 2016/679. Insofern der LfD Bezug auf das Abstandsgebot nimmt, steht dies dem Gesetzentwurf nicht entgegen. Nach dem vom BVerfG entwickelten Abstandsgebot muss der Vollzug der Sicherungsverwahrung in deutlichem Abstand zum Strafvollzug so ausgestaltet werden, dass, entsprechend dem Resozialisierungsgebot, die Perspektive des Wiedererlangens der Freiheit sichtbar die Praxis des Unterbringens bestimmt und erhebliche therapeutische Anstrengungen zum Mindern der Gefährlichkeit des Untergebrachten unternommen werden. Das BVerfG hat das Abstandsgebot und die freiheitsorientierten und Therapie gerichteten Gesamtkonzepte durch sieben Gebote bzw. Prinzipien konkretisiert: Ultima-ratio-Prinzip: Sicherungsverwahrung darf nur als letztes Mittel angeordnet werden. Alle Möglichkeiten zum Reduzieren der Gefährlichkeit des Täters müssen bereits während des Strafvollzuges ausgeschöpft werden; Individualisierungs- und Intensivierungsgebot: Spätestens zu Beginn des Vollzuges der Sicherungsverwahrung muss eine umfassende und den wissenschaftlichen Anforderungen genügende Behandlungsuntersuchung stattfinden und in einen Vollzugsplan münden. Insbesondere im therapeutischen Bereich müssen alle Möglichkeiten ggf. durch individuell zugeschnittene Therapieangebote, ausgeschöpft werden; Motivierungsgebot: Drohenden psychischen Auswirkungen, die mit unbestimmter Dauer der Sicherungsverwahrung verbunden sind, ist, auch mit individuellen Behandlungs- und Betreuungsangeboten wirksam zu begegnen; Trennungsgebot: Der äußerer Vollzugsrahmen muss einen deutlichen Abstand zum regulären Strafvollzug erkennen lassen, wobei ein vollständiges räumliches Ablösen vom Strafvollzug nicht erforderlich ist; Minimierungsgebot: Konzeptionen müssen Vollzugslockerungen vorsehen, Vorgaben zum Vorbereiten des Entlassens enthalten und sind mit planmäßigen Hilfen für die Phase nach dem Entlassen zu verzahnen; Rechtsschutz- und Unterstützungsgebot: Untergebrachten ist ein Rechtsanspruch zum Durchführen der zum Reduzieren ihrer Gefährlichkeit gebotenen Maßnahmen einzuräumen und sie sind bei der Wahrnehmung ihrer Interessen zu unterstützen; Kontrollgebot: Die Fortdauer des Vollzuges der Sicherungsverwahrung ist mindestens jährlich gerichtlich zu überprüfen. Anhaltspunkte für Aussetzungsreife gebieten ein unverzügliches gesondertes Überprüfen.

Das Abstandsgebot beruht auf den kategorial unterschiedlichen Legitimationsgrundlagen und Zwecksetzungen des Vollzuges der Freiheitsstrafe und des Vollzuges der Sicherungsverwahrung. Während repressiver Strafvollzug eine Reaktion auf das vorwerfbare Begehen einer Straftat darstellt, beruht das präventive Instrument der Sicherungsverwahrung allein auf dem Prinzip des überwiegenden Interesses. Wird ein als hochgefährlich eingeschätzter Verurteilter nach dem Verbüßen seiner Strafe allein aufgrund eines überwiegenden Sicherheitsinteresses der Allgemeinheit in seinen Freiheitsinteressen beschränkt, verlangt der Staat von dieser Person ein "Sonderopfer" ab. Diesem ist mit einem privilegierten Vollzug Rechnung zu tragen. Der

Vollzug der Sicherungsverwahrung bleibt verfassungskonform, wenn die Beeinträchtigungen Untergebrachter zumindest in qualitativer Hinsicht so gering, d.h. so erträglich, wie irgend möglich, gestaltet sind. Im Ergebnis kommt es nicht auf einen unter allen Umständen einzuhaltenden Abstand zwischen den Vollzugsformen an, sondern um das Gewährleisten eines unterschiedlichen Mindestniveaus an Lebensqualität und Resozialisierungsbemühungen. Das Abstandsgebot stellt insoweit eine Art Mindestfürsorgegebot dar, umfasst aber nicht den Bereich des vollzugsspezifischen Daten-schutzes. Für das Umsetzen des Abstandsgebotes mussten Bundes- und Landesgesetzgeber die wesentlichen Leitlinien bzw. die entsprechenden Vollzugsregelungen schaffen. Beide Gesetzgeber haben die Vorgaben des BVerfG umgesetzt und insofern, insbesondere mit Blick auf das Abstandsgebot, keine unterschiedlichen Datenschutzbestimmungen für den Strafvollzug und den Vollzug der Sicherungsverwahrung geschaffen. Vor diesem Hintergrund bestehen keine konventionsrechtlichen Bedenken. Der Europäische Gerichtshof für Menschenrechte sieht daher den Vollzug der Sicherungsverwahrung in Deutschland mittlerweile nicht mehr als Strafe im Sinne von Art. 7 der Europäischen Menschenrechtskonvention an, so dass alle Länder, wie es auch in Art. 1, § 1 des Gesetzentwurfes für Sachsen-Anhalt vorgesehen ist, weiterhin ihre Datenschutz-bestimmungen im Justizvollzug überwiegend einheitlich regeln werden.

Zu Artikel 1

Der LfD regt an, die in § 2 genannten, konkreten vollzuglichen Zwecke zu beschränken, da die Regelung nicht abschließend sei. Der Anregung des LfD wird nicht gefolgt. Die konkreten vollzuglichen Zwecke sind unbedingt erforderlich. Nach Art. 4 Abs. 1 Buchst. b der Richtlinie (EU) 2016/680 dürfen personenbezogene Daten der betroffenen Person nur für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden (Grundsatz der Zweckbindung). Dies dient nicht nur dem Schutz personenbezogener Daten, sondern insbesondere auch dem Abgrenzen zum Anwendungsbereich der Verordnung (EU) 2016/679. Die Regelung ist der zentrale Bestandteil des Gesetzentwurfes. Zu unbestimmte Zwecksetzungen würden beim Anwender zu erheblichen Abgrenzungs- und Auslegungsschwierigkeiten führen, die wiederum deutlich zu Lasten der Rechtssicherheit gingen. Maßnahmen des Justizvollzuges sind nur bis zu einem bestimmten Punkt statisch und von Routinen geprägt. In vielen Bereichen des Justizvollzuges, insbesondere beim Behandeln und Betreuen der Gefangenen, der Sicherheit und Ordnung der Anstalten und dem Schutz der Allgemeinheit bedarf es eines kontinuierlichen Überprüfens und Anpassens an sich stetig ändernde Bedingungen im Vollzug selbst und im Lebens außerhalb des Vollzuges. Deshalb enthält die Regelung am Ende bewusst eine Öffnungsklausel, die sicherstellt, dass auch neue Maßnahmen, die aufgrund steten Wandels zukünftig Einzug in den Justizvollzug halten könnten, erfasst werden.

Nach Ansicht des LfD sei der Begriff „Weiterverarbeiten“ nicht erforderlich. Die Ansicht des LfD wird nicht geteilt. Die Gesetzessprache ist Teil der juristischen Fachsprache. Wird sie von Nichtfachleuten wahrgenommen, so verliert Vorschriftensprache ihre unmittelbare Bindung an das fachliche juristische Denken und ihre Beziehung zur fachlichen Systematik. Begriffe und Aussagen erschließen sich dem Laien nicht ohne Weiteres. Damit kein missverständlicher oder unverständlicher Vorschriftentext entsteht, müssen Begriffsbestimmungen vorgesehen werden, damit das jeweilige Wort bereits aus sich heraus leicht verständlich ist und so eine rechtssichere Anwendung ermöglicht wird. So liegt es bei den zusätzlich zu den Begriffen der

Richtlinie (EU) 2016/680 aufgenommenen Begriffsbestimmungen. Diese sind für das Verständnis des Gesetzentwurfes essentiell und können nicht ohne weiteres hinweg gedacht werden, ohne dass der Erfolg in seiner konkreten Gestalt - umfassendes und rechtsichere Anwenden - entfiele. Der Gesetzentwurf behält das bewährte Trennen der wesentlichen Einzelvorgänge des Verarbeitens personenbezogener Daten, wie es in Abschnitt 23 des JVollzGB LSA enthalten ist, durchgehend bei. Diese Verfahrensweise war bisher, insbesondere vor dem Hintergrund des bis Mai 2018 in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verwendeten einheitlichen Verarbeitungsbegriffes, europarechtskonform. Daran hat sich nach Inkrafttreten der Richtlinie (EU) 2016/680 nichts geändert.

Es bleibt europarechtlich zulässig, dass Gesetzgeber den Begriff „Verarbeiten“, insbesondere zum besseren Verständnis von Fachgesetzen, teilen können, solange kein inhaltlich anderer Regelungsgehalt geschaffen wird. Der im Gesetzentwurf verwendete Begriff „Weiterverarbeiten“ erfüllt diese Anforderungen. Er fasst trennscharf die unter ihn fallenden, einzelnen benannten Teilvorgänge des Verarbeitens personenbezogener Daten zusammen und trennt sie so von den übrigen Teilvorgängen des Verarbeitens personenbezogener Daten (z. B. vom Erheben, Offenlegen, Löschen, Einschränken oder Berichtigen) ab. Er schafft so die erforderliche Rechtssicherheit, beugt gesetzlichen Unschärfen und hierzu korrespondierenden erheblichen Abgrenzungs- und Auslegungsschwierigkeiten wirksam vor. Er gilt für Zwecke, zu denen personenbezogene Daten erhoben wurden als auch für Zwecke, zu denen sie ursprünglich nicht erhoben wurden. An dieser Stelle den umfassenden Begriff „Verarbeiten“ zu verwenden, würde hier den Anwender nicht nur verunsichern, sondern auch zu falschen Schlüssen und Wertungen führen. Da im Verhältnis zu Richtlinie (EU) 2016/680 inhaltlich kein neuer Begriff geschaffen wird, steht der Begriff „Weiterverarbeiten“ in der im Gesetzentwurf gewählten Form in Einklang mit europäischem Recht. Andere, bereits konsolidierte Fachgesetze wie bspw. das Bundeskriminalamtgesetz und die Bayerischen Vollzugsgesetze verwenden diesen Begriff ebenso wie die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (vgl. 95. Konferenz am 25. und 26. April 2018 in Düsseldorf zum Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (V.1.1-Erprobungsfassung) unter Nr. 5.3: „…, die Erhebung personenbezogener Daten und ihre Weiterverarbeitung…“

Der LfD ist der Ansicht, dass „Verarbeiten“, „Pseudonymisieren“ oder „Einwilligen“ als eigene Begriffe verwendet würden, während die Richtlinie (EU) 2016/680 nur vom „Verarbeiten“ oder „Einwilligen“ spreche und der Gesetzentwurf anzupassen sei. Die Ansicht des LfD wird nicht geteilt. § 3 Nr. 5 enthält den Begriff „Verarbeiten“. Die Formulierung entspricht Art. 3 Nr. 2 der Richtlinie (EU) 2016/680. Der Begriff „Pseudonymisieren“ wird nicht in § 3 Nr. 5 geregelt, sondern in § 3 Nr. 10 und entspricht Art. 3 Nr. 5 der Richtlinie (EU) 2016/680. Soweit der LfD auf den Begriff „Einwilligen“ rekurriert, entspricht dieser der Regelung in Art. 1, § 2 Nr. 22 des Entwurfes eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Drs. 7/3207).

Nach Ansicht des LfD sei der Begriff „anstaltsfremde Person“ entbehrlich. Die Ansicht des LfD wird nicht geteilt. Der Begriff „anstaltsfremde Person“ ist unbedingt erforderlich. Er ist nicht neu, sondern wurde bisher unterschiedlich, auch unter Einbeziehen des Besuchers definiert. Mehrere Länder verwenden ihn schon identisch in ihren Vollzugsgesetzen. Andere Länder, so auch Sachsen-Anhalt, haben bisher die Formulierung „vollzugsfremde Person“ (vgl. §§ 35, 147 JVollzGB LSA) gewählt. Zukünftig soll im Justizvollzug der Länder einheitlich der Begriff „anstaltsfremde Person“ verwandt werden.

Nach Ansicht des LfD setze § 5 den Art. 9 der Richtlinie (EU) 2016/680 nicht um, wonach für das Verarbeiten personenbezogener Daten zu anderen als den in Art. 1 der Richtlinie (EU) 2016/680 genannten Zwecken die Verordnung (EU) 2016/679 gelte, es sei denn, das Verarbeiten personenbezogener Daten erfolge im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts falle. Die Ansicht des LfD wird nicht geteilt. Die Regelung setzt nicht Art. 9 der Richtlinie (EU) 2016/680 um. Mit Satz 1 wird Art. 4 Abs. 2 der Richtlinie (EU) 2016/680 umgesetzt und klargestellt, dass Justizvollzugsbehörden als Behörden mit Gesamtaufgaben personenbezogene Daten zu anderen Zwecken weiterverarbeiten dürfen, insofern es sich bei diesen anderen Zwecken auch um vollzugliche Zwecke handelt und das Weiterverarbeiten dieser Daten dazu erforderlich und verhältnismäßig ist. Hier wurde von der in Art. 4 Abs. 2 der Richtlinie (EU) 2016/680 eröffneten Möglichkeit Gebrauch gemacht, personenbezogene Daten auch für andere vollzugliche Zwecke zu verarbeiten, wobei das Verarbeiten personenbezogener Daten innerhalb der Bandbreite aller zur Verfügung stehenden vollzuglichen Zwecke gerade keine Zweckänderung ist. Satz 2 betrifft das Weiterverarbeiten personenbezogener Daten zu anderen in § 1 genannten und nach diesem Gesetzentwurf anerkannten Zwecken. Dies ist insbesondere zulässig, wenn es in einer Regelung dieses Gesetzentwurfes oder einer anderen Rechtsvorschrift vorgesehen ist. Dem Anliegen des LfD tragen die §§ 1 und 83 Rechnung.

Nach Ansicht des LfD fehle in § 6 der von Art. 9 der Richtlinie (EU) 2016/680 verlangte Hinweis an Empfänger personenbezogener Daten, dass Bedingungen für das besondere Verarbeiten gelten würden. Die Ansicht des LfD wird nicht geteilt. Insofern dieser auf Art. 9 Abs. 3 der Richtlinie (EU) 2016/680 rekurriert, trägt bereits der speziellere § 44 Abs. 3 dem Anliegen Rechnung.

Die Regelung entspricht Art. 1, § 6 des Entwurfes eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Drs. 7/3207).

Der DGB weist mit Blick auf § 11 Abs. 4 auf eine ggf. erschwerte Nachweisführung des freien Entscheidens zum Einwilligen der betroffenen Person hin. Eine Vielzahl der Gefangenen sei der deutschen Sprache nicht oder nur eingeschränkt mächtig. Zudem könne bei einer nicht unerheblichen Zahl Gefangener nicht ausgeschlossen werden, dass deren Einsichtsfähigkeit eingeschränkt ist. Hier bedürfe es Vorgaben, wie in solchen Fällen vorzugehen sei. Der Hinweis des DGB ist grds. nachzuvollziehen und wird begrüßt. Eine gesetzliche Regelung ist aber, insbesondere mit Blick auf die Vielzahl von Möglichkeiten des Nachweisführens, an dieser Stelle erforderlich. Vielmehr soll es dem individuellen Umsetzen der rechtlichen Vorgaben in der Praxis bspw. durch umfassendes und lückenloses Dokumentieren, aber auch der Recht-

sprechung überlassen werden, ob und inwieweit Nachweise im Einzelfall ausreichen. Verständigungsschwierigkeiten ist mit Sprachmittlern und Dolmetschern zu begegnen.

Nach Ansicht des LfD stelle die Formulierung in § 13 Abs. 3 S. 2 "… sollen dazu führen, ... " nur eine Erklärung, aber keine Verpflichtung dar, weshalb die Regelung „„...müssen umgesetzt werden, …“ lauten sollte. Zudem sollte Absatz 3 um das Gewährleistungsziel des "Datenminimierens" ergänzt werden, da er mit Bezug auf das Standard-Datenschutzmodell (SDM) nur die Gewährleistungsziele, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettunq, Transparenz und Intervenierbarkeit übernehme, aber das in Art. 20 der Richtlinie (EU) 2016/680 als Grundsatz genannte Gewährleistungsziel des "Datenminimierens" nicht berücksichtigt werde. Die Bedenken des LfD sind unbegründet. § 13 Abs. 3 S. 2 ist als Sollvorschrift ausgestaltet und verpflichtet die Justizvollzugsbehörden grds. zum Umsetzen von Schutzmaßnahmen. Davon dürfen sie nur in begründeten Einzelfällen abweichen. Die Norm entspricht Art. 1, § 20 Abs. 2 S. 2 des Entwurfes eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Drs. 7/3207). Der Grundsatz des Datenminimierens ist zudem bereits in § 4 Abs. 2 Nr. 3 enthalten, der Art. 4 Abs. 1 Buchst. c) der Richtlinie (EU) 2016/680 umsetzt. Auf Anregung des LfD wurde in der Begründung zu Abs. 3 der Begriff „Datensparsamkeit“ durch den Begriff „Datenminimieren“ ersetzt.

Der LfD regt an, in den Überschriften der §§ 18 bis 21 vom „Erheben personenbezogener Daten“ zu sprechen. Die Anregung des LfD wurde aufgegriffen und der Gesetzentwurf angepasst.

Nach Ansicht des LfD bestehe für § 23 kein Regelungsbedürfnis. Die Eingriffsbefugnisse seien erst in den §§ 24 und 25 enthalten. Die Ansicht des LfD wird nicht geteilt. Die Norm enthält den gesetzlichen Auftrag, Gefangene und andere anstaltsfremde Personen sicherheitsbezogen zu überprüfen. Die nachfolgenden Bestimmungen eröffnen den Justizvollzugsbehörden gerade das Ermessen, im Einzelfall von einem sicherheitsbezogenen Überprüfen absehen zu können (vgl. Gesetzentwurfsbegründung zu § 23).

Nach Ansicht des LfD sei der Begriff „drohende Gefahr“ in § 24 im Zusammenhang mit der vorbeugenden Bekämpfung terroristischer Gefahrenlagen im Strafvollzug nicht erforderlich. Die Ansicht des LfD wird nicht geteilt. Das vorbeugende Bekämpfen terroristischer Gefahrenlagen endet nicht mit Antritt einer richterlich angeordneten Freiheitsentziehung und beginnt auch nicht erst an deren Ende. Sie wirkt vielmehr während des Vollzuges fort. Auch in dieser Zeit muss entsprechenden Gefahren und Radikalisierungstendenzen anderer Gefangener und weiterer betroffener Personen wirksam begegnen werden können. Hierfür sind u. a. auch umfassende Erkenntnisse und personenbezogen Daten über die betroffene Person erforderlich. Nur so kann die Wahrscheinlichkeit, konkrete Gefahren auch rechtssicher erkennen und diese rechtzeitig verhindern zu können, wirksam erhöht werden. Ohne diese Schwelle des Erhebens personenbezogener Daten würden bei und zwischen den Justizvollzugsbehörden, den Justizbehörden und den Behörden mit Sicherheitsaufgaben erhebliche Informations- und Erkenntnisverluste bzgl. etwaiger Gefährder drohen. Vergegenwärtigt man sich, dass bspw. der Attentäter des Berliner Breit-

scheidplatzes, der in Italien etwa vier Jahre in einem Gefängnis untergebracht gewesen, sich dort radikalisiert haben und unter nicht weniger als 14 Identitäten bekannt gewesen sein soll, wird klar, dass Identitätsverwechselungen zum Schutz der Allgemeinheit und der Sicherheit der Anstalten jederzeit kategorisch und wirksam ausgeschlossen werden müssen. Aber auch Selbsttötungen Gefangener, wie bspw. am 12.10.2016 in Sachsen, zeigen ein erforderliches Informationsbedürfnis auf, dem nur durch gesetzliche Regelungen in Form ausdrücklicher Ermächtigungsgrundlagen im erforderlichen Umfang Rechnung zu tragen ist.

Die Regelung enthält aus diesem Grund die Befugnis, sich mit einer Sicherheitsanfrage - nur um diese geht es hier - an die dort genannten Behörden wenden zu dürfen, wenn tatsächliche Anhaltspunkte für eine drohende Gefahr für die Sicherheit der Anstalten vorliegt. Die „drohende Gefahr“ begründet hier nur die Schwelle für den mit einer Sicherheitsanfrage verbundenen Eingriff in das Recht auf informationelle Selbstbestimmung. Die Gefahrenprognose muss aber tatsachengestützt sein und darf sich nicht auf Vermutungen und allgemeine Erfahrungssätze stützen. Sie ist insoweit der konkreten Gefahr im polizeirechtlichen Sinne vorgelagert. Nicht das Verletzen des Schutzgutes „Sicherheit der Anstalten“ muss drohen, sondern eine Gefahr für diese (sog. „Gefahr der Gefahr“). Es müssen tatsächliche Anhaltspunkte für das Entstehen einer konkreten Gefahr für die Sicherheit der Anstalten bestehen. Der zum Schaden führende Kausalverlauf muss aber noch nicht mit hinreichender Wahrscheinlichkeit vorhersehbar sein, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für die Sicherheit der Anstalten hindeuten. Ausreichend ist, dass ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, aus dem heraus das Verletzen der Sicherheit der Anstalten resultieren könnte. Nicht ausreichend ist etwa allein die Erkenntnis, dass Gefangene sich zu einem bestimmten fundamentalistischen Religionsverständnis hingezogen fühlen. Deshalb ist ein Offenlegen personenbezogener Daten, nur um herauszufinden, ob eine Gefahr droht, nach dieser Regelung ausgeschlossen. Die Sicherheitsanfrage erfolgt mit Blick darauf, dass Gefangene nicht freiwillig im Justizvollzug sind, auch nicht verdachtsunabhängig. Die drohende Gefahr muss dem Gefangenen in dem Sinne zurechenbar sein, dass er in die Gefahrenlage als mutmaßlicher Störer „verstrickt ist“. Der Gesetzentwurf folgt hier konsequent der Rechtsprechung des BVerfG zum Begriff „drohende Gefahr“ (Urt. v. 20. April 2016 – 1 BvR 966/09 -, juris, Rn 109ff, 162 ff.). Mit der Antwort auf die Sicherheitsanfrage ist sogleich der zweite Schritt für das Überprüfen des Gefangenen eröffnet. Ergibt sich aus der Antwort der angefragten Behörde nun eine konkrete Gefahr für die Sicherheit der Anstalt, dürfen die Justizvollzugsbehörden weitere Auskünfte oder Unterlagen einholen. Der Gesetzentwurf findet so einen angemessenen Ausgleich zwischen den Persönlichkeitsrechten der Gefangenen und der durchgehend zu gewährleistenden Anstaltssicherheit.

Nach Ansicht des LfD seien in § 25 der Begriff „anstaltsfremde Person“ und das regelmäßige sicherheitsbezogene Überprüfen dieses Personenkreises nicht nötig. Die Ansicht des LfD wird nicht geteilt. Zum Begriff „anstaltsfremde Person“ wird auf die obigen Ausführungen verwiesen. Infolge des Grundsatzes, dass anstaltsfremde Personen nur dann in Anstalten tätig werden oder diese besuchen dürfen, wenn keine Sicherheitsbedenken bestehen, ermöglicht Absatz 1 das Überprüfen ihrer Zuverlässigkeit und ermächtigt zu einer Sicherheitsanfrage bei den Polizei- und Verfassungsschutzbehörden, wenn nicht eine Gefährdung der Anstaltssicherheit fernliegend erscheint. Ist dies der Fall, sollen die Anstalten gerade von einer Sicherheitsanfrage absehen. Absatz 3 dreht das Regel-Ausnahme-Verhältnis der Absätze 1 und 2 für

Besucher insoweit um, als eine drohende Gefahr für die Anstaltssicherheit positiv festgestellt werden muss, bevor die Zuverlässigkeit einer Person tatsächlich überprüft werden kann. Eingriffe in Rechte der betroffenen Personen unterbleiben damit nicht erst, wenn eine Gefahr für die Sicherheit der Anstalt als fernliegend ausgeschlossen werden kann. Die Systematik der Regelungen begründet sich darin, dass der Zugang anstaltsfremder Personen zu einer Anstalt, um dort beruflich tätig zu werden, regelmäßig freiwillig erfolgt und die Möglichkeit gibt, auch weitere Einblicke in (Sicherheits-)Abläufe der Anstalten zu erhalten. Das ist in erhöhtem Maße gefahrgeneigt. Bei Besuchern von Gefangenen stehen hingegen auch Grundrechtspositionen von Gefangenen und Besuchern im Raum, die über das Recht auf informationelle Selbstbestimmung hinausweisen und daher im Sinne einer doppelten Verhältnismäßigkeitsprüfung zu beachten sind. Da Besuche regelmäßig auf bestimmte Räumlichkeiten beschränkt sind, grds. gut überwacht werden können und so die Sicherheit der Anstalt vergleichsweise weniger gefährdet sein kann, ist dies in die Verhältnismäßigkeitsprüfung mit einzubeziehen. Absatz 4 konkretisiert den Verhältnismäßigkeits-grundsatz dahingehend weiter, dass der Schriftwechsel mit den dort genannten Personen und Stellen von einem Überprüfen ihrer Zuverlässigkeit ausgenommen ist (vgl. auch Gesetzentwurfs-begründung zu § 25).

Nach Ansicht des LfD werde in Unterabschnitt 3 das Offenlegen personenbezogener Daten durch ihr Übermitteln oder eine andere Art des Bereitstellens geregelt. Der Begriff „Bereitstellen“ sei als Form des Offenlegens, um auch das Bereitstellen personenbezogener Daten zum Einsehen von elektronischen Akten oder Dateisystemen zu ermöglichen, nicht erforderlich, da es nach bisherigem Landesrecht im Begriff „Übermitteln“ enthalten sei. Der Begriff „Offenlegen“ würde im Sprachgebrauch mit Preisgeben, Aufdecken bzw. Enthüllen gleichgesetzt und suggeriere ein Veröffentlichen von personenbezogenen Daten im Strafvollzug, was missverstanden werden könnte. Die Bedenken des LfD sind unbegründet.

Nach der Richtlinie (EU) 2016/680 stellt „Offenlegen“ den Oberbegriff und „Übermitteln“, „Verbreiten“ oder die „andere Art des Bereitstellens“ nur eine Form des Offenlegens dar. Art. 3 Nr. 2 der Richtlinie (EU) 2016/680 spricht hier im Wortlaut von „Offenlegen durch Übermitteln, Verbreiten oder eine andere Art des Bereitstellens“. „Übermitteln“ ist so immer auch „Offenlegen“, während „Offenlegen“ nicht auch das „Übermitteln“ umfassen muss. Der EU-Gesetzgeber hat dies bspw. in Art. 25 Abs. 1 der Richtlinie (EU) 2016/680 deutlich gemacht. Dort wird ausdrücklich von „Offenlegen einschließlich des Übermittelns“ gesprochen und klargestellt, dass an dieser Stelle „Übermitteln“ umfasst wird. Der Gesetzentwurf übernimmt hier nur den von der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 vorgegebenen Oberbegriff „Offenlegen“, wodurch bisheriges Landesrecht modifiziert wird. Um Missverständnissen beim Auslegen der Normen wirksam vorzubeugen und zum besseren Verständnis für Leser und Anwender, enthalten die Überschriften der Unterabschnitte 3 und 4 sowie die Begründung einheitlich und richtlinienkonform den Begriff „Offenlegen“. Dadurch wird klargestellt, welche einzelnen Teilvorgänge des Offenlegens erfasst und welche bewusst ausgeschlossen werden sollen. In Unterabschnitt 3 geht es nur um das Offenlegen durch Übermitteln oder eine andere Art des Bereitstellens und das Abfragen, während Unterabschnitt 4 richtlinienkonform auf das Übermitteln beschränkt ist. Beiden Unterabschnitten gemein ist, dass das Verbreiten, also das an die Öffentlichkeit dringen, in Umlauf kommen und vielen bekannt werden, in einen weiteren Umkreis gelangen oder sich dort ausbreiten (lassen), durch die gewählte Formulierung ausdrücklich ausgeschlossen ist.

Nach Ansicht des LfD sei der Begriff „drohende Gefahr“ in § 36 im Zusammenhang mit der vorbeugenden Bekämpfung terroristischer Gefahrenlagen, im Strafvollzug nicht erforderlich. Die Ansicht des LfD wird nicht geteilt. Zur Begründung wird auf die Ausführungen zu § 24 und die Gesetzentwurfsbegründung zu § 36 verwiesen.

Der LfD regt an, in Unterabschnitt 4 nicht den Begriff „Offenlegen“, sondern den Begriff „Übermitteln“ zu verwenden. Die Ansicht des LfD wird nicht geteilt. Zur Begründung wird auf die obigen Ausführungen verwiesen.

Nach Ansicht des LfD seien § 47 Absatz 1 Nr. 4 und Nr. 5 zu streichen. Die Schutzgüter würden im Vergleich zu den hochrangigen Schutzgütern in den Nrn. 1 bis 3 nicht ausreichen, um ein Übermitteln personenbezogener Daten zu rechtfertigen. Die Bedenken des LfD sind unbegründet. Der Katalog der Schutzgüter wird durch Art. 38 Abs. 1 Nrn. 1 bis 5 der Richtlinie (EU) 2016/680 vorgegeben und wurde für das bereichsspezifische Umsetzen in Landesrecht entsprechend der Richtlinie (EU) 2016/680 konkretisiert.

Nach Ansicht des LfD werde mit § 48 der Art. 39 der Richtlinie (EU) 2016/680 umgesetzt, der das Übermitteln personenbezogener Daten an in Drittländer niedergelassene Empfänger regele. Dies sollte auch in der Überschrift zum Ausdruck kommen. Die Ansicht des LfD wird nicht geteilt. Durch die Überschrift des Unterabschnittes 4 „Offenlegen durch Übermitteln an Drittstaaten und an internationale Organisationen“ wird klargestellt, dass es in diesem Unterabschnitt nur um den Einzelvorgang „Übermitteln“ geht. Das Erweitern der einzelnen Paragraphenüberschriften ist nicht erforderlich. Die Gesetzentwurfsbegründung verhält sich hierzu ebenso wie die oben zu Unterabschnitt 3 dargelegten Ausführungen zum Oberbegriff „Offenlegen“.

Nach Ansicht des LfD erwecke § 48 Absatz 4 den Eindruck, dass personenbezogene Daten mit dem Zustimmen der übermittelnden Behörde auch zu anderen Zwecken verarbeitet werden dürften. Diese widerspreche Art. 39 Abs. 1 Nr. e der Richtlinie (EU) 2016/680. Die Bedenken des LfD sind unbegründet. Die Vorschrift dient dem Umsetzen von Artikel 39 der Richtlinie (EU) 2016/680. Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Justizvollzug tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Umfasst werden etwa das Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die zwingend mit dem Offenlegen personenbezogener Daten verbunden sind. Für dieses Offenlegen „im besonderen Einzelfall“ gelten die in § 48 Abs. 1 genannten strengen Voraussetzungen. Absatz 4 sieht genau aus diesem Grund eine verstärkte Zweckbindung der nach § 38 offengelegten personenbezogenen Daten vor. Das schließt zweckänderndes Weiterverarbeiten durch die Empfänger aus. Die Regelung entspricht Art. 1, § 37 Abs. 4 des Entwurfes eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Drs. 7/3207).

Nach Ansicht des LfD lasse § 49 Abs. 3 das Auftragsverarbeiten generell auf der Grundlage eines anderen Rechtsinstrumentes, also auch von Rechtsinstrumenten von Nicht-EU- Staaten, zu. Dies stehe nicht in Einklang mit Art. 22 Abs. 3 der Richtlinie (EU) 2016/680.

Die Bedenken des LfD sind unbegründet. § 49 Abs. 3 normiert die Voraussetzungen für das Eingehen von Unterauftragsverarbeitungsverhältnissen, wodurch Art. 22 Abs. 2 der Richtlinie (EU) 2016/680 umgesetzt wird. Durch die Unterrichtungspflicht in Satz 2 wird Verantwortlichen die Möglichkeit eingeräumt, gegen Änderungen in Bezug auf das Hinzuziehen oder das Ersetzen anderer Auftragsverarbeiter Einspruch zu erheben. Das Umsetzen von Art. 22 Abs. 3 der Richtlinie (EU) 2016/680 erfolgt in § 49 Abs. 5. Durch den Verweis auf Art. 22 Abs. 3 der Richtlinie (EU) 2016/680 wird klar, dass Rechtsinstrumente von Nicht-EU-Staaten nicht erfasst werden. Die Regelung entspricht Art. 1, § 18 Abs. 5 des Entwurfes eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Drs. 7/3207).

Nach Ansicht des LfD bestehe für § 50 kein Regelungsbedürfnis. Die Ansicht des LfD wird nicht geteilt. Beauftragen Verantwortliche Andere, weisungsabhängig und im Auftrag, personenbezogene Daten zu verarbeiten, liegt Auftragsverarbeiten vor. Das erfordert, dass Auftragnehmer (Dienstleister) beim Verarbeiten personenbezogener Daten unterstützend tätig werden, also nur Hilfsleistungen erbringen. Sie sind bildlich nur verlängerter Arm des Auftraggebers, also in den Befugnissen beim Verarbeiten überlassener personenbezogener Daten erheblich eingeschränkt. Die Auftragsnehmer haben beim Verarbeiten personenbezogener Daten keinen inhaltlichen Entscheidungsspielraum und sind abhängig von Weisungen und Vorgaben des Auftraggebers. Insoweit ist das Auftragsverarbeiten dem Auftraggeber zuzurechnen, der als Verantwortlicher auch für Verstöße des Auftragnehmers bzw. des Dienstleisters gegenüber den Betroffenen haftet. Der Auftraggeber muss rechtlich und faktisch in der Lage sein, dem Auftragnehmer jeden einzelnen Arbeitsschritt des Verarbeitens personenbezogener Daten vorzuschreiben und weiterhin die tatsächliche Verantwortung und Weisungshoheit für die personenbezogenen Daten haben, die durch einen Anderen verarbeitet werden. Klassische Tätigkeiten des Auftragsverarbeitens sind bspw. ausgelagerte Callcenter, Marketingaktionen durch externe Agenturen, Dienstleistungsverträge zur Datenträgerentsorgung, externe Lohn- bzw. Gehaltsabrechnung oder ausgelagerte Rechenzentren. Werden personenbezogene Daten nach diesen Grundsätzen verarbeitet, liegt ein gesetzliches Privileg vor, so dass bspw. das Weitergeben von personenbezogenen Daten nicht als Offenlegen durch Übermitteln, Verbreiten oder eine andere Form des Bereitstellens anzusehen ist. Da Auftragnehmer datenschutzrechtlich nur als verlängerter Arm des Auftraggebers gelten, ist hier ein besonderes Einwilligen der betroffenen Person oder eine gesonderte Rechtsgrundlage für das Weitergeben personenbezogenen Daten nicht erforderlich. Ohne eine solche Regelung ist der Auftraggeber aber nicht mehr Herr des Verfahrens „Verarbeiten personenbezogener Daten“ und es liegt eine „Funktionsübertragung“ vor. Bei dieser werden Andere, nicht wie beim Auftragsverarbeiten ausdrücklich mit dem Verarbeiten personenbezogener Daten beauftragt, sondern ein gesamter Aufgabenbereich zum Erledigen übertragen. Der Andere ist nun nicht mehr nur Auftragnehmer, sondern datenschutzrechtlich selbst „Verantwortlicher“, der in Bezug auf den Prozess des Verarbeitens personenbezogener Daten, der nur zum Erfüllen des übertragenen Aufgabenbereiches erforderlich ist, eigene Entscheidungs-befugnisse oder eigenes Ermessen hat oder im Rahmen des konkreten Verarbeitens personenbezogener Daten selbständig kommuniziert, einheitliche Stellenausschreibungen und Bewerbungsverfahren durchführt, Personalentscheidungen vornimmt sowie Benachrichtigungen und Auskünfte erteilt. Das ist bspw. der Fall, wenn, wie in einer Anstalt, Gefangene durch private Fachdienste (Psychiater, Psychotherapeuten, Psychologen,

Sozialarbeiter u. a.) behandelt und betreut werden. Diese nehmen insofern gerade keine hoheitlichen (Eingriffs-)Tätigkeiten bzw. nur Hilfs- oder Unterstützungsleistungen vor, sondern handeln, wie ihre Berufskollegen außerhalb des Justizvollzuges auch, nach den von ihnen erlernten fachlichen Grundsätzen, Kenntnissen und Standards. In diesen Fällen bedarf das Weitergeben personenbezogene Daten zum Erfüllen des übertragenen Aufgabenbereiches jedoch zwingend einer gesonderten Erlaubnis. § 50 schafft diese unbedingt erforderliche Rechtsgrundlage (vgl. auch § 54 JVollzGB I BW).

Nach Ansicht des LfD fehle in § 51 die Weisungsbefugnis des Verantwortlichen gegenüber dem Auftragsverarbeiter. Die Bedenken des LfD sind unbegründet. Nach dem Wortlaut der Norm hat jede Person, also auch der Auftragsverarbeiter, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung der Justizvollzugsbehörden zu verarbeiten, es sei denn, dass die Person aufgrund einer Rechtsvorschrift der Europäischen Union oder eines ihrer Mitgliedstaaten zum Verarbeiten personenbezogener Daten verpflichtet ist. Die Regelung entspricht Art. 1, § 8 des Entwurfes eines Gesetzes zur Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (vgl. Drs. 7/3207).

Der DGB regt mit Blick auf § 63 an, zu regeln, wie und in welchen Fällen im Justizvollzug bekannt gewordene Erkenntnisse zu Suizidversuchen von Gefangenen oder Gewaltakten gegen Bedienstete bei künftigen Gefängnisaufenthalten bekannt bleiben könnten. Dem Anliegen trägt der Gesetzentwurf bereits hinreichend Rechnung. Nach dem Grundsatz des Datenminimierens sind personenbezogene Daten durch Justizvollzugsbehörden unverzüglich zu löschen und zu vernichten, wenn deren Verarbeiten unzulässig oder zum Erfüllen ihrer Aufgaben nicht mehr erforderlich sind. § 63 enthält einen Katalog, der dies konkretisiert. So wird sichergestellt, dass bestimmte personenbezogener Daten, auch nach dem Entlassen eines Gefangenen, weiterhin verfügbar sind. Darüber hinaus enthalten die §§ 64 bis 66 weitere Befugnisse der Justizvollzugsbehörden, der Gefahr, bestimmter Informationen verlustig zu werden, wirksam begegnen zu können.

Nach Ansicht des LfD rechtfertigten die in § 69 Abs. 7 genannten Kriterien, insbesondere technisch-organisatorische Maßnahmen (Nr. 1) und Verschlüsseln (Nr. 2), nicht das Absehen vom Benachrichtigen der betroffenen Person. Die Bedenken des LfD sind unbegründet. Nach Art. 31 Abs. 3 der Richtlinie (EU) 2016/680 ist das Benachrichtigen der betroffenen Person nicht erforderlich, wenn Verantwortliche geeignete Vorkehrungen (technische und organisatorische) getroffen haben und diese Vorkehrungen auf die vom Verletzen betroffenen personenbezogenen Daten angewandt wurden. Dies gilt für Vorkehrungen, durch welche personenbezogenen Daten für Personen, die nicht zu deren Zugang befugt sind, unzugänglich gemacht werden (Verschlüsseln u.a.) oder Verantwortliche durch Folgemaßnahmen sichergestellt haben, dass hohe Risiken für die Rechte und Freiheiten betroffener Personen aller Wahrscheinlichkeit nach nicht mehr bestehen oder die mit unverhältnismäßigem Aufwand verbunden wäre. Die vermutete Gefahr, die ein Benachrichtigen bedingen würde, wird hier wirksam verhindert. Aufgrund der beseitigten Gefahr entsteht auf Seiten der betroffenen Person insoweit auch kein Rechtsschutzbedürfnis mehr.

Nach Ansicht des LfD setze § 70 Abs. 1 den Art. 14 der Richtlinie (EU) 2016/680 nicht vollständig um. Das Recht der betroffenen Person, vom Verantwortlichen eine Bestätigung darüber zu erhalten, dass sie betreffende personenbezogene Daten verarbeitet werden, werde nicht geregelt. Die Bedenken des LfD sind unbegründet. Nach dem Wortlaut von Abs. 1 S. 1 wird der betroffenen Person auf Antrag Auskunft darüber erteilt, ob sie betreffende personenbezogene Daten verarbeitet werden. Der Regelungsgehalt von Abs. 1 zielt gerade darauf ab, dass die betroffene Person auf ihren Antrag hin eine Bestätigung erhält, dass (also ob), ihre personenbezogenen Daten verarbeitet werden, während Abs. 1 S. 2 das „Wie“ des Verarbeitens ihrer personenbezogenen Daten regelt.

Nach Ansicht des LfD stelle § 70 Abs. 9, der § 159 Abs. 10 JVollzGB LSA entspreche, eine überflüssige, nicht mehr zeitgemäße Übersicherung dar. Die Bedenken des LfD sind unbegründet. Das Recht auf Informationsfreiheit nach Art. 5 Abs. 1 S. 1 GG gibt jedermann das Recht, sich ungehindert aus allgemein zugänglichen Quellen zu unterrichten. Durch das IZG LSA sind grundsätzlich alle amtlichen Informationen, die bei den Behörden, Gemeinden und anderen öffentlichen Stellen des Landes Sachsen-Anhalt vorhanden sind, zu allgemein zugänglichen Quellen geworden. Das IZG LSA setzt sich zum Ziel, die Anliegen der Menschen nach mehr Mitsprache beim Handeln der Verwaltung und nach mehr Transparenz sowie stärkerer bürgerschaftlicher Kontrolle der Verwaltung durch verbesserte Informationszugangsrechte zu stärken. Vor diesem Hintergrund gewährt das IZG LSA grds. jeder Person einen freien, an keine weiteren Voraussetzungen gebundenen Zugang zu allen amtlichen Informationen, die bei Behörden, Gemeinden und anderen öffentlichen Stellen des Landes vorhanden sind, wodurch der Grundsatz der Amtsverschwiegenheit durch das Prinzip der Aktenöffentlichkeit ersetzt wird. Das Recht auf Informationsfreiheit nach Art. 5 Abs. 1 S. 1 GG wird jedoch nicht schrankenlos gewährt. Deshalb regeln einige Informationszugangsgesetze (z. B. Bund, Bayern, Thüringen und Nordrhein-Westfalen), dass besondere Rechtsvorschriften über den Zugang zu amtlichen Informationen den allgemeinen Regelungen zum Informationszugang vorgehen (Grundsatz der Spezialität). Der Vorrang besteht dabei unabhängig davon, ob der Informationszugang enger oder weiter als im allgemeinen Informationszugangsgesetz geregelt ist. Auch der Gesetzgeber hat mit § 1 Abs. 3 IZG LSA eine solche Regelung geschaffen und damit deutlich zum Ausdruck gebracht, dass er spezialgesetzliche Sonderregelungen schaffen will oder geschaffen hat, die entweder den Anwendungsbereich des IZG LSA einschränken oder erst gar nicht eröffnen sollen. Die Nachrangigkeit des IZG LSA hängt somit vom Vorliegen einer spezialgesetzlichen Regelung in einem anderen Landesgesetz ab. Insofern dieses Gesetz nach dem Willen des Gesetzgebers abschließend ist, geht es als Lex specialis dem IZG LSA vor. Dabei sind die Grenzen des Spezialgesetzes bindend, da ein umfassender Informationsanspruch dem Schutzzweck des Spezialgesetzes gerade zuwiderlaufen würde.

Aus diesen Gründen hat sich der Gesetzgeber bewusst für die Spezialregelung des § 159 Abs. 10 JVollzGB LSA entschieden und so zum Ausdruck gebracht, dass der Sicherheit in den Justizvollzugsanstalten des Landes und dem Schutz der Allgemeinheit, insbesondere im Verhältnis zu allgemeinen Informationsinteressen des Einzelnen, der Vorrang gebührt. Er hat damit klargestellt, dass diesem besonderen Sicherungsbedürfnis nur mit einer gesetzlichen Sperrwirkung in vollem Umfang Rechnung getragen werden kann und der Anwendungsbereich des IZG LSA in diesem besonderen Fachrecht nicht eröffnet ist. Aufgrund der sich seit Dezember 2015 stetig verschärfenden Sicherheitslage in Deutschland, den anderen Mitgliedsstaaten

der EU und den Ländern außerhalb von Europa, wird, auch und gerade beim Umsetzen der Richtlinie, weiterhin an der Sperrwirkung dieser Regelung mit seiner sicherheitsorientierten Ausrichtung konsequent festgehalten und mit § 70 Abs. 9 bisher geltendes Landesrecht fortgeschrieben. Eine gleichlautende Regelung findet sich bspw. in § 49 Abs. 3 JVollzGB I BW (vgl. Drs. 7/1836, Drs. 7/3067 und 7/REV/22).

Nach Ansicht des LfD werde Art. 47 Abs. 2 der Richtlinie (EU) 2016/680 nicht umgesetzt. Die Bedenken des LfD sind unbegründet. Der Gesetzentwurf setzt die für den Justizvollzug des Landes maßgeblichen Bestimmungen der Richtlinie (EU) 2016/680 um. Die bereichsspezifischen Sonderregelungen gehen weiterhin den allgemeinen Datenschutzregeln des Landes vor. Dies gilt aber nur, soweit damit die Notwendigkeit gesonderter Regelungsbedürfnisse zum Ausdruck gebracht wird. Für allgemeine Befugnisse des LfD im Anwendungsbereich der Richtlinie (EU) 2016/680 besteht dieses Regelungsbedürfnis im bereichsspezifischen Datenschutz nicht. Mit dem Gesetz zur Organisationsfortentwicklung des LfD hat der Gesetzgeber die Richtlinie (EU) 2016/680 diesbzgl. bereits umgesetzt. Nach § 22 Abs. 1 DSG LSA erfüllt der LfD im Geltungsbereich der Richtlinie (EU) 2016/680 die Aufgaben aus deren Art. 46 und verfügt über die Befugnisse aus Art. 47. Weil sich der Gesetzentwurf zu diesem Regelungskontext bewusst nicht verhält, gilt § 22 Abs. 1 DSG LSA unmittelbar und es bedarf keines, auch nicht eines klarstellenden Verweises auf diese Norm. Dies gilt auch für § 23 Abs. 2 des Entwurfes eines Gesetzes zum Anpassen des Datenschutzrechtes in Sachsen-Anhalt an das Recht der Europäischen Union (DSAnpG EU LSA-E), der als Folgeregelung zu § 22 Abs. 1 DSG LSA geplant ist. Mit dieser Regelung soll sichergestellt werden, dass der LfD unabhängig davon, ob ein Verarbeiten personenbezogener Daten in den Anwendungsbereich der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 oder allein des nationalen Rechts fällt, als Aufsichtsbehörde die gleichen Pflichten und Befugnisse hat. Aus diesem Grund enthält auch der Entwurf eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes (Drs. 7/3207) keine Norm, die auf § 22 Abs. 1 DSG LSA oder die geplante Folgeregelung verweist.

Zu Artikel 2

Nach Ansicht des LfD werde der Unterschied zwischen Strafvollzug und dem Vollzug der Sicherungsverwahrung aufgegeben. Die Bedenken des LfD sind unbegründet. Nach dem formellen Ordnen und Überführen der Justizvollzugsgesetze des Landes in die neue Gesamtsystematik von vier Büchern des Justizvollzugsgesetzbuches Sachsen-Anhalt handelt es sich bei jedem der einzelnen Bücher (weiterhin) materiellrechtlich um eigene Gesetze. Alle rechtlich erforderlichen Abgrenzungen und Spezifika, die im Vollzug der unterschiedlichen Freiheitsentziehungen (bspw. im Vollzug der Sicherungsverwahrung oder des Jugendarrestes) zu beachten und umzusetzen sind, werden davon nicht berührt und bleiben uneingeschränkt erhalten.

F. Zuständigkeit

Zuständig ist das Ministerium für Justiz und Gleichstellung.

Entwurf

Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung der Datenschutzvorschriften im Bereich des Justizvollzuges von Sachsen-Anhalt (Justizvollzugsdatenschutzumsetzungsgesetz Sachsen-Anhalt - JVollzDSUG LSA).

Artikel 1
Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - JVollzGB IV LSA)

Inhaltsübersicht

Unterabschnitt 2
Weiterverarbeiten personenbezogener Daten

Unterabschnitt 3
Offenlegen personenbezogener Daten durch Übermitteln oder eine andere Art des Bereitstellens; Abfrage

Unterabschnitt 4
Offenlegen personenbezogener Daten durch Übermitteln an Drittstaaten und an internationale Organisationen

Unterabschnitt 5
Besondere Bedingungen

Unterabschnitt 6
Schutz von Geheimnisträgern

Unterabschnitt 7
Löschen und Vernichten, Einschränken des Verarbeitens, Berichtigen personenbezogener Daten

Abschnitt 5
Rechte der betroffenen Person

Abschnitt 6
Datenschutzbeauftragter

Abschnitt 7
Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz
und zwischen den Aufsichtsbehörden

Abschnitt 8
Rechtsbehelfe

Abschnitt 9
Haftung und Sanktionen

Abschnitt 10
Schlussvorschriften

Abschnitt 1
Allgemeine Bestimmungen

§ 1
Anwendungsbereich

Dieses Gesetz regelt das Verarbeiten personenbezogener Daten in Dateisystemen und Akten durch die Justizvollzugsbehörden im Vollzug

1. der Untersuchungshaft,

2. der Freiheitsstrafe,

3. der Jugendstrafe,

4. des Strafarrestes,

5. des Jugendarrestes,

6. der Unterbringung in der Sicherungsverwahrung,

7. der Haft nach § 127b Abs. 2, § 230 Abs. 2, § 236, § 329 Abs. 3, § 412 Satz 1 oder § 453c der Strafprozessordnung oder

8. der einstweiligen Unterbringung nach § 275a Abs. 6 der Strafprozessordnung,

soweit sie personenbezogene Daten von Gefangenen oder anderen betroffenen Personen zu vollzuglichen oder anderen nach diesem Gesetz anerkannten Zwecken verarbeiten.

§ 2
Vollzugliche Zwecke

Vollzugliche Zwecke sind insbesondere das Vorbereiten, das Prüfen, das Besprechen, das Festlegen, das Umsetzen, das Abgleichen, das Auswerten, das Ändern, das Fortschreiben und das Aufheben von Maßnahmen der Justizvollzugsbehörden im Zusammenhang mit:

1. dem Gestalten und Evaluieren des Vollzuges der jeweiligen Freiheitsentziehung,

2. dem Zu- und Abgang der Gefangenen,

3. dem Aufnahmeverfahren, dem Diagnoseverfahren und der Vollzugs- und Eingliederungsplanung der Gefangenen, auch unter dem Einsatz von Videotechnik,

4. dem Unterbringen, dem Überstellen, dem Verlegen, dem Ausführen, dem Vorführen, dem Transportieren und dem Ausantworten der Gefangenen, auch länderübergreifend,

5. dem Behandeln und Betreuen der Gefangenen beispielsweise

a) zum Fördern ihrer Mitwirkungsbereitschaft,
b) zu ihrer sozialtherapeutischen, psychotherapeutischen, psychologischen oder psychosozialen Behandlung und Betreuung,
c) zum Verbessern ihrer sozialen Kompetenzen,
d) zum Behandeln des Konsums, des Missbrauchs und der Abhängigkeit von Suchtmitteln, auch soweit diese Maßnahmen außerhalb des Vollzuges stattfinden,
e) zur Arbeitstherapie, zum Arbeitstraining, zur schulischen oder beruflichen Qualifizierung, zur Arbeit, zum freien Beschäftigungsverhältnisses oder zur Selbstbeschäftigung,
f) zur sozialen Hilfe, einschließlich ihres Beratens und Unterstützens beim Klären finanzieller Verbindlichkeiten, dem Schuldenregulieren oder dem Schuldentilgen, dem Erfüllen von Unterhaltspflichten, des Täter-Opfer-Ausgleiches oder einer anderen Art des Wiedergutmachens, des durch die Straftat verursachten Schadens und in sozialversicherungsrechtlichen Angelegenheiten,
g) durch ihre Außenkontakte, einschließlich Schriftwechsel, Besuchs-, Paket- und Telefonverkehr, Videodolmetschen oder anderen Telekommunikationsformen,
h) zum persönlichen Besitz, zum Einkauf oder zum Bezug von Zeitungen und Zeitschriften,
i) zum Gestalten ihrer Freizeit,
j) zum Ausüben ihrer Religion,
k) zu ihrer Versorgung und Gesundheitsfürsorge,
l) zu ihrer Vergütung, ihren Geldern und der Verwaltung ihrer Konten in den Anstalten,
m) zu ihrer Beteiligung an den Kosten des Vollzuges,
n) zu ihrer Disziplinierung,
o) zur Erziehung junger Gefangener,
p) zum Gewährleisten ihres Wahlrechtes,
q) zum Beteiligen und Hinzuziehen von Ehrenamtlichen, Beiräten, Einrichtungen, Organisationen, Vereinen oder Verbänden oder anderen beteiligten Personen,
r) im Rahmen von Lockerungen oder anderen Arten des Öffnens ihres Vollzuges, einschließlich ihres Begutachtens und Untersuchens oder
s) bei ihrer Entlassungsvorbereitung, ihrem Entlassen, ihrem Übergang in die Freiheit, ihrem Wiedereingliedern, nachgehenden Betreuen oder Verbleiben auf freiwilliger Grundlage, einschließlich ihrer Begutachtens und Untersuchens,

6. dem Aufrechterhalten von Sicherheit und Ordnung in den Anstalten zum Bespiel in Form

a) des Verhinderns von Entweichungen und Befreiungen,
b) des Vermeidens der Nichtrückkehr und des Missbrauches von Lockerungen oder anderen Arten des Öffnens des Vollzuges, einschließlich des Nacheilens, des Fahndens und des Wiederergreifens,
c) des erkennungsdienstlichen Behandelns, des Überprüfens, des Beobachtens, des Überwachens sowie des Absuchens und Durchsuchens der Gefangenen oder anderen betroffenen Personen und deren Sachen, auch mit technischen Hilfsmitteln,
d) des Feststellens von Konsum, Missbrauch oder Abhängigkeit von Suchtmitteln oder einer nicht stoffgebundenen Sucht,

e) des Abwehrens von Gefahren von Gewalttätigkeiten gegen Personen oder Sachen, des Selbstverletzens oder des Selbsttötens der Gefangenen und des Anwendens unmittelbaren Zwanges oder
f) des Verhinderns, des Störens oder des Beendens von Mobilfunkverkehr und des unbefugten Überfluges von Flugmodellen oder von unbemannten Luftfahrtsystemen,

7. dem Geltendmachen und dem Durchsetzen von Forderungen im Justizvollzug,

8. den Verwaltungsgeschäften im Justizvollzug, soweit diese sich auf die Gefangenen beziehen, einschließlich des Führens der Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern sowie des Buchwerks und der Justizvollzugsstatistiken,

9. dem Verfolgen oder dem Ahnden von Ordnungswidrigkeiten im Justizvollzug,

10. der Rechts- und Fachaufsicht, insbesondere

a) den Eingaben, Beschwerden und Petitionen,
b) dem Bau, dem Aufbau und der Organisation der Anstalten,
c) dem zentralen Führen der Justizvollzugsstatistiken,
d) dem Erstellen von Vollzugs- und Sicherheitskonzeptionen,
e) dem Vollstreckungsplan und der Belegungsfähigkeit,
f) dem Bilden von Vollzugsgemeinschaften und länderübergreifender Zusammenarbeit,
g) dem Zustimmen zu Lockerungen und anderen Arten des Öffnens des Vollzuges,
h) dem Überstellen, Verlegen, Ausführen, Vorführen und Ausantworten oder
i) dem Kooperieren und dem Austauschen mit den Justizvollzugsbehörden, den Justizbehörden und den Behörden mit Sicherheitsaufgaben,

11. der Ausbildung und der Fortbildung der im Justizvollzug Beschäftigten,

12. des Kriminologischen Dienstes im Justizvollzug,

13. der Strafvollstreckung,

14. dem Mitwirken der Justizvollzugsbehörden an den sonstigen durch Gesetz übertragenen Aufgaben, insbesondere dem Fertigen von Stellungnahmen und Einschätzungen zu den Gefangenen in behördlichen und gerichtlichen Verfahren oder

15. den weiteren, zum Erreichen der Vollzugsziele, zum Aufrechterhalten, zum Wiederherstellen und zum Durchsetzen der Sicherheit oder Ordnung und dem Zusammenleben in der Anstalt, zum Versorgen der Gefangenen, zur Resozialisierung, zum Schutz der Allgemeinheit vor weiteren Straftaten, zum Schutz für den Leib, das Leben, die Freiheit und das Vermögen einer Person sowie das Vermögen des Landes, erforderlichen Tätigkeiten.

Im Vollzug der Untersuchungshaft tritt an die Stelle des Erreichens der Vollzugsziele der Zweck, durch das sichere Unterbringen der Gefangenen und das Umsetzen von

haftgrundbezogenen Beschränkungen, das Durchführen eines geordneten Strafverfahrens zu gewährleisten.

§ 3
Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. „Gefangene“ Personen, an denen Freiheitsentziehungen nach § 1 vollzogen werden, auch die, welche die nachbetreuenden Angebote des Vollzuges annehmen oder dort verbleiben,

2. „Anstalten“ die Justizvollzugsanstalten, die Jugendanstalt, die Jugendarrestanstalt und die Einrichtung für den Vollzug der Unterbringung in der Sicherungsverwahrung,

3. „Justizvollzugsbehörden“ die Anstalten, der Landesbetrieb für Beschäftigung und Bildung der Gefangenen, die Zentrale Rechtsbeschwerdestelle in Strafvollzugssachen und Vollzugssachen der Unterbringung in der Sicherungsverwahrung, die IT-Leitstelle für den Justizvollzug, die Zentrale Beschaffungsstelle für den Justizvollzug und das für Justizvollzug zuständige Ministerium,

4. „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 durch das Zuordnen 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,

5. „Verarbeiten“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, das Organisieren, das Ordnen, das Speichern, das Anpassen, das Verändern, das Auslesen, das Abfragen, das Verwenden, das Offenlegen durch das Übermitteln, das Verbreiten oder eine andere Form des Bereitstellens, das Abgleichen, das Verknüpfen, das Berichtigen, das Einschränken, das Löschen oder das Vernichten,

6. „Weiterverarbeiten“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen aten, der oder die nicht das Erheben, das Auslesen, das Abfragen, das Offenlegen durch das Übermitten, das Verbreiten oder eine andere Form des Bereitstellens, das Berichtigen, das Einschränken, das Löschen oder das Vernichten umfasst,

7. „Einschränken des Verarbeitens“ das Markieren gespeicherter personenbezogener Daten mit dem Ziel, ihr künftiges Verarbeiten einzuschränken,

8. „Profiling“ jede Art des automatisierten Verarbeitens personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die

sich auf eine natürliche Person beziehen zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen,

9. „Anonymisieren“ das Verarbeiten personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

10. „Pseudonymisieren“ das Verarbeiten personenbezogener Daten in einer Weise, in der die Daten ohne das Hinzuziehen 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,

11. „Verschlüsseln“ eine technische Maßnahme, die Daten unter dem Anwenden kryptographischer Verfahren in eine für Dritte unverständliche Form umwandelt, so dass diese nach dem Stand von Wissenschaft und Technik ausschließlich von einem Schlüsselinhaber wieder in eine allgemein verständliche Form überführt (entschlüsselt) werden können,

12. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig, ob die Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird,

13. „Verantwortlicher“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel des Verarbeitens von personenbezogenen Daten entscheidet,

14. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet,

15. „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 Untersuchungsauftrages nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; das Verarbeiten dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken des Verarbeitens,

16. „Verletzen des Schutzes personenbezogener Daten“ ein Verletzen der Sicherheit, das zum unbeabsichtigten oder unrechtmäßigen Vernichten, zum Verlorengehen, zum Verändern oder zum unbefugten Offenlegen von personenbe-

zogenen Daten oder zu unbefugtem Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden,

17. „personenbezogene Daten besonderer Kategorien“

    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 zum eindeutigen Identifizieren einer natürlichen Person,

    d) Gesundheitsdaten und

    e) Daten zum Sexualleben oder zur sexuellen Orientierung,

18. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, welche eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden,

19. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die ein eindeutiges Identifizieren dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten,

20. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich des Erbringens von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen,

21. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehreren Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde,

22. „Einwilligen“ jedes freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Bekunden des Willens in Form einer Erklärung oder eines sonstigen eindeutigen bestätigenden Handelns, mit dem die betroffene Person zu verstehen gibt, dass sie mit dem Verarbeiten der sie betreffenden personenbezogenen Daten einverstanden ist,

23. „anstaltsfremde Person“ eine Person, die zu den Justizvollzugsbehörden nicht in einem Dienst- oder Arbeitsverhältnis steht und nicht im Auftrag einer anderen Stelle tätig ist oder nicht als Organ der Rechtspflege handelt,

24. „Öffentliche Stellen“

    a) Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform,

    b) Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden, der Verbandsgemeinden, der Landkreise und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen, ungeachtet ihrer Rechtsform,

    c) Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Mitgliedstaates der Europäischen Union,

25. „nicht öffentliche Stellen“ natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht die Voraussetzungen von Nummer 24 erfüllen; nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes,

26. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89, L 127 vom 23.5.2018, S. 9) eingerichtete unabhängige staatliche Stelle.

Abschnitt 2
Grundsätze des Verarbeitens personenbezogener Daten

§ 4
Allgemeine Grundsätze

(1) Im Justizvollzug ist das Recht einer jeden Person zu schützen, grundsätzlich selbst über das Preisgeben und Verwenden ihrer personenbezogenen Daten zu bestimmen.

(2) Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszweckes erforderlich sein und ihr Verarbeiten nicht außer Verhältnis zu diesem Zweck stehen,

4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihres Verarbeitens unrichtig sind, unverzüglich gelöscht und vernichtet oder berichtigt werden,

5. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die ein Identifizieren der betroffenen Person ermöglicht, und

6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugtem oder unrechtmäßigem Verarbeiten, unbeabsichtigtem Verlorengehen, unbeabsichtigtem Zerstören oder unbeabsichtigtem Beschädigen.

(3) Werden personenbezogene Daten besonderer Kategorien verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Person vorzusehen. Geeignete Garantien können insbesondere sein:

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,

2. das Festlegen von besonderen Aussonderungsprüffristen,

3. das Sensibilisieren der an Verarbeitungsvorgängen Beteiligten,

4. das Beschränken des Zugangs innerhalb der Justizvollzugsbehörden,

5. das von anderen personenbezogenen Daten getrennte Verarbeiten,

6. das Pseudonymisieren personenbezogener Daten,

7. das Anonymisieren personenbezogener Daten,

8. das Verschlüsseln personenbezogener Daten oder

9. spezifische Verfahrensregelungen, die, im Fall des Offenlegens personenbezogener Daten durch das Übermitteln oder andere Art des Bereitstellens oder des Verarbeitens für andere Zwecke, die Rechtmäßigkeit des Verarbeitens sicherstellen.

§ 5
Andere Zwecke

Das Verarbeiten personenbezogener Daten zu einem anderen vollzuglichen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn das Verarbeiten zu diesem Zweck erforderlich und verhältnismäßig ist. Das Verarbeiten personenbezogener Daten zu einem anderen nach diesem Gesetz anerkannten Zweck, ist insbesondere zulässig, wenn es in einer Regelung dieses Gesetzes oder einer anderen Rechtsvorschrift vorgesehen ist oder zwingend vorausgesetzt wird.

§ 6
Archivarische, wissenschaftliche oder statistische Zwecke

Das Verarbeiten personenbezogener Daten ist im Rahmen der in § 1 genannten Zwecke auch in archivarischer, wissenschaftlicher oder statistischer Form zulässig, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Person vorgesehen werden. Solche Garantien können in einem so zeitnah wie möglich erfolgenden Anonymisieren der personenbezogenen Daten, in Vorkehrungen gegen das Kenntnisnehmen durch unbefugte Personen oder in ihrem räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeiten bestehen.

§ 7
Unterscheiden verschiedener Kategorien von betroffenen Personen

Die Justizvollzugsbehörden unterscheiden beim Verarbeiten personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen. Dies betrifft insbesondere die folgenden Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,

2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,

3. verurteilte Straftäter,

4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten,

5. Besucher und andere anstaltsfremden Personen sowie

6. andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 8
Unterscheiden zwischen auf Fakten basierenden und auf persönlichen Einschätzungen beruhenden personenbezogenen Daten

Die Justizvollzugsbehörden unterscheiden beim Verarbeiten personenbezogener Daten so weit wie möglich danach, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck sollen sie, soweit dies im Rahmen des jeweiligen Verarbeitungsvorganges möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 9
Automatisiertes Entscheiden im Einzelfall

Das ausschließlich auf einem automatisierten Verarbeiten personenbezogener Daten beruhende Entscheiden, das mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder diese erheblich beeinträchtigt, ist nur zulässig, wenn es in einer Rechtsvorschrift vorgesehen ist. Entscheidungen nach Satz 1 dürfen nicht auf personenbezogenen Daten besonderer Kategorien beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Person getroffen wurden. Profiling, das zur Folge hat, dass die betroffene Person auf der Grundlage von personenbezogenen Daten besonderen Kategorien diskriminiert wird, ist verboten.

§ 10
Prüfen nach Fristen

Die Justizvollzugsbehörden prüfen regelmäßig nach festgesetzten Fristen, ob personenbezogene Daten weiterhin zu speichern, zu löschen und zu vernichten, in ihrem Verarbeiten einzuschränken oder zu berichtigen sind. Sie stellen, insbesondere durch organisatorische und verfahrensrechtliche Vorkehrungen sowie Beteiligen des Datenschutzbeauftragten sicher, dass diese Pflichten eingehalten werden.

§ 11
Einwilligen der betroffenen Person

(1) Soweit die betroffene Person in das Verarbeiten ihrer personenbezogenen Daten aufgrund einer Rechtsvorschrift einwilligen kann, müssen die Justizvollzugsbehörden das Einwilligen der betroffenen Person nachweisen können.

(2) Hat die betroffene Person eingewilligt und sind davon noch andere Sachverhalte betroffen, muss das Ersuchen um das Einwilligen der betroffenen Person in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person kann jederzeit ihr Einwilligen in das Verarbeiten ihrer personenbezogenen Daten widerrufen. Durch den Widerruf wird die Rechtmäßigkeit des bis zum Widerruf erfolgten Verarbeitens ihrer personenbezogenen Daten nicht berührt. Die betroffene Person ist, bevor sie einwilligt, hiervon in Kenntnis zu setzen.

(4) Hat die betroffene Person eingewilligt, so ist dies nur wirksam, wenn eine freie Entscheidung der betroffenen Person nachgewiesen werden kann. Beim Beurteilen, ob eine freiwillige Entscheidung vorliegt, sind auch die Umstände zu berücksichtigen, die die betroffene Person dazu veranlasst haben, in das Verarbeiten ihrer personenbezogenen Daten einzuwilligen. Die betroffene Person ist auf den vorgesehenen Zweck des Verarbeitens ihrer personenbezogenen Daten hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen zu belehren, wenn sie nicht in das Verarbeiten personenbezogener Daten einwilligt.

(5) Soweit personenbezogene Daten besonderer Kategorien auf der Grundlage des Einwilligens der betroffenen Person verarbeitet werden können, muss die betroffene Person ausdrücklich in das Verarbeiten dieser personenbezogenen Daten eingewilligt haben.

(6) Soweit die betroffene Person nicht die für eine Entscheidung notwendige Einsichtsfähigkeit besitzt und das Erfüllen der in § 1 genannten Zwecke nicht gefährdet wird, steht das ihr zustehende Recht, informiert und gehört zu werden oder Fragen und Anträge zu stellen, ihren gesetzlichen Vertretern zu. Sind mehrere betroffene Personen berechtigt, kann jeder von ihnen die in diesem Gesetz bestimmten Rechte allein ausüben. Sind Mitteilungen vorgeschrieben, genügt es, wenn sie an einen von ihnen gerichtet werden.

Abschnitt 3
Sicherheit personenbezogener Daten

§ 12
Datengeheimnis

(1) Die in den Justizvollzugsbehörden beschäftigten Personen dürfen sich nach Maßgabe dieses Gesetz von personenbezogenen Daten nur Kenntnis verschaffen, soweit dies zum Erfüllen der in § 1 genannten Zwecke oder für die Zusammenarbeit erforderlich ist. Ihnen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Personen, die nicht Amtsträger im Sinne des § 11 Abs. 1 Nr. 2 des Strafgesetzbuches sind und Personen, die für eine nicht öffentliche Stelle Kenntnis von personenbezogenen Daten erlangen sollen, die durch die Justizvollzugsbehörden offengelegt werden können, sind vor dem Aufnehmen ihrer Tätigkeit über die zu beachtenden Bestimmungen zu unterrichten und auf deren Einhalten förmlich nach dem Verpflichtungsgesetz zu verpflichten.

(2) Personen, die nicht nach Absatz 1 förmlich verpflichtet wurden, dürfen von personenbezogenen Daten nur Kenntnis erlangen, wenn

1. die personenbezogenen Daten vorher pseudonymisiert wurden,

2. das förmliche Verpflichten vor dem Kenntnisnehmen Leib oder Leben eines Menschen oder bedeutende Sachwerte gefährden würde und das Verpflichten veranlasst und unverzüglich nachgeholt wird; erfolgt das Offenlegen personenbezogener Daten nicht durch die Justizvollzugsbehörden, sind diese hiervon unverzüglich unter Angabe der Personalien der Kenntnis nehmenden Personen zu unterrichten oder

3. sie Amtsträger im Sinne von § 11 Abs. 1 Nr. 2 des Strafgesetzbuches sind.

(3) Die Justizvollzugsbehörden stellen auf geeignete Weise sicher, dass bei nicht öffentlichen Stellen nur solche Personen Kenntnis von personenbezogenen Daten nehmen, die zuvor nach Absatz 1 verpflichtet wurden oder die nach Absatz 2 auch ohne das förmliche Verpflichten Kenntnis von personenbezogenen Daten nehmen dürfen.

(4) Personenbezogene Daten der Gefangenen dürfen innerhalb der Anstalten allgemein kenntlich gemacht werden, soweit dies für ein geordnetes Zusammenleben in den Anstalten erforderlich ist und Bestimmungen dieses Gesetzes nicht entgegenstehen. Personenbezogene Daten besonderer Kategorien dürfen nicht allgemein kenntlich gemacht werden.

(5) Personenbezogene Daten in Akten sind vor unbefugtem Zugang und Gebrauch zu schützen. Hierzu sollen Gesundheitsakten und Krankenblätter sowie Therapieakten getrennt von anderen Unterlagen und die Gefangenenpersonalakte in Teil- oder Unterbänden geführt und gesichert werden.

(6) Das Datengeheimnis und die hieraus entstehenden Pflichten bestehen auch nach dem Beenden der Tätigkeit fort.

§ 13
Technische und organisatorische Maßnahmen

(1) Die Justizvollzugsbehörden und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeiten für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihres Verarbeitens, 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.

(2) Unter Berücksichtigung des Standes der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke des Verarbeitens sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere der mit dem Verarbeiten verbundenen Gefahren für die Rechtsgüter der betroffenen Person treffen die Justizvollzugsbehörden und der Auftragsverarbeiter zum Zeitpunkt des Festlegens der Mittel für das Verarbeiten personenbezogener Daten und zum Zeitpunkt des eigentlichen Verarbeitens personenbezogener Daten auch die erforderlichen technischen und organisatorischen Maßnahmen, die beim Verarbeiten personenbezogener Daten ein dem Risiko angemessenes Schutzniveau gewährleisten, insbesondere im Hinblick auf das Verarbeiten personenbezogener Daten besonderer Kategorien. Die Justizvollzugsbehörden berücksichtigen hierbei auch die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik.

(3) Die in Absatz 2 genannten Maßnahmen können unter anderem das Pseudonymisieren und das Verschlüsseln personenbezogener Daten umfassen, soweit dies in Anbetracht der Verarbeitungszwecke möglich ist. Die Maßnahmen nach Absatz 2 sollen dazu führen, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

2. personenbezogene Daten während des Verarbeitens 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 beim Verarbeiten 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 (Nichtverkettbarkeit)

und

8. Verfahren so gestaltet werden, dass sie den betroffenen Personen das Ausüben der in Abschnitt 5 genannten Rechte wirksam ermöglichen (Intervenierbarkeit).

(4) Im Fall eines automatisierten Verarbeitens ergreifen die Justizvollzugsbehörden und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen, die Folgendes bezwecken:

1. Verwehren des Zugangs zu Verarbeitungsanlagen, mit denen das Verarbeiten personenbezogener Daten durchgeführt wird, für Unbefugte (Zugangskontrolle),

2. Verhindern des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),

3. Verhindern des unbefugten Eingebens von personenbezogenen Daten sowie des unbefugten Kenntnisnehmens, Veränderns und Löschens von gespeicherten personenbezogenen Daten (Speicherkontrolle),

4. Verhindern des Nutzens automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zum Übertragen personenbezogener Daten durch Unbefugte (Benutzerkontrolle),

5. Gewährleisten, dass die zum Benutzen eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),

6. Gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zum Datenübertragen übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

7. Gewährleisten, 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. Gewährleisten, dass beim Übermitteln personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität personenbezogener Daten geschützt werden (Transportkontrolle),

9. Gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),

10. Gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),

11. Gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),

12. Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Justizvollzugsbehörden verarbeitet werden können (Auftragskontrolle),

13. Gewährleisten, dass personenbezogene Daten gegen das Zerstören oder das Verlorengehen geschützt sind (Verfügbarkeitskontrolle),

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

Ein Zweck nach Satz 1 Nrn. 2 bis 5 kann insbesondere durch das Verwenden von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

(5) Die von den Justizvollzugsbehörden zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzeptes zu ermitteln, zu dessen Bestandteilen auch das Abschätzen der Eintrittswahrscheinlichkeit und der Schwere der mit dem Verarbeiten personenbezogener Daten verbundenen Risiken für das Recht auf informationelle Selbstbestimmung gehört.

(6) Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik regelmäßig zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen, soweit dies mit einem angemessenen Aufwand möglich ist.

§ 14
Datenschutzfolgenabschätzung

(1) Hat eine Form des Verarbeitens personenbezogener Daten, insbesondere beim Verwenden neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke des Verarbeitens personenbezogener Daten voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge, so schätzen die Justizvollzugsbehörden vorab die Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffene Person ab.

(2) Für das Untersuchen mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Folgenabschätzung vorgenommen werden.

(3) Die Justizvollzugsbehörden beteiligen dn Datenschutzbeauftragten an dem Durchführen der Folgenabschätzung.

(4) Die Folgenabschätzung trägt den Rechten der von dem Verarbeiten personenbezogener Daten betroffenen Person Rechnung und enthält zumindest die folgenden Angaben:

1. das systematische Beschreiben der geplanten Verarbeitungsvorgänge und der Zweck des Verarbeitens personenbezogener Daten,

2. das Bewerten der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,

3. das Bewerten der Gefahren für die Rechtsgüter der betroffenen Person und

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

§ 15
Verzeichnis von Verarbeitungstätigkeiten

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

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten des Datenschutzbeauftragten,

2. die Zwecke des Verarbeitens personenbezogener Daten,

3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,

4. das Beschreiben der Kategorien betroffener Personen und der Kategorien von personenbezogenen Daten,

5. das Verwenden von Profiling,

6. die Kategorien des Offenlegens personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,

7. Angaben über die Rechtsgrundlagen des Verarbeitens personenbezogener Daten,

8. die vorgesehenen Fristen für das Löschen und Vernichten oder das Überprüfen der Erforderlichkeit des Speicherns der verschiedenen Kategorien von personenbezogenen Daten und

9. das allgemeine Beschreiben der technischen und organisatorischen Maßnahmen.

(2) Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten personenbezogener Daten, die er im Auftrag einer Justizvollzugsbehörde durchführt, das folgende Angaben enthält:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, der Justizvollzugsbehörde, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie des Datenschutzbeauftragten,

2. das Offenlegen von personenbezogenen Daten gegenüber Stellen in einem Drittstaat oder an internationale Organisationen unter Angabe des Staates oder der Organisation und

3. das allgemeine Beschreiben der technischen und organisatorischen Maßnahmen.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse werden schriftlich oder in einem elektronischen Format geführt.

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

§ 16
Protokollieren des Verarbeitens personenbezogener Daten

(1) In automatisierten Verarbeitungssystemen protokollieren die Justizvollzugsbehörden und der Auftragsverarbeiter mindestens die folgenden Vorgänge des in ihrer Verantwortung liegenden Verarbeitens personenbezogener Daten:

1. das Erheben,

2. das Speichern,

3. das Verändern,

4. das Abfragen,

5. das Offenlegen durch das Übermitteln oder eine andere Art des Bereitstellens,

6. das Kombinieren

7. das Einschränken und

8. das Löschen und Vernichten.

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

(3) Die Protokolle dürfen ausschließlich für das Überprüfen der Rechtmäßigkeit des Verarbeitens personenbezogener Daten durch den Datenschutzbeauftragten oder den Landesbeauftragten für den Datenschutz und die betroffene Person sowie für das Eigenüberwachen, für das Gewährleisten der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Die Protokolldaten werden zwei Jahre nach deren Generieren gelöscht.

(5) Die Justizvollzugsbehörden und der Auftragsverarbeiter stellen auf Anfordern die Protokolle dem Landesbeauftragten für den Datenschutz zur Verfügung.

§ 17
Melden von Verstößen

Die Justizvollzugsbehörden stellen sicher, dass ihnen vertrauliche Meldungen über die in ihrem Verantwortungsbereich erfolgenden Verstöße gegen Datenschutzvorschriften zugeleitet werden.

Abschnitt 4
Rechtsgrundlagen des Verarbeitens personenbezogener Daten

Unterabschnitt 1
Erheben personenbezogener Daten

§ 18
Zulässigkeit des Erhebens personenbezogener Daten

(1) Personenbezogene Daten dürfen erhoben werden, soweit dies zu vollzuglichen Zwecken erforderlich ist.

(2) Personenbezogene Daten besonderer Kategorien dürfen erhoben werden, soweit

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. dies zu vollzuglichen Zwecken oder

3. dies unter Berücksichtigung der Interessen der betroffenen Person an dem Geheimhalten ihrer personenbezogenen Daten

   a) zum Abwehren einer Gefahr für das Leben eines Menschen, insbesondere zum Verhüten von Selbsttötungen,

   b) zum Abwehren einer erheblichen Gefahr für die Gesundheit oder anderer lebenswichtiger Interessen eines Menschen,

c) zum Abwehren der Gefahr von Straftaten von erheblicher Bedeutung oder

d) zum Abwehren erheblicher Nachteile für das Gemeinwohl oder sonst unmittelbar drohender Gefahren für die öffentliche Sicherheit

unbedingt erforderlich ist oder

4. die Daten von der betroffenen Person offenkundig öffentlich gemacht wurden.

§ 19
Erheben personenbezogener Daten bei der betroffenen Person

(1) Personenbezogene Daten sind grundsätzlich bei der betroffenen Person und mit deren Kenntnis zu erheben.

(2) Werden personenbezogene Daten bei der betroffenen Person mit deren Kenntnis erhoben, so ist diese in geeigneter Weise über den Zweck des Erhebens und das Bestehen von Auskunfts- und Berichtigungsrechten aufzuklären. Werden die personenbezogenen Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist das Erteilen der Auskunft Voraussetzung für das Gewähren von Rechtsvorteilen, ist die betroffene Person hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Sind die Angaben für das Gewähren einer Leistung erforderlich, ist die betroffene Person über die möglichen Folgen des Nichtbeantwortens aufzuklären.

(3) Das Erheben personenbezogener Daten bei der betroffenen Person ohne deren Kenntnis ist zulässig, wenn keine Anhaltspunkte vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

§ 20
Erheben personenbezogener Daten über Gefangene bei Dritten

(1) Soweit das Erheben personenbezogener Daten über Gefangene bei der betroffenen Person zulässig ist, dürfen sie auch bei Dritten erhoben werden, wenn

1. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

2. dies zum Abwehren erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,

3. dies zum Abwehren einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,

4. offensichtlich ist, dass dies im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass sie in Kenntnis des Zweckes nicht einwilligen würde,

5. sich das Erheben auf personenbezogene Daten aus gerichtlichen Verfahren bezieht, die dem Vollstrecken der gegenwärtigen Freiheitsentziehung und er-

forderlichenfalls auch vorhergehender Freiheitsentziehungen zugrunde liegen oder lagen oder diese sonst betreffen,

6. keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Person dem Erheben ohne ihr Mitwirken entgegenstehen und

   a) die betroffene Person einer durch Rechtsvorschrift festgelegten Auskunftspflicht nicht nachgekommen und über das beabsichtigte Erheben personenbezogener Daten bei Dritten unterrichtet worden ist,

   b) das Erheben personenbezogene Daten bei der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde oder

   c) die personenbezogenen Daten der betroffenen Person allgemein zugänglich sind.

7. dies zum Erreichen des Vollzugsziels oder zum Abwehren einer drohenden Gefahr für die Sicherheit der Anstalten erforderlich ist oder

8. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt.

(2) Personenbezogene Daten über den Gefangenen dürfen ohne dessen Kenntnis auch bei seinen gesetzlichen Vertretern zu vollzuglichen Zwecken erhoben werden, wenn der Gefangene nicht die für sein Einwilligen notwendige Einsichtsfähigkeit besitzt.

(3) Nicht öffentliche Stellen sind auf die Rechtsvorschrift, die zur Auskunft verpflichtet, ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 21
Erheben personenbezogener Daten über Personen, die keine Gefangenen sind

Personenbezogene Daten über Personen, die keine Gefangenen sind, dürfen ohne ihre Kenntnis bei Gefangenen oder Dritten erhoben werden, soweit dies zu vollzuglichen Zwecken unbedingt erforderlich ist und schutzwürdige Interessen der betroffenen Person hierdurch nicht beeinträchtigt werden. Nicht öffentliche Stellen sind auf die Rechtsvorschrift, die zur Auskunft verpflichtet, ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 22
Identifizieren von Gefangenen und anstaltsfremden Personen

(1) Zu vollzuglichen Zwecken, insbesondere zum Sichern des Vollzuges und zum Aufrechterhalten der Sicherheit oder Ordnung der Anstalten sind die folgenden Maßnahmen zum Feststellen der Identität des Gefangenen zulässig:

1. das Aufnehmen von Lichtbildern,

2. das Abnehmen von Finger- und Handflächenabdrücken,

3. das Feststellen von äußerlichen körperlichen Merkmalen,

4. Messungen,

5. das Erheben von Merkmalen der Finger, der Hände, des Gesichtes, der Augen, der Stimme auch mittels biometrischer Verfahren und

6. das Erheben der Unterschrift.

(2) Bestehen Zweifel an der Identität des Gefangenen, dürfen die Justizvollzugsbehörden, soweit dies zum Feststellen der Identität des Gefangenen erforderlich ist, unverzüglich das Landeskriminalamt um Auskunft ersuchen und hierzu die von ihnen erhobenen oder anderweitig bei ihnen vorliegenden personenbezogenen Daten des Gefangenen offenlegen. Das Landeskriminalamt veranlasst den Abgleich dieser personenbezogenen Daten zum Zwecke des Identifizierens des Gefangenen und teilt das Ergebnis den Justizvollzugsbehörden mit. Unter den Voraussetzungen von Satz 1 dürfen die Justizvollzugsbehörden auch das Bundeskriminalamt sowie das Bundesamt für Migration und Flüchtlinge um einen Abgleich der personenbezogenen Daten des Gefangenen ersuchen.

(3) Das Betreten der Anstalten durch eine anstaltsfremde Person kann davon abhängig gemacht werden, dass diese zum Feststellen ihrer Identität

1. ihre Vornamen, ihren Namen und ihre Anschrift angibt und durch amtliche Ausweise nachweist und

2. das Erheben von Merkmalen der Finger, der Hände, des Gesichtes, der Augen, der Stimme auch mittels biometrischer Verfahren oder der Unterschrift duldet, soweit dies erforderlich ist, um das Verwechseln und das Austauschen von Gefangenen mit anderen Personen zu verhindern.

Die nach Satz 1 erhobenen Identifikationsmerkmale sind spätestens 24 Stunden nach ihrem Erheben zu löschen und zu vernichten, soweit nicht ein Fall von § 30 Abs. 2 Nr. 2 vorliegt; in diesem Fall sind sie unverzüglich offenzulegen und danach zu löschen und zu vernichten.

§ 23
Sicherheitsrelevante Erkenntnisse über Gefangene und anstaltsfremde Personen

Zum Zwecke des Aufrechterhaltens, des Wiederherstellens und des Durchsetzens der Sicherheit der Anstalten dürfen die Justizvollzugsbehörden regelmäßig prüfen, ob sicherheitsrelevante Erkenntnisse über Gefangene oder anstaltsfremde Personen, die Zugang zu den Anstalten begehren, vorliegen. Insbesondere Erkenntnisse zu diesen Personen über ihre extremistischen, gewaltorientierten Einstellungen oder ihre Kontakte zu derartigen Organisationen, Gruppierungen oder Personen oder ihre Kontakte zur organisierten Kriminalität sind sicherheitsrelevant. Wirken anstaltsfremde Personen beim Erreichen vollzuglicher Zwecke der Gefangenen mit, können über Satz 1 hinaus auch Erkenntnisse über strafrechtliche Verurteilungen, eine bestehende Suchtproblematik oder andere, für das Beurteilen der Zuverlässigkeit der anstaltsfremden Person notwendige Umstände sicherheitsrelevant sein.

§ 24
Überprüfen des Gefangenen

(1) Bestehen tatsächliche Anhaltspunkte für eine in einem überschaubaren Zeitraum drohende und einem Gefangenen zurechenbare Gefahr für die Sicherheit der Anstalten, dürfen die Justizvollzugsbehörden, die Justizbehörden, die Behörden mit Sicherheitsaufgaben und andere Justizvollzugsbehörden um Auskunft ersuchen. Insbesondere dürfen sie dazu

1. eine Auskunft nach § 41 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes einholen,

2. sicherheitsrelevante Erkenntnisse bei den Polizeibehörden des Bundes und der Länder anfragen und,

3. soweit im Einzelfall erforderlich, beim Verfassungsschutz des Landes das Vorliegen sicherheitsrelevanter Erkenntnissen anfragen.

Tatsächliche Anhaltspunkte für eine in einem überschaubaren Zeitraum drohende und einem Gefangenen zurechenbare Gefahr können sich insbesondere auch aus dessen Persönlichkeit oder Verurteilungen oder seinem Verhalten im Vollzug ergeben.

(2) Die Anfrage nach Absatz 1 Satz 2 Nr. 2 erstreckt sich nur auf die personengebundenen Hinweise und die Erkenntnisse des polizeilichen Staatsschutzes. Bei der Anfrage nach Absatz 1 Satz 2 Nr. 3 erfolgt die Abfrage des nachrichtendienstlichen Informationssystems durch den Verfassungsschutz des Landes.

(3) Die Justizvollzugsbehörden legen den angefragten Behörden, soweit möglich, den Nachnamen, Geburtsnamen, die Vornamen, das Geburtsdatum, das Geschlecht, den Geburtsort, das Geburtsland und die Staatsangehörigkeit des Gefangenen offen. Über Satz 1 hinaus sollen bekannt gewordene Aliaspersonalien, die voraussichtliche Vollzugsdauer sowie das Aktenzeichen der der Vollstreckung zugrundeliegenden Entscheidungen offengelegt werden.

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

(5) Bestehen aufgrund der offengelegten sicherheitsrelevanten Erkenntnisse tatsächliche Anhaltspunkte für eine Gefahr der Sicherheit der Anstalten, dürfen die Justizvollzugsbehörden zusätzliche Auskünfte oder Unterlagen bei den Justizbehörden, den Behörden mit Sicherheitsaufgaben und anderen Justizvollzugsbehörden einholen.

(6) Die im Rahmen der Anfrage mitgeteilten sicherheitsrelevanten Erkenntnisse sind in gesonderten Akten oder Dateisystemen zu führen.

(7) Die Befugnis zum Verarbeiten sicherheitsrelevanter Erkenntnisse über den Gefangenen zum Aufrechterhalten, Wiederherstellen und Durchsetzen der Sicherheit

der Anstalt schließt die Befugnis zum Weiterverarbeiten und Offenlegen dieser personenbezogenen Daten zum Zwecke der Vollzugs- und Eingliederungsplanung des Gefangenen ein.

§ 25
Überprüfen einer anstaltsfremden Person

(1) Eine anstaltsfremde Person, die in den Anstalten tätig werden soll, darf zu diesen Tätigkeiten nur zugelassen werden, wenn keine Sicherheitsbedenken bestehen. Die Justizvollzugsbehörden nehmen zum Aufrechterhalten der Sicherheit der Anstalten eine Zuverlässigkeitsüberprüfung der anstaltsfremden Person vor, wenn diese einwilligt. Dazu dürfen sie insbesondere

1. eine Auskunft nach § 41 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes einholen,

2. sicherheitsrelevante Erkenntnisse der Polizeibehörden des Bundes und der Länder anfragen und,

3. soweit im Einzelfall erforderlich, beim Verfassungsschutz des Landes das Vorliegen sicherheitsrelevanter Erkenntnisse anfragen.

Ist ein Überprüfen in Eilfällen, beispielsweise bei kurzfristig notwendigen Reparaturarbeiten, nicht möglich, soll die anstaltsfremde Person bei der Tätigkeit in den Anstalten beaufsichtigt werden.

(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 der anstaltsfremden Person in den Anstalten, eine Gefährdung der Sicherheit der Anstalten fernliegt.

(3) Darüber hinaus dürfen die Justizvollzugsbehörden bei tatsächlichen Anhaltspunkten einer drohenden Gefahr für die Sicherheit der Anstalten auch bei Personen, welche das Zulassen zum Besuch von Gefangenen oder zum Besuch der Anstalten begehren, eine Zuverlässigkeitsüberprüfung vornehmen, wenn diese einwilligen. Absatz 1 Satz 3 gilt entsprechend. Bei Anfragen nach Absatz 1 Satz 3 Nrn. 2 und 3 teilen die Justizvollzugsbehörden auch mit, ob und für welchen Gefangenen das Zulassen zum Besuch begehrt wird.

(4) Absatz 3 gilt nicht für Besuche von Verteidigern und Beiständen sowie von Rechtsanwälten und Notaren in einer den Gefangenen betreffenden Rechtssache sowie für die im Rahmen des Überwachens des Schriftwechsels privilegierten Personen und Stellen.

(5) Werden den Justizvollzugsbehörden sicherheitsrelevante Erkenntnisse bekannt, wird die anstaltsfremde Person nicht oder nur unter Beschränkungen zu der Tätigkeit oder dem Besuch in den Anstalten zugelassen. Gleiches gilt, wenn die anstaltsfremde Person nicht in eine Zuverlässigkeitsüberprüfung einwilligt.

(6) Wenn neue sicherheitsrelevante Erkenntnisse vorliegen, spätestens jedoch nach Ablauf von fünf Jahren, sollen Zuverlässigkeitsüberprüfungen erneuert werden, sofern ihre Erforderlichkeit nach Absatz 1 Satz 1 und 2 und Absatz 3 weiterbesteht.

§ 26
Optisch-elektronisches Beobachten

(1) Die Anstalten dürfen personenbezogene Daten durch optisch-elektronisches Beobachten in ihren Gebäuden, Räumen und Freiflächen sowie ihrem unmittelbar angrenzenden Umfeld erheben, soweit

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. dies zum Aufrechterhalten, Wiederherstellen und Durchsetzen der Sicherheit oder Ordnung der Anstalten und des Schutzes der Allgemeinheit erforderlich ist, insbesondere um das Entweichen oder das Befreien der Gefangenen sowie Werfen von Gegenständen auf das Gelände der Anstalten und das Betreten bestimmter Zonen und Bereiche der Anstalten und Bereiche der Anstalten durch Unbefugte zu verhindern oder zu beenden,

3. dies dem Wahrnehmen und dem Durchsetzen des Hausrechts dient,

4. dies für das Wahrnehmen und das Durchsetzen berechtigter Interessen für konkret festgelegte Zwecke, beispielsweise zum Schutz des Eigentums oder des Besitzes erforderlich ist oder

5. dies in § 27 für Räume oder Bereiche zum Unterbringen der Gefangenen gesondert bestimmt ist

und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Satz 1 gilt auch für und in Fahrzeugen zum Durchführen des Transportes von Gefangenen.

(2) Der Umstand und die Reichweite des Erhebens personenbezogener Daten durch optisch-elektronisches Beobachten sowie der Name und die Kontaktdaten der Anstalten sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt und für jedermann eindeutig kenntlich zu machen.

(3) Die Anstalten, die Einrichtungen zum Erheben personenbezogener Daten durch optisch-elektronisches Beobachten einsetzen, erstellen hierzu nach Maßgabe dieses Gesetzes ein einheitliches Konzept. Das Konzept enthält alle betriebsfähigen optisch-elektronischen Einrichtungen sowie die von ihnen erfassten Bereiche in kartenmäßiger Darstellung und ist regelmäßig auf seine Aktualität und Notwendigkeit zu überprüfen, anzupassen und fortzuschreiben.

§ 27
Optisch-elektronisches Beobachten in Räumen oder Bereichen zum Unterbringen der Gefangenen

(1) Das Erheben personenbezogener Daten durch optisch-elektronisches Beobachten in Räumen oder Bereichen zum Unterbringen der Gefangenen ist nur zulässig, soweit

1. dies zum Abwehren von Gefahren von Gewalttätigkeiten gegen Personen oder Sachen, des Selbstverletzens oder des Selbsttötens von Gefangenen erforderlich ist und innerhalb von besonders gesicherten Hafträumen, besonders gesicherten Räumen, Kamera überwachten Hafträumen und anderen, dem Überwachen und Beaufsichtigen von Gefangenen dienenden Räumen erfolgt oder

2. dies für die Dauer eines Einsatzes des Sicherheits- und Revisionsdienstes der Anstalten oder des Besonderen Sicherheits- und Revisionsdienstes des Landes zum Aufrechterhalten oder Wiederherstellen der Sicherheit und Ordnung in den Anstalten, insbesondere zum Abwehren der in Nummer 1 genannten Gefahren, erforderlich ist.

(2) Das optisch-elektronische Beobachten ist unverzüglich zu beenden, wenn der Zweck dessen Anordnung nicht mehr erreicht werden kann. Das optisch-elektronische Beobachten ist gesondert durch den Anstaltsleiter schriftlich anzuordnen und zu begründen. Die Anordnung enthält auch den Umfang des optisch-elektronischen Beobachtens. Das optisch-elektronische Beobachten ist spätestens nach 72 Stunden zu beenden, sofern es nicht durch eine neue Anordnung des Anstaltsleiters verlängert wird. Die Anordnungen sind zur Gefangenenpersonalakte des betroffenen Gefangenen zu nehmen.

(3) Während der Dauer des optisch-elektronischen Beobachtens ist dieses für die Gefangenen kenntlich zu machen.

(4) Beim Gestalten der Gebäude, Räume oder Bereiche, die optisch-elektronisch beobachtet werden und beim bildlichen Wiedergeben der dadurch erhobenen personenbezogenen Daten, ist auf die Bedürfnisse der Gefangenen auf Wahrung ihrer Intimsphäre angemessen Rücksicht zu nehmen, insbesondere sollen sanitäre Einrichtungen vom optisch-elektronischen Beobachten, soweit möglich, ausgenommen werden. Das Erkennen dieser Bereiche kann, auch durch technische Maßnahmen, teilweise ausgeschlossen werden.

(5) Das optisch-elektronische Beobachten ist zu unterbrechen, wenn es vorübergehend nicht erforderlich oder das Beaufsichtigen gesetzlich ausgeschlossen ist.

§ 28
Auslesen von Datenspeichern

(1) Die Justizvollzugsbehörden dürfen elektronische Datenspeicher sowie elektronische Geräte mit Datenspeichern auslesen, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies zu vollzuglichen Zwecken erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Ist die betroffene Person bekannt, sind ihr die

Gründe vor dem Auslesen mitzuteilen. Beim Auslesen sind ihre schutzwürdigen Interessen zu berücksichtigen. Das Auslesen ist möglichst auf die Inhalte zu beschränken, die zum Erreichen der die Anordnung begründenden Zwecke erforderlich sind.

(2) Personenbezogene Daten, die in den Kernbereich der privaten Lebensgestaltung der betroffenen Person fallen, dürfen nicht erhoben werden. Sind solche personenbezogenen Daten versehentlich erhoben wurden, sind sie unverzüglich zu löschen und zu vernichten. Erkenntnisse zu diesen personenbezogenen Daten dürfen nicht weiterverarbeitet werden. Die Tatsache ihres Erhebens, ihres Löschens und ihres Vernichtens sind zu dokumentieren.

(3) Der Gefangene ist bei der Aufnahme in die Anstalt über die Möglichkeit des Auslesens nach Absatz 1 aktenkundig zu belehren.

Unterabschnitt 2
Weiterverarbeiten personenbezogener Daten

§ 29
Zulässigkeit des Weiterverarbeitens personenbezogener Daten

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, weiterverarbeiten, soweit dies zu vollzuglichen Zwecken erforderlich ist.

(2) Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, zu Zwecken, zu denen sie nicht erhoben wurden, weiterverarbeiten, soweit

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. die Voraussetzungen vorliegen, die ein Erheben bei Dritten zulassen; soweit andere Gefangene als diejenigen, deren Freiheitsentziehung ursprünglicher Anlass des Erhebens war, von dem anderweitigen Verarbeiten personenbezogene Daten betroffen sind, dürfen die personenbezogenen Daten nur zu einem anderen Zweck weiterverarbeitet werden, wenn diese Gefangenen zuvor unter Angabe des beabsichtigten Verarbeitens personenbezogener Daten angehört wurden und sich hieraus kein überwiegendes schutzwürdiges Interesse an einem Ausschluss des Verarbeitens der sie betreffenden personenbezogenen Daten ergeben hat,

3. dies dem gerichtlichen Rechtsschutz im Vollzug, dem Wahrnehmen von Aufsichts- und Kontrollbefugnissen, dem Automatisieren des Berichtswesens, der Rechnungsprüfung, dem Durchführen von Organisationsuntersuchungen oder statistischen Zwecken der Justizvollzugsbehörden dient und überwiegende schutzwürdige Interessen der betroffenen Person nicht entgegenstehen,

4. dies zum Abwehren sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht oder von Bestrebungen in der Bundesrepublik Deutschland, die durch das Anwenden von Gewalt oder darauf gerichtete Vorbereitungshandlungen

a) gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes sind,

b) ein ungesetzliches Beeinträchtigen der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben oder

c) auswärtige Belange der Bundesrepublik Deutschland gefährden,

5. dies zum Abwehren erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit,

6. dies zum Abwehren einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person,

7. dies zum Verhindern oder Verfolgen von Straftaten, zum Vollstrecken oder zum Vollziehen von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zum Verhindern, Verfolgen oder Ahnden von Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Anstalten gefährdet werden oder zum Vollstrecken von Bußgeldentscheidungen,

8. dies für Maßnahmen der Strafvollstreckung oder strafvollstreckungsrechtliche Entscheidungen hinsichtlich der betroffenen Person oder

9. dies für Maßnahmen der Schuldenregulierung und -tilgung, des Vorbereitens des Entlassens, des Entlassens, des Übergehens in die Freiheit, dem Wiedereingliedern, dem nachgehenden Betreuen oder dem freiwilligen Verbleiben der Gefangenen erforderlich ist oder

10. sich die Justizvollzugsbehörden zum Erfüllen der in § 1 genannten Zwecke einer öffentlichen Stelle bedienen, zu deren Aufgaben das elektronische Überwachen von Weisungen nach § 68b Abs. 1 Satz 1 Nr. 12 des Strafgesetzbuches gehört.

(3) Personenbezogene Daten besonderer Kategorien dürfen für Zwecke, zu denen sie nicht erhoben wurden, unter den Voraussetzungen von Absatz 2 weiterverarbeitet werden, soweit dies unbedingt erforderlich ist. Soweit personenbezogene Daten besonderer Kategorien einem Amts- oder Berufsgeheimnis unterliegen und von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Amts- oder Berufspflicht erlangt wurden, dürfen sie, soweit dieses Gesetz keine andere Regelung trifft, nur für Zwecke weiterverarbeitet werden, für die die verantwortliche Stelle sie erhalten hat.

(4) Personenbezogene Daten, die über Personen, die keine Gefangenen sind, erhoben wurden, dürfen nur unter den Voraussetzungen des Absatzes 1 oder des Absatzes 2 Nrn. 1 und 4 bis 6 oder unter den Voraussetzungen des § 37 oder zum Verhindern oder Verfolgen von Straftaten von erheblicher Bedeutung weiterverarbeitet werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 oder Absatz 2 weiterverarbeitet werden dürfen, weitere personenbezogene Daten der betroffenen Person

oder von einem Dritten so verbunden, dass ein Trennen, Anonymisieren oder Pseudonymisieren nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist das Weiterverarbeiten auch dieser personenbezogenen Daten zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder des Dritten an deren Geheimhalten offensichtlich überwiegen. Ein Weiterverarbeiten dieser personenbezogenen Daten ist unzulässig.

(6) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, des Datensicherns oder zum Sicherstellen des ordnungsgemäßen Betriebes mittels einer Datenverarbeitungsanlage weiterverarbeitet werden, dürfen für andere Zwecke nur weiterverarbeitet werden, wenn dies zum Abwehren einer erheblichen Gefahr für die öffentliche Sicherheit, insbesondere für Leben, Gesundheit oder Freiheit einer Person sowie zum Verfolgen von Straftaten erheblicher Bedeutung erforderlich ist.

§ 30
Weiterverarbeiten von Identifikationsmerkmalen; Gefangenenausweise

(1) Die nach § 22 erhobenen Identifikationsmerkmale des Gefangenen werden erfasst und zur Gefangenenpersonalakte des betroffenen Gefangenen genommen oder in personenbezogenen Dateisystemen gespeichert. Sie dürfen nur weiterverarbeitet werden

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

2. zum Identifizieren des Gefangenen, soweit dies für Zwecke des Fahndens und des Festnehmens des entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalten aufhaltenden Gefangenen erforderlich ist, oder

3. für die in § 29 Abs. 2 und § 37 genannten Zwecke.

(2) Das Weiterverarbeiten der nach § 22 Abs. 3 erhobenen Identifikationsmerkmale ist zulässig, soweit dies erforderlich ist zum

1. Überprüfen der Identität vor dem Verlassen der Anstalten oder

2. Verfolgen von Straftaten, bei denen der Verdacht besteht, dass sie bei Gelegenheit des Aufenthaltes in den Anstalten begangen wurden; die zum Verfolgen von Straftaten erforderlichen personenbezogenen Daten dürfen hierzu gegenüber den zuständigen Strafverfolgungsbehörden offengelegt werden; dies gilt auch für das Verfolgen von Ordnungswidrigkeiten nach § 115 des Gesetzes über Ordnungswidrigkeiten.

(3) Aus Gründen der Sicherheit und Ordnung der Anstalten ist der Gefangene verpflichtet, einen Ausweis mit sich zu führen, der mit einem Lichtbild zu versehen ist. Der Ausweis darf nur die zum Erreichen dieser Zwecke notwendigen personenbezogenen Daten enthalten. Er darf mit Einrichtungen versehen werden, die ein elektronisches Auslesen, auch mittels Funk- oder Digitaltechnik, ermöglichen. Auf diese Weise darf allein ein eindeutiges pseudonymisiertes Merkmal auslesbar sein.

§ 31
Weiterverarbeiten personenbezogener Daten nach optisch-elektronischem Beobachten und akustisch-elektronischem Überwachen

(1) Die mittels optisch-elektronischem Beobachten erhobenen personenbezogenen Daten dürfen weiterverarbeitet werden, soweit und solange dies zum Erreichen vollzuglicher Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zum Abwehren von Gefahren für die staatliche und öffentliche Sicherheit sowie zum Verfolgen von Straftaten erforderlich ist.

(2) Für das Weiterverarbeiten der mittels akustisch-elektronischer Einrichtungen erhobenen personenbezogenen Daten gilt Absatz 1 entsprechend. Darüber hinaus ist das Weiterverarbeiten zulässig, soweit und solange dies zum Offenlegen der personenbezogenen Daten gegenüber dem Gericht, das das inhaltliche Überwachen der Gespräche angeordnet hat, erforderlich ist.

(3) Die Maßnahmen nach Absatz 1 und 2 sind zu dokumentieren. Diese Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen und zu vernichten, wenn sie für diese Zwecke nicht mehr erforderlich ist.

(4) Personenbezogene Daten, die in den Kernbereich der privaten Lebensgestaltung fallen, dürfen mittels optisch-elektronischen Beobachtens oder akustisch-elektronischer Einrichtungen nicht erhoben werden. Sind solche personenbezogenen Daten versehentlich erhoben wurden, sind diese unverzüglich zu löschen und zu vernichten. Erkenntnisse zu diesen personenbezogenen Daten dürfen nicht weiterverarbeitet werden. Die Tatsachen ihres Erhebens, ihres Löschens und ihres Vernichtens sind zu dokumentieren. Nicht erfasst sind Gespräche über Straftaten oder Gespräche, durch die Straftaten begangen werden.

§ 32
Weiterverarbeiten personenbezogener Daten nach Beaufsichtigen, Überwachen und Kontrollieren

(1) Die während des Beaufsichtigens oder des Überwachens der Besuche, des Überwachens der Telekommunikation, des Kontrollierens und des Überwachens des Schriftwechsels oder des Kontrollierens des Inhalts von Paketen bekannt gewordenen personenbezogenen Daten sind in Akten und Dateisystemen sowie beim Offenlegen gegenüber anderen Stellen eindeutig als solche zu kennzeichnen. Sie dürfen nur weiterverarbeitet werden

1. für das Behandeln und Betreuen des Gefangenen,

2. zum Aufrechterhalten, Wiederherstellen und Durchsetzen der Sicherheit oder Ordnung der Anstalten oder

3. für die in § 29 Abs. 2 und § 37 genannten Zwecke.

(2) Die nach Absatz 1 Satz 1 zulässig bekannt gewordenen personenbezogenen Daten dürfen über die in Absatz 1 Satz 2 bezeichneten Zwecke hinaus im Vollzug einer Freiheitsentziehung nach § 1 Nrn. 1, 7 und 8 auch weiterverarbeitet werden zum

1. Abwehren von Gefährdungen des Zweckes des Vollzuges der Untersuchungshaft oder

2. Umsetzen von Anordnungen nach § 119 der Strafprozessordnung.

(3) Soweit die in den Absätzen 1 und 2 bezeichneten personenbezogenen Daten dem Kernbereich der privaten Lebensgestaltung unterfallen, sind sie unverzüglich zu löschen und zu vernichten. Erkenntnisse über solche personenbezogenen Daten dürfen nicht weiterverarbeitet werden. Die Tatsache ihres Erhebens, ihres Löschens und ihres Vernichtens sind zu dokumentieren. Nicht erfasst sind Gespräche über Straftaten oder Gespräche, durch die Straftaten begangen werden.

§ 33
Weiterverarbeiten personenbezogener Daten nach dem Auslesen von Datenspeichern

Die nach § 28 erhobenen personenbezogenen Daten dürfen zu den Zwecken, zu denen sie erhoben wurden, weiterverarbeitet werden, soweit dies erforderlich ist. Aus anderen Gründen ist das Weiterverarbeiten nur zulässig, soweit dies für das Erreichen der in § 29 Abs. 2 oder § 37 genannten Zwecke erforderlich ist und schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

Unterabschnitt 3
Offenlegen personenbezogener Daten durch Übermitteln oder eine andere Art des Bereitstellens; Abfrage

§ 34
Offenlegen personenbezogener Daten gegenüber öffentlichen Stellen

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, gegenüber öffentlichen Stellen offenlegen, soweit dies zu vollzuglichen Zwecken erforderlich ist. Für Zwecke, zu denen sie nicht erhoben wurden, dürfen sie offengelegt werden, soweit

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. dies erforderlich ist für

   a) das Erfüllen der Aufgaben der Gerichtshilfe, der Jugendgerichtshilfe, der Bewährungsaufsicht, der Führungsaufsicht oder forensischer Ambulanzen,

   b) Entscheidungen in Gnadensachen,

   c) Statistiken der Rechtspflege,

   d) das Erfüllen von Aufgaben, die den für Sozialleistungen zuständigen Leistungsträgern durch Rechtsvorschrift übertragen worden sind,

e) das Einleiten von Hilfsmaßnahmen für Angehörige nach § 11 Abs. 1 Nr. 1 des Strafgesetzbuches der Gefangenen,

f) dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit dem Aufnehmen und Entlassen von Soldaten,

g) asyl- oder ausländerrechtliche Maßnahmen,

h) das Erfüllen der Aufgaben der Jugendämter,

i) das Durchführen des Besteuerns oder

j) das Erreichen der in § 29 Abs. 2 Nrn. 1 und 3 bis 10 oder § 37 genannten Zwecke.

Im Vollzug einer Freiheitsentziehung nach § 1 Nrn. 1, 7 und 8 werden personenbezogene Daten nach Satz 2 Nr. 2 nicht offengelegt, wenn der Gefangene unter Berücksichtigung der Art der Information und seiner Rechtsstellung als Untersuchungsgefangener hieran ein schutzwürdiges Interesse hat.

(2) Personenbezogene Daten besonderer Kategorien dürfen gegenüber öffentlichen Stellen unter den Voraussetzungen des § 29 Abs. 3 oder § 37 und, soweit dies unbedingt erforderlich ist, zum Erreichen vollzuglicher Zwecke und gegenüber forensischen Ambulanzen zum Zweck des Behandelns und Betreuens, des Schuldenregulierens und -tilgens, des Vorbereitens des Entlassens, des Übergehens in die Freiheit, des Entlassens, des Wiedereingliederns, des nachgehenden Betreuens oder des freiwilligen Verbleibens des Gefangenen, offengelegt werden.

(3) Personenbezogene Daten, die über Personen, die keine Gefangenen sind, erhoben wurden, dürfen nur unter den Voraussetzungen des Absatzes 1 oder für die in § 29 Abs. 2 Nrn. 4 bis 6 oder § 37 aufgeführten Zwecke sowie zum Verhindern oder Verfolgen von Straftaten von erheblicher Bedeutung offengelegt werden. Dies gilt auch, soweit es für Zwecke des Fahndens und des Festnehmens eines entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen erforderlich ist.

(4) Sind mit personenbezogenen Daten, die offengelegt werden dürfen, weitere personenbezogene Daten der betroffenen Person oder eines Dritten so verbunden, dass ein Trennen, Anonymisieren oder Pseudonymisieren nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist das Offenlegen auch dieser personenbezogenen Daten zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder des Dritten an deren Geheimhalten offensichtlich überwiegen. In diesen Fällen ist ein Weiterverarbeiten der personenbezogenen Daten durch den Empfänger unzulässig.

(5) Für personenbezogener Daten, die im Rahmen einer Maßnahme zum elektronischen Aufenthaltsüberwachen erhoben wurden, gilt § 463a Abs. 4 der Strafprozessordnung entsprechend mit der Maßgabe, dass

1. diese personenbezogenen Daten der betroffenen Person nur offengelegt werden, soweit dies erforderlich ist zum

a) Feststellen oder Ahnden eines Verstoßes gegen eine im Rahmen einer Maßnahme zum elektronischen Aufenthaltsüberwachen erteilten Weisung,

b) Wiederergreifen des Gefangenen,

c) Abwehren einer erheblichen gegenwärtigen Gefahr für das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder sexuelle Selbstbestimmung einer anderen Person oder

d) Verfolgen einer Straftat und

2. sich die Justizvollzugsbehörden zum Verarbeiten der personenbezogenen Daten einer öffentlichen Stelle bedienen, zu deren Aufgaben das elektronische Überwachen von Weisungen nach § 68b Abs. 1 Satz 1 Nr. 12 des Strafgesetzbuches gehört.

§ 35
Offenlegen personenbezogener Daten gegenüber nicht öffentlichen Stellen

(1) Gegenüber nicht öffentlichen Stellen dürfen die Justizvollzugsbehörden zulässig erhobene personenbezogene Daten für Zwecke, zu denen sie erhoben wurden, offenlegen, soweit

1. sich die Justizvollzugsbehörden zum Erfüllen oder Unterstützen bei dem Erreichen einzelner vollzuglicher Zwecke in zulässiger Weise dem Mitwirken nicht öffentlicher Stellen bedienen und diese Stellen ohne das Weiterverarbeiten, der von den Justizvollzugsbehörden offengelegten personenbezogenen Daten, ihre Tätigkeit nicht oder nur unter wesentlich erschwerten Bedingungen ausüben könnten,

2. es dazu erforderlich ist, den Gefangenen

a) den Besuch von Behandlungs-, Beratungs-, Trainings- und Bildungsmaßnahmen sowie sowie das Beschäftigen innerhalb und außerhalb von Anstalten,

b) das Inanspruchnehmen von Leistungen der Berufsgeheimnisträger und deren Hilfspersonen,

c) den Einkauf,

d) das Inanspruchnehmen von Telekommunikations- und Mediendienstleistungen,

e) das Inanspruchnehmen von Maßnahmen des Vorbereitens des Entlassens, des Übergehens in die Freiheit, des Schuldenregulierens und -tilgens, des Entlassens, des Wiedereingliederns, des nachgehenden Betreuens oder des freiwilligen Verbleibens

zu ermöglichen.

(2) Nicht öffentlichen Stellen gegenüber dürfen Justizvollzugsbehörden zulässig erhobene personenbezogene Daten für Zwecke, zu denen sie nicht erhoben wurden, nur unter den Voraussetzungen des § 29 Abs. 2 Nrn. 1 und 3 bis 10 oder § 37 offenlegen.

(3) Personenbezogene Daten besonderer Kategorien dürfen nicht öffentlichen Stellen gegenüber nur unter den Voraussetzungen des § 29 Abs. 3 oder § 37 oder, wenn dies zum Erreichen vollzuglicher Zwecke unbedingt erforderlich ist, offengelegt werden.

(4) § 34 Abs. 3 bis 5 gilt entsprechend.

§ 36
Weitere Bedingungen beim Offenlegen personenbezogener Daten gegenüber Behörden mit Sicherheitsaufgaben

(1) Das Offenlegen personenbezogener Daten gegenüber Behörden mit Sicherheitsaufgaben zum Zwecke des Verhütens und Abwehrens von Gefahren, zum Verhindern oder Verfolgen von Ordnungswidrigkeiten, zum Verhindern oder Verfolgen von Straftaten oder zu den in § 29 Abs. 2 Nr. 4 genannten Zwecken ist zulässig, wenn

1. sich im Einzelfall konkrete Ansätze ergeben

   a) zum Verhüten, Aufdecken oder Verfolgen von Straftaten oder Ordnungswidrigkeiten oder

   b) zum Abwehren von in einem überschaubaren Zeitraum drohenden Gefahren und

2. mindestens

   a) der Schutz solch bedeutsamer Rechtsgüter oder

   b) das Verhüten, Aufdecken oder Verfolgen solch schwerwiegender Straftaten oder Ordnungswidrigkeiten verwirklicht werden soll, dass ein im Vergleich zum Erheben personenbezogener Daten gleichwertiger Rechtsgüterschutz sichergestellt ist.

(2) Gleiches gilt für das Erheben personenbezogener Daten durch die Justizvollzugsbehörden über Gefangene, anstaltsfremde oder sonstige Personen bei den Behörden mit Sicherheitsaufgaben zum Zwecke des Verhütens und Abwehrens von Gefahren, zum Verhindern oder Verfolgen von Ordnungswidrigkeiten oder zum Verhindern oder Verfolgen von Straftaten.

(3) Für das Offenlegen und das Erheben personenbezogener Daten, die durch das verdeckte Einsetzen technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, gilt Absatz 1 Nr. 1 Buchst. 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 Erhalten im öffentlichen Interesse geboten ist, vorliegen muss und

2. bei personenbezogenen Daten, die durch verdecktes Eingreifen 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 Schäden an Leib, Leben oder Freiheit einer Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, eintreten.

(4) Die Befugnis, personenbezogener Daten zum Zwecke des Identifizierens von Personen nach diesem Gesetz weiterzuverarbeiten und offenzulegen bleibt unberührt.

§ 37
Offenlegen personenbezogener Daten im Rahmen von 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, gegenüber den Polizeibehörden des Bundes und der Länder offenlegen, sofern

1. tatsächliche Anhaltspunkte für die fortdauernde Gefährlichkeit des Gefangenen für die Allgemeinheit vorliegen,

2. das Entlassen des Gefangenen aller Voraussicht nach in einem Zeitraum von nicht mehr als einem Jahr bevorsteht und

3. dies zum vorbeugenden Bekämpfen von Straftaten von erheblicher Bedeutung erforderlich ist.

Fallkonferenzen dürfen auch zum Vorbereiten des Ausführens, Vorführens, Ausantwortens, Überstellens und Verlegens, bei tatsächlichen Anhaltspunkten für eine Gefahr des Entweichens, von Gewalttätigkeiten gegen Personen oder Sachen von bedeutendem Wert, deren Erhalten im öffentlichen Interesse geboten ist, und des Selbstverletzens oder Selbsttötens des Gefangenen stattfinden. An den Fallkonferenzen nach Satz 1 sollen die Bewährungshilfe und die Führungsaufsichtsstellen beteiligt werden. Im Rahmen der vorgenannten Fallkonferenzen dürfen personenbezogene Daten, einschließlich solcher besonderer Kategorien, durch die Justizvollzugsbehörden bei den Polizeibehörden des Bundes und der Länder auch angefragt, erhoben, erfasst und abgeglichen werden.

(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 gegen-

über den Verfassungsschutzbehörden des Bundes und der Länder offenlegen, sofern

1. bestimmte Tatsachen den Verdacht für Tätigkeiten oder Bestrebungen nach § 29 Abs. 2 Nr. 4 begründen,

2. eine damit im Zusammenhang stehende Gefahr für die Sicherheit der Anstalten oder das Erreichen des Vollzugsziels in einem überschaubaren Zeitraum einzutreten droht und

3. dies zum Verhüten der in Nummer 2 genannten Gefahren unbedingt erforderlich ist.

An den Fallkonferenzen sollen die Bewährungshilfe und die Führungsaufsichtsstellen beteiligt werden, sofern das Entlassen des Gefangenen in voraussichtlich nicht mehr als einem Jahr bevorsteht. Im Rahmen der vorgenannten Fallkonferenzen dürfen personenbezogene Daten, einschließlich solcher besonderer Kategorien, durch die Justizvollzugsbehörden bei den Verfassungsschutzbehörden des Bundes und der Länder auch angefragt, erhoben, erfasst und abgeglichen werden.

(3) Fallkonferenzen dürfen zwischen den Justizvollzugsbehörden, den Polizeibehörden des Bundes und der Länder sowie 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 Erhalten im öffentlichen Interesse geboten ist, begründen,

2. bestimmte Tatsachen den Verdacht für Tätigkeiten oder Bestrebungen nach § 29 Abs. 2 Nr. 4 begründen und

3. dies zum Abwehren der in Nummer 1 genannten Gefahren unbedingt erforderlich ist.

Absatz 2 Satz 2 gilt entsprechend. Im Rahmen der vorgenannten Fallkonferenzen dürfen personenbezogene Daten, einschließlich solcher besonderer Kategorien, durch die Justizvollzugsbehörden bei den Polizeibehörden des Bundes und der Länder sowie den Verfassungsschutzbehörden des Bundes und der Länder auch angefragt, erhoben, erfasst und abgeglichen werden.

(4) Die Ergebnisse der durchgeführten Fallkonferenzen sind zu dokumentieren.

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

§ 38
Offenlegen von Identifikationsmerkmalen

Nach § 22 erhobene personenbezogene Daten dürfen offengelegt werden gegenüber:

1. den Vollstreckungs- und Strafverfolgungsbehörden, soweit dies für Zwecke des Fahndens nach und Festnehmen des entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalten aufhaltenden Gefangenen erforderlich ist,

2. den Polizeibehörden des Bundes und der Länder, soweit dies zum Abwehren einer gegenwärtigen innerhalb der Anstalten drohenden Gefahr für erhebliche Sachwerte oder für Leib, Leben oder Freiheit einer Person erforderlich ist,

3. den in § 22 und § 37 genannten öffentlichen Stellen unter den dort genannten Voraussetzungen

und

4. anderen öffentlichen Stellen auf deren Ersuchen, soweit die betroffene Person verpflichtet wäre, ein unmittelbares Erheben der ersuchten personenbezogenen Daten durch den Empfänger zu dulden oder an dem Erheben mitzuwirken; die ersuchende Stelle hat in ihrem Ersuchen die Rechtsgrundlage der Mitwirkungs- oder Duldungspflicht mitzuteilen; beruht diese Pflicht auf einer Regelung gegenüber der betroffenen Person im Einzelfall, so weist die ersuchende Stelle zugleich nach, dass eine entsprechende Regelung ergangen und vollziehbar ist

oder wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt.

§ 39
Offenlegen personenbezogener Daten durch das Mitteilen von Haftverhältnissen

(1) Öffentlichen und nicht öffentlichen Stellen dürfen die Justizvollzugsbehörden auf schriftlichen Antrag gegenüber offenlegen, ob und in welcher Anstalt sich eine Person in Haft befindet sowie ob und wann ihre Entlassen voraussichtlich innerhalb eines Jahres bevorsteht, soweit

1. das Offenlegen zum Erfüllen der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben erforderlich ist oder

2. von nicht öffentlichen Stellen ein berechtigtes Interesse glaubhaft dargelegt wird und der Gefangene kein schutzwürdiges Interesse am Ausschluss des Offenlegens hat.

(2) Zuständigen öffentlichen Stellen können über Absatz 1 hinaus auf schriftlichen Antrag Auskünfte über die Entlassungsadresse oder die Vermögensverhältnisse des Gefangenen erteilt werden, wenn dies zum Feststellen, Durchsetzen oder Vollstrecken von Forderungen erforderlich ist.

(3) Im Vollzug einer Freiheitsentziehung nach § 1 Nrn. 1, 7 und 8 besteht die zulässige Auskunft nach den Absätzen 1 und 2 in der Angabe, ob sich eine Person in der Anstalt in Untersuchungshaft oder wegen einer anderen Freiheitsentziehung befindet. Eine Auskunft unterbleibt, wenn der Gefangene unter Berücksichtigung der Art der Information und seiner Rechtsstellung als Untersuchungsgefangener hieran ein schutzwürdiges Interesse hat.

(4) Der Gefangene wird vor dem Offenlegen gehört, soweit dadurch nicht das Verfolgen des Interesses des Antragstellers vereitelt oder wesentlich erschwert wird und eine Abwägung ergibt, dass das Interesse des Antragstellers das Interesse des Gefangenen am vorherigen Anhören überwiegt. Ist die Anhörung unterblieben, wird der betroffene Gefangene über das Offenlegen durch die Justizvollzugsbehörde nachträglich unterrichtet.

(5) Beim Anhören und Unterrichten des Gefangenen ist auf die berechtigten Interessen des nicht öffentlichen Empfängers am Geheimhalten seiner Lebensumstände in besonderer Weise Rücksicht zu nehmen. Die Anschrift des Empfängers darf dem Gefangenen gegenüber nicht offengelegt werden.

(6) Die Auskünfte sind in der Gefangenenpersonalakte des betroffenen Gefangenen zu dokumentieren.

§ 40
Offenlegen personenbezogener Daten durch das Erteilen von Auskünften an Opfer

(1) Dem Opfer einer Straftat wird auf schriftlichen Antrag Auskunft über die Inhaftierung und deren Beendigung, das Gewähren von Lockerungen oder anderen vollzugsöffnender Maßnahmen, opferbezogene Weisungen und das Unterbringen im offenen Vollzug erteilt, wenn es ein berechtigtes Interesse darlegt und kein überwiegendes schutzwürdiges Interesse des Gefangenen am Ausschluss der Auskunft vorliegt. Das Darlegen eines berechtigten Interesses ist nicht erforderlich, wenn der Antragsteller Opfer einer Straftat nach

1. den §§ 174 bis 174c, 176 bis 178, 180, 180a, 181 bis 182, 184 i und 184j des Strafgesetzbuches,

2. den §§ 211 und 212 des Strafgesetzbuches,

3. den §§ 221, 223 bis 226 und 340 des Strafgesetzbuches,

4. den §§ 232 bis 238, § 239 Abs. 3 und den §§ 239a, 239b und 240 Abs. 4 des Strafgesetzbuches oder

5. § 4 des Gewaltschutzgesetzes ist.

Der Nachweis des Zulassens zur Nebenklage ersetzt in der Regel auch das Darlegen des berechtigten Interesses. Dies gilt nicht, wenn dem Gefangenen erneut Lockerungen oder andere vollzugsöffnende Maßnahmen gewährt werden.

(2) Besteht aufgrund des Entweichens oder des Fliehens eines Gefangenen eine Gefahr für Leib oder Leben, ergeht eine Auskunft nach Absatz 1 auch ohne Antrag.

(3) Opfern und anderen aus der Straftat Anspruchsberechtigten können auf schriftlichen Antrag Auskünfte über die Entlassungsadresse oder die Vermögensverhältnisse des Gefangenen erteilt werden, wenn das Erteilen der Auskunft zum Feststellen, Durchsetzen oder Vollstrecken von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist.

(4) Besteht Anlass zu der Besorgnis, dass das Offenlegen von Lebensumständen des Antragstellers dessen Leib oder Leben gefährdet, unterbleibt das Offenlegen gegenüber dem Gefangenen. Darüber hinaus darf dem Gefangenen die Anschrift des Antragstellers nur offengelegt werden, wenn dieser ausdrücklich in das Offenlegen einwilligt.

(5) Im Vollzug der Untersuchungshaft bleibt § 406d der Strafprozessordnung unberührt. Die Justizvollzugsbehörden dürfen Auskünfte nach § 406d der Strafprozessordnung im Einvernehmen mit der Staatsanwaltschaft oder dem nach § 126 der Strafprozessordnung zuständigen Gericht auch unmittelbar erteilen.

(6) Die Auskünfte sind in der Gefangenenpersonalakte des betroffenen Gefangenen zu dokumentieren.

§ 41
Offenlegen personenbezogener Daten durch das Überlassen von Akten und Dateisystemen

(1) Soweit personenbezogene Daten offengelegt werden dürfen, können auch Akten und Dateisysteme den folgenden Stellen überlassen oder beim elektronischen Führen von Akten auch in Form von Duplikaten bereitgestellt werden:

1. den Justizvollzugsbehörden,

2. den Stellen der Gerichtshilfe, Jugendgerichtshilfe, Bewährungsaufsicht oder Führungsaufsicht,

3. den für strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen zuständigen Gerichten,

4. den Strafvollstreckungs- und Strafverfolgungsbehörden,

5. von Justizvollzugs-, Strafverfolgungs- oder Strafvollstreckungsbehörden oder von einem Gericht mit dem Erstellen von Gutachten beauftragten Stellen und

6. den sonstigen öffentlichen Stellen, wenn das Erteilen einer Auskunft entweder einen unvertretbaren Aufwand erfordern würde oder nach Darlegen der die Akteneinsicht begehrenden Stelle das Erteilen einer Auskunft für das Erfüllen ihrer Aufgaben nicht ausreicht.

(2) Sind mit offengelegten personenbezogenen Daten, weitere personenbezogene Daten der betroffenen Person oder eines Dritten so verbunden, dass ein Trennen, Anonymisieren oder Pseudonymisieren nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist das Offenlegen dieser personenbezogenen Daten nach Absatz 1 zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder des Dritten an deren Geheimhalten offensichtlich überwiegen. In diesen Fällen ist ein Weiterverarbeiten der personenbezogenen Daten durch den Empfänger unzulässig.

§ 42
Offenlegen personenbezogener Daten durch das Einsehen von Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern

Die Justizvollzugsbehörden dürfen gegenüber den Mitgliedern einer Delegation des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe und den Mitgliedern einer durch das Übereinkommen der Vereinten Nationen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe legitimierten Stelle während des Besuches in der Anstalt personenbezogene Daten des Gefangenen durch das Einsehen von Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern offenlegen, soweit dies zum Wahrnehmen der Aufgaben des Ausschusses oder der Stelle unbedingt erforderlich ist.

§ 43
Offenlegen personenbezogener Daten gegenüber wissenschaftlichen Einrichtungen

(1) Die Justizvollzugsbehörden dürfen gegenüber Hochschulen, anderen Einrichtungen und öffentlichen Stellen, die wissenschaftliche Forschung betreiben, personenbezogene Daten offenlegen, soweit

1. dies für das Durchführen wissenschaftlicher Forschungsarbeiten erforderlich ist,

2. das Verarbeiten anonymisierter oder pseudonymisierter personenbezogener Daten zu diesem Zweck nicht möglich oder das Anonymisieren oder das Pseudonymisieren mit einem unverhältnismäßigen Aufwand verbunden ist und

3. das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse der betroffenen Personen an dem Ausschluss des Offenlegens erheblich überwiegt.

Beim Abwägen nach Satz 1 Nr. 3 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(2) Das Offenlegen personenbezogener Daten erfolgt durch das Erteilen von Auskünften, wenn dadurch der Zweck der Forschungsarbeit erreicht werden kann und das Erteilen der Auskunft keinen unverhältnismäßigen Aufwand erfordert. Andernfalls können auch Akten und Dateisysteme eingesehen oder übersandt werden.

(3) Das Offenlegen personenbezogener Daten erfolgt nur gegenüber solchen Personen, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zum Geheimhalten verpflichtet worden sind. § 1 Abs. 2, 3 und 4 Nr. 2 des Verpflichtungsgesetzes findet auf das Verpflichten zum Geheimhalten entsprechende Anwendung.

(4) Die offengelegten personenbezogenen Daten dürfen nur für die Forschungsarbeit verwendet werden, für die sie offengelegten worden sind. Das Weiterverarbeiten dieser personenbezogenen Daten für andere Forschungsarbeiten oder ihr Offenle-

gen durch den Empfänger richtet sich nach den Absätzen 1 bis 3. Die Stelle, die das Offenlegen angeordnet hat, muss dazu ihr Einverständnis erteilen.

(5) Die personenbezogenen Daten sind gegen das Kenntnisnehmen durch Unbefugte zu schützen. Die wissenschaftliche Forschung betreibende Stelle hat dafür zu sorgen, dass das Verarbeiten der personenbezogenen Daten räumlich und organisatorisch getrennt von dem Erfüllen solcher Verwaltungsaufgaben oder Geschäftszwecke erfolgt, für die diese personenbezogenen Daten gleichfalls von Bedeutung sein können. Erfolgt das Offenlegen personenbezogener Daten auf elektronischem Weg, ist ein sicherer Übertragungsweg zu gewährleisten.

(6) Sobald der Forschungszweck es erlaubt, sind die personenbezogenen Daten zu anonymisieren. Solange dies nicht möglich ist, sind die Merkmale gesondert aufzubewahren, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren betroffenen Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(7) Empfänger dürfen die nach den Absätzen 1 bis 3 erhaltenen personenbezogenen Daten nur veröffentlichen, wenn dies für das Darstellen von Forschungsergebnissen über Ereignisse der Zeitgeschichte unbedingt erforderlich ist und die Stelle, die die personenbezogenen Daten offengelegt hat, ihr Einverständnis zum Veröffentlichen dieser personenbezogenen Daten erteilt hat.

§ 44
Verantwortung und Verfahren beim Offenlegen personenbezogener Daten

(1) Die Verantwortung für die Zulässigkeit des Offenlegens personenbezogener Daten tragen die Justizvollzugsbehörden. Erfolgt das Offenlegen personenbezogener Daten auf Ersuchen einer öffentlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüft die Justizvollzugsbehörde nur, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt und die Bestimmungen dieses Gesetzes nicht entgegenstehen, es sei denn, dass besonderer Anlass zum Prüfen der Zulässigkeit des Offenlegens personenbezogener Daten besteht.

(2) Die Justizvollzugsbehörden stellen sicher, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht offengelegt werden. Zu diesem Zweck überprüfen sie im Vorfeld des Offenlegens, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der personenbezogenen Daten. Bei jedem Offenlegen personenbezogener Daten fügen sie zudem, soweit dies möglich und angemessen ist, Informationen bei, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der personenbezogenen Daten sowie deren Aktualität zu beurteilen.

(3) Gelten für das Verarbeiten personenbezogener Daten besondere Bedingungen, so weist die Justizvollzugsbehörde den Empfänger personenbezogener Daten auf diese Bedingungen und die Pflicht zu ihrem Beachten hin. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend gekennzeichnet oder markiert werden.

(4) Die Justizvollzugsbehörden dürfen auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des dritten Teils des Vertrages über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für ein entsprechendes innerstaatliches Offenlegen personenbezogener Daten gilt.

(5) Personenbezogene Daten, die gegenüber nicht öffentlichen Stellen offengelegt werden sollen, sind in der Regel vorher zu pseudonymisieren. Dabei ist die Gefangenenbuchnummer als Pseudonym zu verwenden, wenn nicht besondere Gründe entgegenstehen. Dies gilt auch bei der Inanspruchnahme von Telekommunikations- und Mediendienstleistungen von Dritten. Abweichend von Satz 1 und 2 ist ein Pseudonymisieren nicht vorzunehmen, wenn zum Erfüllen des zugrundeliegenden Zweckes des Offenlegens personenbezogener Daten, die Kenntnis der Identität der betroffenen Person erforderlich ist.

(6) Empfänger personenbezogener Daten dürfen diese nur zu dem Zweck weiterverarbeiten, zu dessen Erfüllen sie sie erhalten haben. Für andere Zwecke dürfen sie diese personenbezogenen Daten nur weiterverarbeiten, soweit sie ihnen auch für diese Zwecke hätten überlassen werden dürfen und wenn, im Fall des Offenlegens personenbezogener Daten an eine nicht öffentliche Stelle, die Justizvollzugsbehörde zugestimmt hat. Die Justizvollzugsbehörde weist den Empfänger auf die Zweckbindung nach Satz und 1 und 2 hin.

Unterabschnitt 4
Offenlegen personenbezogener Daten durch Übermitteln an Drittstaaten und an internationale Organisationen

§ 45
Allgemeine Voraussetzungen

(1) Das Offenlegen personenbezogener Daten gegenüber Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen hierfür geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für das Erreichen vollzuglicher Zwecke zuständig ist und

2. die Europäische Kommission gemäß Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

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

(3) Wenn personenbezogene Daten, die von Stellen aus einem anderen Mitgliedstaat der Europäischen Union offengelegt und zur Verfügung gestellt wurden, nach Absatz 1 offengelegt werden sollen, muss dies zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Ohne vorherige Genehmigung ist das Offenlegen nur dann zulässig, wenn es erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 wird die Stelle des anderen Mitgliedstaates, die für das Erteilen der Genehmigung zuständig gewesen wäre, unverzüglich über das Offenlegen unterrichtet.

(4) Die Justizvollzugsbehörden, die personenbezogene Daten nach Absatz 1 offenlegen, stellen durch geeignete Maßnahmen sicher, dass Empfänger die erhaltenen personenbezogenen Daten nur dann gegenüber anderen Drittstaaten oder anderen internationale Organisationen offenlegen, wenn die Justizvollzugsbehörden dies zuvor genehmigt haben. Bei der Entscheidung über das Erteilen der Genehmigung berücksichtigen die Justizvollzugsbehörden alle maßgeblichen Faktoren, insbesondere die Schwere der Straftat, den Zweck des ursprünglichen Offenlegens und das in dem Drittstaat oder der internationalen Organisation, gegenüber dem oder der die personenbezogenen Daten auch offengelegt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch ein direktes Offenlegen gegenüber dem anderen Drittstaat oder der anderen internationalen Organisation zulässig wäre.

§ 46
Offenlegen personenbezogener Daten bei geeigneten Garantien

(1) Liegt entgegen § 45 Abs. 1 Nr. 2 kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor, ist das Offenlegen personenbezogener Daten bei Vorliegen der weiteren Voraussetzungen des § 45 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

2. die Justizvollzugsbehörden nach dem Beurteilen aller Umstände, die bei dem Offenlegen personenbezogener Daten eine Rolle spielen, zu der Auffassung gelangt sind, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Die Justizvollzugsbehörden dokumentieren das Offenlegen nach Absatz 1 Nr. 2. Die Dokumentation enthält den Zeitpunkt des Offenlegens, die Identität des Empfängers, den Grund des Offenlegens und die offengelegten personenbezogenen Daten. Die Dokumentation ist dem Landesbeauftragten für den Datenschutz auf Anfordern zur Verfügung zu stellen.

(3) Die Justizvollzugsbehörden unterrichten den Landesbeauftragten für den Datenschutz zumindest jährlich über das Offenlegen, das aufgrund einer Beurteilung nach Absatz 1 Nr. 2 erfolgt ist. Hierzu dürfen sie die Empfänger und die Zwecke des Offenlegens angemessen kategorisieren.

§ 47
Offenlegen personenbezogener Daten ohne geeignete Garantien

(1) Liegt entgegen § 45 Abs. 1 Nr. 2 kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 46 Abs. 1 vor, ist das Offenlegen personenbezogener Daten bei Vorliegen der übrigen Voraussetzungen des § 45 auch dann zulässig, wenn das Offenlegen erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,

2. zum Wahren berechtigter Interessen der betroffenen Person,

3. zum Abwehren einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,

4. im Einzelfall für vollzugliche Zwecke oder

5. im Einzelfall zum Geltendmachen, Ausüben oder Verteidigen von Rechtsansprüchen im Zusammenhang mit vollzuglichen Zwecken oder der Strafvollstreckung.

(2) Die Justizvollzugsbehörden sehen von dem Offenlegen personenbezogener Daten nach Absatz 1 ab, wenn die Grundrechte der betroffenen Person das öffentliche Interesse überwiegen.

(3) Für das Offenlegen personenbezogener Daten nach Absatz 1 gilt § 46 Abs. 2 entsprechend.

§ 48
Sonstiges Offenlegen personenbezogener Daten gegenüber Drittstaaten

(1) Justizvollzugsbehörden dürfen bei Vorliegen der übrigen für das Offenlegen gegenüber Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar gegenüber nicht in § 45 Abs. 1 Nr. 1 genannten Stellen in Drittstaaten offenlegen, wenn dies für vollzugliche Zwecke unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse überwiegen,

2. das Offenlegen personenbezogener Daten an die in § 45 Abs. 1 Nr. 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere, weil sie nicht rechtzeitig durchgeführt werden kann, und

3. die Justizvollzugsbehörden dem Empfänger die Zwecke des Verarbeitens personenbezogener Daten mitteilen und ihn darauf hinweisen, dass die erhaltenen personenbezogenen Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihr Verarbeiten für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 unterrichten die Justizvollzugsbehörden die in § 45 Abs. 1 Nr. 1 genannten Stellen unverzüglich über das Offenlegen personenbezogener Daten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für das Offenlegen personenbezogener Daten nach Absatz 1 gilt § 46 Abs. 2 und 3 entsprechend.

(4) Beim Offenlegen personenbezogener Daten nach Absatz 1 verpflichten die Justizvollzugsbehörden den Empfänger, die erhaltenen personenbezogenen Daten ohne ihre Zustimmung nur für den Zweck zu verarbeiten, für den er sie erhalten hat.

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

Unterabschnitt 5
Besondere Bedingungen

§ 49
Auftragsverarbeiter

(1) Werden personenbezogene Daten im Auftrag einer Justizvollzugsbehörde durch andere Personen oder Stellen verarbeitet, sorgt die Justizvollzugsbehörde für das Einhalten der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz. Die Rechte der betroffenen Person auf Auskunft, Berichtigen, Löschen und Vernichten, Einschränken des Verarbeitens personenbezogener Daten und auf Schadensersatz, sind in diesem Fall gegenüber der beauftragenden Justizvollzugsbehörde geltend zu machen.

(2) Die Justizvollzugsbehörden dürfen nur solche Auftragsverarbeiter mit dem Verarbeiten personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass das Verarbeiten personenbezogener Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(3) Ein Auftragsverarbeiter darf ohne vorherige schriftliche oder in einem elektronischen Format erteilte Genehmigung einer Justizvollzugsbehörde keine weiteren Auftragsverarbeiter hinzuziehen. Hat eine Justizvollzugsbehörde einem Auftragsverarbeiter eine Genehmigung zum Hinzuziehen weiterer Auftragsverarbeiter oder Ersetzen durch diese erteilt, informiert der Auftragsverarbeiter die Justizvollzugsbehörde über jedes beabsichtigte Hinzuziehen oder Ersetzen weiterer Auftragsverarbeiter und jedes Ändern der hierzu von der Justizvollzugsbehörde erteilten Genehmigung. Die Justizvollzugsbehörde kann Einwände erheben und dem Hinzuziehen oder Ersetzen widersprechen oder dies untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so legt er diesem dieselben Verpflichtungen aus seinem Vertrag mit der Justizvollzugsbehörde nach Absatz 5 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 der Justizvollzugsbehörde für das Einhalten der Pflichten des weiteren Auftragsverarbeiters.

(5) Das Verarbeiten personenbezogener Daten durch einen Auftragsverarbeiter erfolgt nur auf der Grundlage eines Vertrages oder eines anderen Rechtsinstrumentes, der oder das den Auftragsverarbeiter an die Justizvollzugsbehörde bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck des Verarbeitens personenbezogener Daten, 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 Justizvollzugsbehörde handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er die Justizvollzugsbehörde unverzüglich zu informieren;

2. gewährleistet, dass die zum Verarbeiten der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

3. die Justizvollzugsbehörde mit geeigneten Mitteln dabei unterstützt, das Einhalten der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss des Erbringens der Verarbeitungsleistungen nach Wahl der Justizvollzugsbehörde zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zum weiteren Speichern der personenbezogenen Daten besteht;

5. der Justizvollzugsbehörde alle erforderlichen Informationen, insbesondere das nach diesem Gesetz vorzunehmende Protokollieren, zum Nachweis des Einhaltens seiner Pflichten zur Verfügung stellt;

6. Überprüfungen, die von der Justizvollzugsbehörde oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;

7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für das Inanspruchnehmen der Dienste eines weiteren Auftragsverarbeiters einhält;

8. alle erforderlichen technischen und organisatorischen Maßnahmen ergreift und

9. unter Berücksichtigung der Art des Verarbeitens personenbezogener Daten und der ihm zur Verfügung stehenden Informationen die Justizvollzugsbehörde beim Einhalten der in den §§ 13, 14, 69 Abs. 5 bis 9 und §§ 75 und 76 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder in einem elektronischen Format abzufassen.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel des Verarbeitens personenbezogener Daten unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf das Verarbeiten personenbezogener Daten als Verantwortlicher.

§ 50
Funktionsübertragung

(1) Werden Aufgaben zu vollzuglichen Zwecken öffentlichen oder nichtöffentlichen Stellen zum Erledigen übertragen, dürfen diesen Stellen gegenüber personenbezogene Daten offengelegt werden, soweit dies für das Erfüllen der Aufgaben erforderlich ist. Personenbezogene Daten besonderer Kategorien dürfen nur offengelegt werden, soweit dies für das Erfüllen der Aufgaben unbedingt erforderlich ist. Ist das Offenlegen personenbezogener Daten nach Satz 1 oder 2 zulässig ist, dürfen auch Akten und Dateisysteme überlassen werden, soweit dies zum Erfüllen der Aufgaben erforderlich ist.

(2) Die Justizvollzugsbehörden wählen die zu beauftragenden Stellen sorgfältig aus. Dabei berücksichtigen sie insbesondere, ob diese Stellen die ausreichende Gewähr dafür bieten, die für ein datenschutzgerechtes Verarbeiten personenbezogener Daten erforderlichen technischen und organisatorischen Maßnahmen treffen zu können. Der Auftrag ist schriftlich oder in einem elektronischen Format zu erteilen und enthält Angaben zum Gegenstand und zum Umfang der übertragenen Aufgaben, die Erforderlichkeit des Verarbeitens von personenbezogenen Daten zu deren Erfüllen und das Verpflichten, des eingesetzten Personals nach dem Verpflichtungsgesetz. Die Justizvollzugsbehörden sind verpflichtet, das Einhalten, der von den beauftragten Stellen getroffenen datenschutzrechtlichen Maßnahmen, regelmäßig zu überprüfen und dies zu dokumentieren.

(3) Soweit die beauftragten Stellen zum Erfüllen der übertragenen Aufgaben personenbezogene Daten verarbeiten sind diese auch Verantwortliche und finden die Vorschriften dieses Gesetzes entsprechende Anwendung.

§ 51
Verarbeiten personenbezogener Daten auf Weisung des Verantwortlichen

Jede einer Justizvollzugsbehörde oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese ausschließlich auf Weisung der Justizvollzugsbehörde verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zum Verarbeiten dieser personenbezogenen Daten verpflichtet ist.

§ 52
Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel des Verarbeitens personenbezogener Daten fest, gelten sie als gemeinsam Verantwortliche. Gemeinsam Verantwortliche legen ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung fest, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachkommt und wie und gegenüber wem die betroffene Person ihre Rechte wahrnehmen kann. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

§ 53
Elektronisches Führen von Akten

Die Justizvollzugsbehörden dürfen ihre Akten auch in einem elektronischen Format führen.

§ 54
Zentrales Datei-, Buchhaltungs- und Abrechnungssystem

(1) Die Justizvollzugsbehörden dürfen personenbezogene Daten auch in einem zentralen Datei-, Buchhaltungs- und Abrechnungssystem verarbeiten. Dabei kann dieses System so ausgestaltet werden, dass weitgehende Standardisierungen beim Protokollieren, beispielsweise von Abfrage- und Abrufgründen, im Rahmen des zulässigen Offenlegens personenbezogene Daten gegenüber anderen Stellen möglich sind.

(2) Werden personenbezogene Daten auf der Grundlage von Absatz 1 verarbeitet, stellen die Justizvollzugsbehörden auch technisch sicher, dass Zugriffe nur auf diejenigen personenbezogenen Daten und Erkenntnisse möglich sind, deren Kenntnis für das Erfüllen der jeweiligen dienstlichen Pflichten erforderlich ist und ein Verarbeiten von personenbezogenen Daten nur durch hierzu befugte Personen erfolgt. Hierzu kann das Vergeben von Zugriffsberechtigungen auf der Grundlage eines abgestuften Rechte- und Rollenkonzeptes erfolgen. Das Erstellen und Fortschreiben des abgestuften Rechte- und Rollenkonzeptes erfolgt unter Beteiligung des und Überwachung durch den Datenschutzbeauftragten. Der Landesbeauftragte für den Datenschutz ist zu unterrichten.

§ 55
Einrichten automatisierter Verfahren

(1) Das Einrichten gemeinsamer automatisierter Dateisysteme und automatisierter Verfahren, in denen innerhalb einer Justizvollzugsbehörde oder in und aus mehreren Justizvollzugsbehörden personenbezogene Daten automatisiert verarbeitet werden und abgerufen werden können, ist zulässig, soweit das automatisierte Offenlegen oder das automatisierte Abrufen von personenbezogenen Daten zum Aufrechterhalten, Wiederherstellen oder Durchsetzen der Sicherheit oder Ordnung in den Anstalten oder anderen Einrichtungen des Justizvollzuges, zu Zwecken des Behandelns und Betreuens oder der Nachsorge von Gefangenen, aus Gründen des Vereinfachens der Verwaltung oder zum Wahrnehmen von Kontroll- und Aufsichtsbefugnissen des für Justizvollzug zuständigen Ministeriums, unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Aufgaben der beteiligten Stellen, angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können.

(2) Die Staatsanwaltschaften bei den Gerichten des Landes sind befugt, personenbezogene Daten über Freiheitsentziehungen im automatisierten Verfahren abzurufen, soweit diese personenbezogenen Daten für Zwecke der Strafrechtspflege erforderlich sind.

(3) Die Zulässigkeit des automatisierten Offenlegens der in § 32 Abs. 2 des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl. I S. 1354), jeweils angeführten personenbezogenen Daten bleibt unberührt.

(4) Das Land kann unter den Voraussetzungen von Absatz 1 mit anderen Ländern und dem Bund einen Datenverbund vereinbaren, der ein automatisiertes Offenlegen und ein automatisiertes Abrufen personenbezogener Daten betroffener Personen ermöglicht.

§ 56
Verantwortung und Verordnungsermächtigung

(1) Die Verantwortung für das Einrichten von automatisierten Verfahren, Verbundverfahren und Verbunddateisystemen trägt das für Justizvollzug zuständige Ministerium oder die von diesem, für die jeweilige Fachverfahren bestimmte Stelle.

(2) Erfolgt das Offenlegen oder das Abrufen von personenbezogenen Daten im automatisierten Verfahren oder im automatisierten Verbundverfahren, so trägt der Empfänger die Verantwortung für die Rechtmäßigkeit des Abrufens.

(3) Die an einem gemeinsamen Datenverbund beteiligten Stellen sind gemeinsame Verantwortliche.

(4) Die speichernden und am automatisierten Abrufverfahren beteiligten Stellen sind für die von ihnen zu treffenden erforderlichen technischen und organisatorischen Maßnahmen verantwortlich und gewährleisten, dass das Verarbeiten personenbezogener Daten nach Maßgabe von § 16 protokolliert wird.

(5) Das für Justizvollzug zuständige Ministerium wird ermächtigt, durch Verordnung die Einzelheiten des elektronischen Führens von Akten und das Einrichten automatisierter Offenlegungs- und Abrufverfahren zu bestimmen sowie der IT-Leitstelle für den Justizvollzug, die Pflichten zum Gewährleisten der Sicherheit personenbezogener Daten und die entsprechende Weisungsbefugnis gegenüber den Anstalten zu übertragen. Die Verordnung sieht zudem Maßnahmen des Datensicherns und der Datenkontrolle vor, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Die Empfänger, die Kategorien der personenbezogenen Daten und die Zwecke des Offenlegens und des Abrufens sind ebenso festzulegen. Der Landesbeauftragte für den Datenschutz ist zu unterrichten.

Unterabschnitt 6
Schutz von Geheimnisträgern

§ 57
Geheimnisträger

(1) Die mit dem Untersuchen, Behandeln, Betreuen oder Beraten der Gefangenen beauftragten

1. Ärzte, Zahnärzte, Apotheker und Psychologischen Psychotherapeuten oder Angehörigen eines anderen Heilberufes, der für das Ausüben des Berufes oder

das Führen der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Diplom-Psychologen,

3. staatlich anerkannten Sozialarbeiter oder staatlich anerkannten Sozialpädagogen und

4. Seelsorger

unterliegen hinsichtlich der ihnen in der ausgeübten Funktion anvertrauten oder sonst bekannt gewordenen Geheimnisse untereinander sowie gegenüber den Justizvollzugsbehörden der Schweigepflicht, soweit dieses Gesetz keine andere Regelung trifft. Dies gilt entsprechend für ihre berufsmäßig tätigen Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind, nicht aber gegenüber dem Berufsträger, sowie für Dolmetscher.

(2) Behandeln Geheimnisträger nach Absatz 1 Satz 1 Nrn. 1 bis 3 (Berufsgeheimnisträger) gleichzeitig oder nacheinander dieselben Gefangenen, so unterliegen sie im Verhältnis zueinander nicht der Schweigepflicht und sind entweder nach § 58 zum Offenbaren personenbezogener Daten verpflichtet oder nach § 59 dazu befugt. Die Justizvollzugsbehörden weisen die Berufsgeheimnisträger auf ihre Offenbarungspflichten und Offenbarungsbefugnisse nach diesem Gesetz hin.

§ 58
Pflicht der Berufsgeheimnisträger zum Offenbaren personenbezogener Daten

(1) Berufsgeheimnisträger sind verpflichtet, ihnen bekannte personenbezogene Daten von sich aus oder auf Befragen gegenüber den Justizvollzugsbehörden zu offenbaren, auch wenn sie ihnen im Rahmen des beruflichen Vertrauensverhältnisses anvertraut wurden oder sonst bekannt geworden sind, soweit

1. die betroffene Person einwilligt oder

2. dies auch unter dem Berücksichtigen der Interessen der betroffenen Person am Geheimhalten der personenbezogenen Daten erforderlich ist zum Abwehren

   a) einer Gefahr für das Leben eines Menschen, insbesondere zum Verhüten von Selbsttötungen,

   b) einer erheblichen Gefahr für Körper oder Gesundheit eines Menschen oder

   c) der Gefahr einer Straftat von erheblicher Bedeutung.

(2) Berufsgeheimnisträger sind über Absatz 1 hinaus dazu verpflichtet, die ihnen bekannt gewordenen personenbezogenen Daten gegenüber den Justizvollzugsbehörden zu offenbaren, soweit dies für das von den Justizvollzugsbehörden vorzunehmende Überprüfen ihrer Tätigkeit bezüglich Abrechnung, Wirtschaftlichkeit und Qualität sowie zum Zwecke der Kostenbeteiligung der Gefangenen oder dem Sicherstellen und Einleiten von strafvollstreckungsrechtlichen Maßnahmen, auch im Fall des Unterbrechens der Haft, erforderlich ist. Hierzu zählen insbesondere

1. die erbrachten Leistungen,

2. die Behandlungsdauer und

3. die allgemeinen Angaben über die Gefangenen, insbesondere

   a) das Verlassen und den Wechsel der stationären Unterbringung, der stationären Einrichtung oder anderen Praxisräumlichkeiten der Berufsgeheimnisträger

   b) den Wechsel der Berufsgeheimnisträger und

   c) das Ende des Untersuchens, Behandelns, Betreuens und Beratens der Gefangenen durch die Berufsgeheimnisträger.

(3) Staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen, die als Bedienstete für Justizvollzugsbehörden tätig sind, sind verpflichtet, die ihnen bekannten personenbezogene Daten von sich aus oder auf Befragen zu offenbaren, soweit dies für das Erreichen der in § 1 genannten Zwecke erforderlich ist.

§ 59
Befugnis der Berufsgeheimnisträger zum Offenbaren personenbezogener Daten

Die Berufsgeheimnisträger sind befugt, die ihnen im Rahmen des beruflichen Vertrauensverhältnisses anvertrauten oder sonst bekannt gewordenen personenbezogenen Daten gegenüber den Justizvollzugsbehörden zu offenbaren, soweit dies für das Erreichen der in § 1 genannten Zwecke, auch unter Berücksichtigung der Interessen der betroffenen Person an deren Geheimhalten, erforderlich ist.

§ 60
Pflicht zum Unterrichten

(1) Die Berufsgeheimnisträger unterrichten die betroffene Person vor dem Erheben personenbezogener Daten schriftlich über ihre nach diesem Gesetz bestehenden Pflichten und Befugnisse zum Offenbaren personenbezogener Daten. Sind Berufsgeheimnisträger mit der Gesundheitsfürsorge außerhalb der Anstalten beauftragt, erfolgt das Unterrichten durch die Anstalten.

(2) Die betroffene Person wird über das Offenbaren ihrer personenbezogenen Daten nach § 58 Abs. 1 Nr. 2, Abs. 2 und 3 sowie nach § 59 benachrichtigt. Dies gilt nicht, sofern die betroffene Person auf andere Weise Kenntnis vom Offenbaren ihrer personenbezogenen Daten erlangt hat. Das Benachrichtigen der betroffenen Person kann unterbleiben, solange durch sie der Zweck der Maßnahme vereitelt würde. Es ist unverzüglich nachzuholen, sobald der Zweck der Maßnahme entfallen ist.

§ 61
Zweckbindung nach dem Offenbaren personenbezogener Daten

Die nach den §§ 58 und 59 offenbarten personenbezogenen Daten dürfen nur für den Zweck, für den sie offenbart wurden oder für den ihr Offenbaren zulässig gewesen wäre, und nur unter denselben Voraussetzungen weiterverarbeitet werden, unter denen Berufsgeheimnisträger selbst hierzu befugt wären. Insoweit kann der Anstaltsleiter das unmittelbare Offenbaren personenbezogenen Daten gegenüber bestimmten Bediensteten in der Anstalt auch allgemein zulassen.

§ 62
Zugriff auf personenbezogene Daten in Notfällen

Alle im Vollzug tätigen Personen dürfen sich Kenntnis auch von personenbezogenen Daten besonderer Kategorien zu dem Zweck verschaffen, diese personenbezogenen Daten unmittelbar und unverzüglich gegenüber den zur Notfallrettung eingesetzten Personen oder Stellen offenzulegen,

1. soweit die betroffene Person einwilligt oder

2. sofern die betroffene Person unfähig ist, einzuwilligen, und die Kenntnis auch der personenbezogenen Daten besonderer Kategorien zum Abwehren einer gegenwärtigen Gefahr für das Leben eines Menschen oder einer gegenwärtigen erheblichen Gefahr für die Gesundheit eines Menschen unbedingt erforderlich ist.

Das Weiterverarbeiten der so erlangten personenbezogenen Daten für andere Zwecke ist unzulässig. Deren Kenntnisnahme ist in der Gefangenenpersonalakte der betroffenen Gefangenen zu dokumentieren.

Unterabschnitt 7
Löschen und Vernichten, Einschränken des Verarbeitens und Berichtigen personenbezogener Daten

§ 63
Löschen und Vernichten personenbezogener Daten

(1) Die Justizvollzugsbehörden löschen und vernichten personenbezogene Daten unverzüglich, wenn deren Verarbeiten unzulässig ist, diese zum Erfüllen einer rechtlichen Verpflichtung gelöscht werden müssen oder

1. zu vollzuglichen Zwecken,

2. zum Verfolgen von Straftaten,

3. für das Durchführen wissenschaftlichen Forschungsvorhaben sowie

4. zum Feststellen, Durchsetzen oder Abwehren von Rechtsansprüchen im Zusammenhang mit dem Vollzug oder dem Vollstrecken von Freiheitsentziehungen

nicht mehr erforderlich sind. Die Erforderlichkeit des Löschens und Vernichtens personenbezogene Daten ist jährlich zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten nach Satz 2 beginnt mit dem Entlassen oder Verlegen des Gefangenen in eine andere Einrichtung, in sonstigen Fällen mit dem Erheben der personenbezogenen Daten.

(2) Personenbezogene Daten sind spätestens fünf Jahre nach dem Entlassen oder Verlegen des Gefangenen in eine andere Einrichtung zu löschen und zu vernichten. Im Vollzug der Jugendstrafe beträgt die Frist drei Jahre und im Vollzug des Jugendarrestes zwei Jahre. Hiervon können bis zum Ablauf der Aufbewahrungsfrist für die Gefangenenpersonalakte die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum des Gefangenen ausgenommen werden, soweit dies für das Auffinden der Gefangenenpersonalakte erforderlich ist.

(3) Soweit Justizvollzugsbehörden im Vollzug einer Freiheitsentziehung nach § 1 Nrn. 1, 7 und 8 von einem nicht nur vorläufigen Einstellen des Verfahrens, einer unanfechtbaren Ablehnung des Eröffnens des Hauptverfahrens oder einem rechtskräftigen Freispruch Kenntnis erlangen, löschen und vernichten sie die personenbezogenen Daten des Gefangenen unverzüglich. Darüber hinaus sind in diesen Fällen auf Antrag des Gefangenen die Stellen, die eine Mitteilung nach § 39 erhalten haben, über den Verfahrensausgang in Kenntnis zu setzen. Der Gefangene ist auf sein Antragsrecht beim Anhören oder dem nachträglichen Unterrichten nach § 39 Abs. 4 Satz 2 hinzuweisen.

(4) Die nach § 22 Abs. 3 erhobenen Identifikationsmerkmale sind spätestens 24 Stunden nach ihrem Erheben zu löschen und zu vernichten, soweit nicht ein Fall von § 30 Abs. 2 Nr. 2 vorliegt; in diesem Fall sind sie unverzüglich offenzulegen und danach zu löschen und zu vernichten.

(5) Aufzeichnungen nach den §§ 26 und 27 sind spätestens nach Ablauf eines Monats zu löschen und zu vernichten. Dies gilt nicht, wenn und solange ein fortdauerndes Speichern oder Aufbewahren zum Aufklären, Verfolgen und Ahnden der aufgezeichneten Vorkommnisse unbedingt erforderlich ist.

§ 64
Einschränken des Verarbeitens personenbezogener Daten

(1) Anstatt personenbezogene Daten zu löschen und zu vernichten, dürfen die Justizvollzugsbehörden deren Verarbeiten einschränken:

1. aufgrund tatsächlicher Anhaltspunkte zum Verhüten und Abwehren von Gefahren, zum Verhindern und Verfolgen von Straftaten oder zu den in § 29 Abs. 2 Nr. 4 genannten Zwecken,

2. die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird und sich weder deren Richtigkeit noch Unrichtigkeit feststellen lässt,

3. dem Löschen und Vernichten der personenbezogenen Daten die Aufbewahrungsfrist einer anderen Rechtsnorm entgegensteht,

4. Grund zu der Annahme besteht, dass das Löschen und Vernichten der personenbezogenen Daten schutzwürdige Interessen der betroffenen Person oder Dritter beeinträchtigen würde,

5. das Löschen und Vernichten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist,

6. zum Feststellen, Durchsetzen oder Abwehren von Rechtsansprüchen im Zusammenhang mit dem Vollzug oder dem Vollstrecken von Freiheitsentziehungen,

7. für das Durchführen wissenschaftlicher Forschungsvorhaben,

8. die personenbezogenen Daten nur zu Zwecken des Datensicherns oder der Datenschutzkontrolle gespeichert sind oder

9. die personenbezogenen Daten zu Beweiszwecken weiter aufbewahrt werden müssen.

(2) In ihrem Verarbeiten eingeschränkte personenbezogene Daten dürfen nur zu dem Zweck weiterverarbeitet werden, der ihrem Löschen und Vernichten entgegenstand. Sie dürfen auch weiterverarbeitet werden, soweit dies zum Beheben einer Beweisnot oder zum Verfolgen von Straftaten erforderlich ist oder die betroffene Person einwilligt.

(3) Das Einschränken des Verarbeitens personenbezogener Daten ist aufzuheben und deren Verarbeiten wieder uneingeschränkt zulässig, wenn die betroffene Person eingewilligt hat oder der Gefangene erneut in derselben oder einer anderen Anstalt innerhalb des Bundesgebietes oder eines Mitgliedstaates der Europäischen Union zum Vollzug einer Strafe, Sicherungsverwahrung, Untersuchungshaft oder einer in § 1 Nrn. 7 und 8 genannten Haftart aufgenommen wird.

(4) Das Einschränken des Verarbeitens personenbezogener Daten darf, soweit dies

1. aus medizinischen Gründen allein zum Wohl der betroffenen Person,

2. zum Schutz elementarer Persönlichkeitsrechte von Berufsgeheimnisträgern,

3. zum Schutz elementarer Persönlichkeitsrechte sowie von Leib oder Leben Dritter oder

4. aufgrund einer Rechtsvorschrift, die zum Geheimhalten verpflichtet,

und auch unter dem Berücksichtigen des Informationsinteresses der betroffenen Person zwingend erforderlich ist, vermerkt werden. Vermerke nach Satz 1 Nrn. 1 und 2 werden von den Berufsgeheimnisträgern angebracht, welche die einzuschränkenden Aktenbestandteile zur Akte verfügt haben; die übrigen Vermerke bringt der An-

staltsleiter an. Vermerke nach Satz 1 sind vom Einschränken des Verarbeitens personenbezogener Daten umfasst.

(5) In ihrem Verarbeiten eingeschränkte personenbezogene Daten dürfen nicht über zehn Jahre hinaus aufbewahrt werden. Dies gilt nicht, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass das Aufbewahren für die in Absatz 1 genannten Zwecke weiterhin erforderlich ist. Die Frist zum Aufbewahren beginnt mit dem auf das Jahr der aktenmäßigen Weglegung folgenden Kalenderjahr. Die Bestimmungen des Archivgesetzes Sachsen-Anhalt bleiben unberührt.

(6) Bei automatisierten Dateisystemen stellen die Justizvollzugsbehörden technisch sicher, dass das Einschränken des Verarbeitens personenbezogener Daten eindeutig erkennbar ist und ein Weiterverarbeiten für andere Zwecke nicht ohne weiteres Prüfen möglich ist.

§ 65
Berichtigen personenbezogener Daten

(1) Die Justizvollzugsbehörden berichtigen personenbezogene Daten unverzüglich, wenn sie unrichtig sind. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der personenbezogenen Daten nicht festgestellt werden kann, tritt an die Stelle ihres Berichtigens das Einschränken des Verarbeitens. In diesem Fall ist die betroffene Person zu unterrichten, bevor das Einschränken des Verarbeitens ihrer personenbezogenen Daten wieder aufgehoben wird.

(2) Die Justizvollzugsbehörden vervollständigen oder ergänzen die unvollständigen personenbezogenen Daten der betroffenen Person, wenn dies unter Berücksichtigung der Verarbeitungszwecke und des berechtigten Interesses der betroffenen Person erforderlich ist. Das Vervollständigen personenbezogener Daten kann auch mittels einer ergänzenden Erklärung erfolgen.

§ 66
Verfahren

(1) Haben die Justizvollzugsbehörden personenbezogene Daten berichtigt, teilen sie einer Stelle, die die personenbezogenen Daten ihnen gegenüber zuvor offengelegt hat, dies mit. Stellen die Justizvollzugsbehörden fest, dass sie unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig offengelegt haben, teilen sie dies den Empfängern unverzüglich mit. In Fällen des Löschens, des Vernichtens oder des Einschränkens des Verarbeitens personenbezogener Daten teilen die Justizvollzugsbehörden den Empfängern, gegenüber denen sie diese personenbezogenen Daten offengelegt haben, diese Maßnahmen mit, wenn dies zum Wahren schutzwürdiger Interessen der betroffenen Personen erforderlich ist. In diesen Fällen berichtigen, löschen und vernichten die Empfänger die ihrer Verantwortung unterliegenden personenbezogenen Daten unverzüglich oder schränken diese in ihrem Verarbeiten ein.

(2) Die Justizvollzugsbehörden unterrichten die betroffene Person schriftlich, wenn sie von einem Berichtigen, Löschen und Vernichten oder über das an deren Stelle tretende Einschränken des Verarbeitens ihrer personenbezogenen Daten absehen.

(3) Das Unterrichten der betroffenen Person nach Absatz 2 kann unterbleiben, wenn

1. dies einen unverhältnismäßigen Aufwand erfordern würde,

2. kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen der betroffenen Person beeinträchtigt werden oder

3. dies eine Gefährdung im Sinne des § 69 Abs. 2 mit sich bringen würde.

(4) Die Mitteilungen sind zu begründen, es sei denn, dass die Angabe der Gründe den mit dem Absehen von dem Unterrichten verfolgten Zweck gefährden würde.

(5) Vor dem Löschen und Vernichten personenbezogener Daten sind diese nach Maßgabe des Archivgesetzes Sachsen-Anhalt dem Landesarchiv Sachsen-Anhalt anzubieten und zu übergeben.

(6) Der Grund und der Umfang des Löschens, des Vernichtens, des Berichtigens und des Einschränkens des Verarbeitens personenbezogener Daten sind zu dokumentieren. Beim Einschränken des Verarbeitens personenbezogener Daten gilt dies auch für den Zweck des Weiterverarbeitens und den Empfänger personenbezogener Daten. In Fällen des Berichtigens personenbezogener Daten genügt es, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt oder aus welchem Grund personenbezogene Daten unrichtig waren oder unrichtig geworden sind.

(7) Wird die betroffene Person nach Absatz 2 unterrichtet, kann sie ihr Auskunftsrecht auch über den Landesbeauftragten für den Datenschutz ausüben. Die Justizvollzugsbehörden unterrichten die betroffene Person über diese Möglichkeit sowie darüber, dass sie den Landesbeauftragten für den Datenschutz anrufen oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht das für Justizvollzug zuständige Ministerium im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Der Landesbeauftragte für den Datenschutz hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder das Überprüfen durch ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung des Landesbeauftragten für den Datenschutz an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der Justizvollzugsbehörden zulassen, sofern diese keiner weitergehenden Auskunft zustimmen. Die Justizvollzugsbehörden dürfen die Zustimmung nur insoweit und solange verweigern, wie sie von einer Auskunft absehen oder diese einschränken könnten. Der Landesbeauftragte für den Datenschutz unterrichtet zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz.

Abschnitt 5
Rechte der betroffenen Person

§ 67
Rechte der betroffenen Person

Die betroffene Person hat nach Maßgabe dieses Gesetzes ein Recht auf

1. das Löschen und das Vernichten (§ 63),

2. das Einschränken des Verarbeitens (§ 64),

3. das Berichtigen (§ 65) ihrer personenbezogenen Daten und

4. Allgemeine Informationen (§ 68),

5. Benachrichtigen (§ 69),

6. Auskunft (§ 70) sowie

7. Akteneinsicht (§ 71).

§ 68
Allgemeine Informationen

Die Justizvollzugsbehörden stellen in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung über

1. die Zwecke des von ihnen vorgenommenen Verarbeitens personenbezogener Daten,

2. die im Hinblick auf das Verarbeiten personenbezogener Daten bestehenden Rechte der betroffenen Person auf Auskunft, Berichtigen, Löschen und Vernichten sowie Einschränken des Verarbeitens ihrer personenbezogenen Daten,

3. den Namen und die Kontaktdaten der Justizvollzugsbehörde und des Datenschutzbeauftragten,

4. das Recht, den Landesbeauftragten für den Datenschutz anzurufen und

5. die Erreichbarkeit des Landesbeauftragten für den Datenschutz.

§ 69
Benachrichtigen der betroffenen Person

(1) Ist das Benachrichtigen der betroffenen Person über das Verarbeiten sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so enthält das Benachrichtigen zumindest die folgenden Angaben:

1. die in § 68 genannten Angaben,

2. die Rechtsgrundlagen des Verarbeitens personenbezogener Daten,

3. die für die personenbezogenen Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für das Festlegen dieser Dauer,

4. die Kategorien von Empfängern personenbezogener Daten sowie

5. weitere Informationen, insbesondere, wenn personenbezogene Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 dürfen die Justizvollzugsbehörden das Benachrichtigen der betroffenen Person insoweit und solange aufschieben, einschränken oder unterlassen, wie dieses andernfalls

1. das Erreichen vollzuglicher Zwecke,

2. die öffentliche Sicherheit oder

3. Verfahren zum Zweck des Verhütens, des Ermittelns, des Aufdeckens oder des Verfolgens von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung oder

4. Rechtsgüter Dritter gefährden würde oder

5. sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde

und das Interesse am Vermeiden dieser Gefahren und Nachteile, das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich das Benachrichtigen auf das Offenlegen personenbezogener Daten gegenüber den Behörden der Staatsanwaltschaft, den Polizeibehörden, den Landesfinanzbehörden, soweit diese personenbezogenen Daten im Erfüllen ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zum Überwachen und Prüfen speichern, den Verfassungsschutzbehörden des Bundes und der Länder, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, anderen Behörden des Bundesministeriums der Verteidigung, ist sie nur mit dem Zustimmen dieser Stellen zulässig. Dies gilt für das Erheben von personenbezogenen Daten bei den in Satz 1 genannten Behörden entsprechend.

(4) Im Fall des Einschränkens nach Absatz 2 gilt § 70 Abs. 8 entsprechend.

(5) Hat das Verletzen des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge, benachrichtigen die Justizvollzugsbehörden die betroffene Person unverzüglich über den Vorfall.

(6) Das Benachrichtigen der betroffenen Person nach Absatz 5 beschreibt in klarer und einfacher Sprache die Art des Verletzens des Schutzes personenbezogener Da-

ten und umfasst zumindest die in § 76 Abs. 3 Nrn. 2 bis 4 genannten Informationen und Maßnahmen.

(7) Von dem Benachrichtigen der betroffenen Person nach Absatz 5 kann abgesehen werden, wenn

1. die Justizvollzugsbehörden geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen haben und diese Vorkehrungen auf die vom Verletzen des Schutzes personenbezogener Daten betroffenen personenbezogenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie das Verschlüsseln, durch das die personenbezogenen Daten für unbefugte Personen unzugänglich gemacht wurden;

2. die Justizvollzugsbehörden durch die im Anschluss an das Verletzen getroffenen Maßnahmen sichergestellt haben, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr im Sinne des Absatzes 5 mehr besteht, oder

3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall erfolgt stattdessen ein öffentliches Bekanntmachen oder eine ähnliche Maßnahme, durch welche die betroffene Person vergleichbar wirksam informiert wird.

(8) Wenn die Justizvollzugsbehörden die betroffene Person über ein Verletzen des Schutzes personenbezogener Daten nicht benachrichtigt haben, kann der Landesbeauftragte für den Datenschutz förmlich feststellen, dass seiner Ansicht nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat er die Wahrscheinlichkeit zu berücksichtigen, dass das Verletzen eine erhebliche Gefahr im Sinne des Absatzes 5 zur Folge hat.

(9) Das Benachrichtigen der betroffenen Person nach Absatz 5 darf unter den in Absatz 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von dem Verletzen ausgehenden erheblichen Gefahr im Sinne des Absatzes 5 überwiegen.

(10) § 76 Abs. 7 findet entsprechende Anwendung.

§ 70
Auskunft an die betroffene Person

(1) Die Justizvollzugsbehörden erteilen der betroffenen Person auf Antrag Auskunft darüber, ob sie betreffende personenbezogene Daten verarbeitet werden. Die betroffene Person erhält darüber hinaus Informationen über

1. die personenbezogenen Daten, die Gegenstand des Verarbeitens sind, und die Kategorie, zu der sie gehören,

2. die verfügbaren Informationen zur Herkunft der personenbezogenen Daten,

3. die Zwecke des Verarbeitens personenbezogener Daten und deren Rechtsgrundlagen,

4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,

5. die für die personenbezogenen Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für das Festlegen dieser Dauer,

6. das Bestehen der Rechte auf Berichtigen, Löschen und Vernichten oder Einschränken des Verarbeitens personenbezogener Daten durch die Justizvollzugsbehörden,

7. das Recht, den Landesbeauftragten für den Datenschutz anzurufen, sowie

8. Angaben zur Erreichbarkeit des Landesbeauftragten für den Datenschutz.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht und vernichtet werden dürfen oder die ausschließlich den Zwecken des Datensicherns oder der Datenschutzkontrolle dienen, wenn das Erteilen der Auskunft einen unverhältnismäßigen Aufwand erfordern würde und das Verarbeiten der personenbezogenen Daten zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Von dem Erteilen einer Auskunft ist abzusehen, wenn die betroffene Person keine Angaben macht, die das Auffinden der personenbezogenen Daten ermöglichen, und deshalb der für das Erteilen der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Die Justizvollzugsbehörden dürfen von der Auskunft nach Absatz 1 Satz 1 absehen oder das Erteilen einer Auskunft nach Absatz 1 Satz 2 teilweise oder vollständig einschränken, soweit und solange

1. das Erreichen vollzuglicher Zwecke,

2. die öffentliche Sicherheit oder

3. Verfahren zum Zweck des Verhütens, des Ermittelns, des Aufdeckens oder des Verfolgens von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung oder

4. Rechtsgüter Dritter gefährdet würden oder

5. sonst dem Wohle des Bundes oder eines Landes Nachteile bereitet würden

und das Interesse am Vermeiden dieser Gefahren und Nachteile das Informationsinteresse der betroffenen Person überwiegt.

(5) Bezieht sich das Benachrichtigen auf das Offenlegen personenbezogener Daten gegenüber den Behörden der Staatsanwaltschaft, den Polizeibehörden, den

Landesfinanzbehörden, soweit diese personenbezogenen Daten im Erfüllen ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zum Überwachen und Prüfen speichern, den Verfassungsschutzbehörden des Bundes und der Länder, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, anderen Behörden des Bundesministeriums der Verteidigung, ist sie nur mit dem Zustimmen dieser Stellen zulässig. Dies gilt für das Erheben von personenbezogenen Daten bei den in Satz 1 genannten Behörden entsprechend.

(6) Soweit im Vollzug einer Freiheitsentziehung nach § 1 Nrn. 1, 7 und 8 Erkenntnisse aus dem Ermittlungsverfahren zur Gefangenenpersonalakte der betroffenen Gefangenen gelangt sind, ist die Staatsanwaltschaft vor dem Erteilen der Auskunft zu hören. Teilt die Staatsanwaltschaft mit, dass die Auskunft die Aufgabe des Vollzuges der Untersuchungshaft gefährden würde, darf insoweit keine Auskunft erteilt werden.

(7) Die Justizvollzugsbehörden unterrichten die betroffene Person über das Absehen von oder das Einschränken einer Auskunft unverzüglich schriftlich. Dies gilt nicht, wenn bereits das Erteilen dieser Informationen eine Gefährdung, einen Nachteil oder eine Beeinträchtigung im Sinne des § 69 Abs. 2 mit sich bringen würde. Die Mitteilungen an die betroffene Person nach Satz 1 sind zu begründen, es sei denn, dass der mit dem Absehen von oder des Einschränkens der Auskunft verfolgte Zweck gefährden würde.

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

(9) Weitergehende Auskunftsrechte nach allgemeinen Gesetzen finden für den Bereich des Justizvollzuges keine Anwendung.

§ 71
Akteneinsicht der betroffenen Person

(1) Ist der betroffenen Person nach § 70 Auskunft zu gewähren, erhält sie auf Antrag Akteneinsicht, soweit eine Auskunft für das Wahrnehmen ihrer rechtlichen Interessen nicht ausreicht, das Einsehen von Akten dafür erforderlich ist und überwiegende berechtigte Interessen Dritter nicht entgegenstehen. Im Vollzug einer Freiheitsentziehung nach § 1 Nrn. 1, 7 und 8 gilt für das Akteneinsichtsrecht § 70 Abs. 6 entsprechend.

(2) In ihrem Verarbeiten eingeschränkte personenbezogene Daten unterliegen nicht der Akteneinsicht.

(3) Die betroffene Person kann bei einer Akteneinsicht auf eigene Kosten

1. eine Person aus dem Kreis

   a) der Rechtsanwälte,

   b) der Notare,

   c) der gewählten Verteidiger nach § 138 Abs. 1 und 2 der Strafprozessordnung,

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

   e) der Beistände nach § 69 des Jugendgerichtsgesetzes,

2. Personensorgeberechtigte sowie

3. einen allgemein beeidigten Dolmetscher hinzuziehen.

Die betroffene Person kann ihr Akteneinsichtsrecht auch durch eine Person aus dem in Satz 1 Nrn. 1 und 2 genannten Personenkreis allein ausüben lassen. Das Begleiten durch andere Gefangene ist unzulässig, auch wenn diese zu dem in Satz 1 genannten Personenkreis gehören.

(4) Bei einer Akteneinsicht haben die betroffene Person oder die von ihr nach Absatz 3 Satz 2 Beauftragten das Recht, sich aus den Akten Notizen zu machen.

(5) Der betroffenen Person und den von ihr nach Absatz 3 Satz 2 Beauftragten sind aus den über die betroffene Person geführten Akten auf schriftlichen Antrag Ablichtungen einzelner Dokumente, aus automatisierten Dateisystemen Ausdrucke eines Teilbestandes der personenbezogenen Daten zu fertigen, soweit die Akten der Einsicht unterliegen und ein berechtigtes Interesse vorliegt. Ein solcher Grund ist insbesondere anzunehmen, wenn die betroffene Person zum Geltendmachen ihrer Rechte gegenüber Gerichten und Behörden auf Ablichtungen oder Ausdrucke angewiesen ist.

§ 72
Verfahren

(1) Zu den Akten im Sinne dieses Gesetzes zählen neben der Gefangenenpersonalakte, der Gesundheitsakte, einschließlich der Krankenblätter, und der Therapieakte auch automatisierte Dateisysteme und elektronisch geführte Akten, soweit sie der Abwicklung des Vollzuges dienen und in einer den papiergebundenen Akten vergleichbaren Weise geordnet geführt werden.

(2) Die Justizvollzugsbehörden kommunizieren mit der betroffenen Person in einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form. Unbeschadet besonderer Formvorschriften sollen beim Beantworten von Anträgen grundsätzlich die für den Antrag gewählte Form verwendet werden.

(3) Bei Anträgen auf Auskunft und Akteneinsicht setzen die Justizvollzugsbehörden die betroffene Person unverzüglich schriftlich darüber in Kenntnis, wie verfahren wurde.

(4) Das Erteilen von allgemeinen Informationen, das Benachrichtigen und das Bearbeiten von Anträgen auf Auskunft, Löschen und Vernichten, Berichtigen oder Einschränken des Verarbeitens personenbezogener Daten erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen auf Auskunft, Löschen und Vernichten, Berichtigen oder Einschränken des Verarbeitens personenbezogener Daten dürfen die Justizvollzugsbehörden eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrages tätig zu werden. In diesem Fall müssen die Justizvollzugsbehörden den offenkundig unbegründeten oder exzessiven Charakter des Antrages belegen.

(5) Das Bearbeiten von Anträgen auf Akteneinsicht ist unentgeltlich. Das Anfertigen von Ablichtungen und Ausdrucken ist gebührenpflichtig. Die Justizvollzugsbehörden erheben auf der Grundlage der Verwaltungskosten hierfür angemessene Gebühren, die im Voraus zu entrichten sind. Werden Gebühren nach Satz 3 nicht entrichtet, dürfen die Justizvollzugsbehörden von dem Bearbeiten des Antrages absehen.

(6) Haben die Justizvollzugsbehörden begründete Zweifel an der Identität der betroffenen Person, die einen Antrag auf Auskunft, Akteneinsicht, Löschen und Vernichten, Berichtigen oder Einschränken des Verarbeitens personenbezogener Daten gestellt hat, dürfen sie von der betroffenen Person zusätzliche Informationen anfordern, die zum Bestätigen ihrer Identität erforderlich sind.

(7) Die Justizvollzugsbehörden dokumentieren die Gründe für ihre Entscheidungen.

Abschnitt 6
Datenschutzbeauftragter

§ 73
Datenschutzbeauftragter

(1) Die Justizvollzugsbehörde benennt einen Datenschutzbeauftragten. Der Datenschutzbeauftragte darf Beschäftigter der Justizvollzugsbehörde sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrages erfüllen. Er wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechtes und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zum Erfüllen der in den Absätzen 7 bis 9 genannten Aufgaben. Die Kontaktdaten des Datenschutzbeauftragten veröffentlichen die Justizvollzugsbehörde und teilen sie dem Landesbeauftragten für den Datenschutz mit.

(2) Die Justizvollzugsbehörde stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Sie unterstützt den Datenschutzbeauftragten beim Erfüllen seiner Aufgaben nach den Absätzen 7 bis 9, indem sie die dazu erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zum Erhalten seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) Die Justizvollzugsbehörde stellt sicher, dass der Datenschutzbeauftragte beim Erfüllen seiner Aufgaben keine Anweisungen bezüglich des Ausübens dieser Aufgaben erhält. Der Datenschutzbeauftragte berichtet unmittelbar dem Leiter der Justizvollzugsbehörde.

(4) Der Datenschutzbeauftragte darf wegen dem Erfüllen seiner Aufgaben nicht abberufen oder benachteiligt werden. Sein Abberufen ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die Anstalt zur Kündigung aus wichtigem Grund ohne das Einhalten einer Kündigungsfrist berechtigen. Nach Ende der Tätigkeit als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne das Einhalten einer Kündigungsfrist berechtigt ist.

(5) Die betroffene Person kann den Datenschutzbeauftragten zu allen mit dem Verarbeiten ihrer personenbezogenen Daten und zum Wahrnehmen ihrer Rechte gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2), diesem Gesetz sowie anderen, einschließlich der zum Umsetzen der Richtlinie (EU) 2016/680 erlassenen, Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf die betroffene

Person zulassen, verpflichtet, soweit er nicht durch die betroffene Person davon befreit wird.

(6) Erhält der Datenschutzbeauftragte bei seiner Tätigkeit Kenntnis von personenbezogenen Daten, für die dem Leiter oder einer bei der Justizvollzugsbehörde beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den ihm unterstellten Beschäftigten zu. Über das Ausüben dieses Rechtes entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Datenschutzbeauftragten reicht, unterliegen seine Akten, andere Dokumente und Dateisysteme einem Beschlagnahmeverbot.

(7) Dem Datenschutzbeauftragten obliegen, neben den in der Verordnung (EU) 2016/679 genannten Aufgaben, zumindest die folgenden Aufgaben:

1. das Unterrichten und das Beraten der Justizvollzugsbehörde und der Beschäftigten, welche die personenbezogenen Daten verarbeiten, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zum Umsetzen der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften,

2. das Überwachen des Einhaltens dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zum Umsetzen der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der Justizvollzugsbehörde für den Schutz personenbezogener Daten, einschließlich des Zuweisens von Zuständigkeiten, des Sensibilisierens und des Schulens der an den Verarbeitungsvorgängen beteiligten Beschäftigten und des diesbezüglichen Überprüfens,

3. das Beraten im Zusammenhang mit der Datenschutzfolgenabschätzung und dem Überwachen ihres Durchführens,

4. die Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz,

5. die Tätigkeit als Anlaufstelle für den Landesbeauftragten für den Datenschutz in mit dem Verarbeiten personenbezogener Daten zusammenhängenden Fragen, einschließlich des vorherigen Konsultierens nach § 75.

(8) Der Datenschutzbeauftragte kann auch andere Aufgaben und Pflichten wahrnehmen. Die Justizvollzugsbehörde verhindert in diesem Zusammenhang aber, dass derartige Aufgaben und Pflichten zu einem Interessenkonflikt führen.

(9) Der Datenschutzbeauftragte trägt beim Erfüllen seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke des Verarbeitens personenbezogener Daten berücksichtigt.

Abschnitt 7
Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und zwischen den Aufsichtsbehörden

§ 74
Grundsatz der Zusammenarbeit

Die Justizvollzugsbehörden arbeiten mit dem Landesbeauftragten für den Datenschutz beim Erfüllen seiner Aufgaben zusammen. Dazu werden dem Landesbeauftragten für den Datenschutz, insbesondere Auskünfte zu seinen Fragen, die Einsicht in alle Unterlagen, Akten und Dateisysteme und der Zutritt in alle Diensträume gewährt.

§ 75
Anhören des Landesbeauftragten für den Datenschutz

(1) Die Justizvollzugsbehörden hören vor dem in Betrieb nehmen von neu anzulegenden Dateisystemen und automatisierten Verfahren den Landesbeauftragten für den Datenschutz an, wenn

1. aus einer Datenschutzfolgenabschätzung hervorgeht, dass das Verarbeiten personenbezogener Daten eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge hätte, wenn die Justizvollzugsbehörden keine Abhilfemaßnahmen treffen würden, oder

2. die Form des Verarbeitens personenbezogener Daten, insbesondere beim Verwenden neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Person zur Folge hat.

Der Landesbeauftragte für den Datenschutz kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zum Anhören nach Satz 1 unterliegen.

(2) Die Justizvollzugsbehörden legen dem Landesbeauftragten für den Datenschutz im Fall des Absatzes 1 vor:

1. die durchgeführte Datenschutzfolgenabschätzung,

2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten der Justizvollzugsbehörden, der gemeinsam Verantwortlichen und der an dem Verarbeiten personenbezogener Daten beteiligten Auftragsverarbeiter oder beauftragten Stellen, den Aufgaben des Vollzuges zum Erledigen übertragen wurden,

3. Angaben zu den Zwecken und Mitteln des beabsichtigten Verarbeitens personenbezogener Daten,

4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Person vorgesehenen Maßnahmen und Garantien und

5. Name und Kontaktdaten des Datenschutzbeauftragten.

Auf Anfordern des Landesbeauftragten für den Datenschutz sind diesem zudem alle sonstigen Informationen zu übermitteln, die er benötigt, um die Rechtmäßigkeit des Verarbeitens personenbezogener Daten sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(3) Falls der Landesbeauftragte für den Datenschutz der Ansicht ist, dass das geplante Verarbeiten personenbezogener Daten gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil die Justizvollzugsbehörden das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen haben, kann er den Justizvollzugsbehörden und gegebenenfalls dem Auftragsverarbeiter oder der beauftragten Stelle, der Aufgaben des Vollzuges zum Erledigen übertragen wurden, innerhalb eines Zeitraums von sechs Wochen nach dem Einleiten des Anhörens schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Der Landesbeauftragte für den Datenschutz kann diese Frist um einen Monat verlängern, wenn das geplante Verarbeiten personenbezogener Daten besonders komplex ist. Er hat in diesem Fall innerhalb eines Monats nach dem Einleiten des Anhörens die Justizvollzugsbehörden und gegebenenfalls den Auftragsverarbeiter und die beauftragte Stelle, der Aufgaben des Vollzuges zum Erledigen übertragen wurden, über die Fristverlängerung zu informieren.

(4) Hat das beabsichtigte Verarbeiten personenbezogener Daten erhebliche Bedeutung für das Erfüllen der Aufgaben der Justizvollzugsbehörden und ist es daher besonders dringlich, können diese mit dem Verarbeiten personenbezogener Daten bereits nach dem Beginn des Anhörens, aber vor dem Ablauf der in Absatz 3 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen des Landesbeauftragten für den Datenschutz im Nachhinein zu berücksichtigen und die Art und Weise des Verarbeitens personenbezogener Daten daraufhin gegebenenfalls anzupassen.

§ 76
Meldungen an den Landesbeauftragten für den Datenschutz

(1) Die Justizvollzugsbehörden melden das Verletzen des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem es ihnen bekannt geworden ist, dem Landesbeauftragten für den Datenschutz, es sei denn, dass voraussichtlich keine Gefahr für die Rechtsgüter der betroffenen Person besteht. Erfolgt die Meldung an den Landesbeauftragten für den Datenschutz nicht innerhalb von 72 Stunden, so ist das Verzögern zu begründen.

(2) Der Auftragsverarbeiter und eine beauftragte Stelle, der Aufgaben des Vollzuges zum Erledigen übertragen wurden, haben das Verletzen des Schutzes personenbezogener Daten unverzüglich den Justizvollzugsbehörden zu melden.

(3) Die Meldung nach Absatz 1 enthält zumindest die folgenden Informationen:

1. das Beschreiben der Art des Verletzens des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl betroffener Personen, die betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze,

2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,

3. das Beschreiben der wahrscheinlichen Folgen und

4. das Beschreiben der von den Justizvollzugsbehörden ergriffenen oder vorgeschlagenen Maßnahmen zum Behandeln des festgestellten Verletzens und zum Abmildern der möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, reichen die Justizvollzugsbehörden sie unverzüglich nach, sobald sie ihnen vorliegen.

(5) Die Justizvollzugsbehörden dokumentieren das Verletzen des Schutzes personenbezogener Daten. Die Dokumentation umfasst alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen.

(6) Soweit personenbezogene Daten betroffen sind, die von einem oder gegenüber einem Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union offengelegt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) Das Melden nach Artikel 33 der Verordnung (EU) 2016/679 oder das Benachrichtigen nach Artikel 34 Abs. 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit dem Zustimmen des Meldepflichtigen oder Benachrichtigenden verwendet werden.

(8) Weitere Pflichten der Justizvollzugsbehörden zu Benachrichtigungen über das Verletzen des Schutzes personenbezogener Daten bleiben unberührt.

§ 77
Gegenseitige Amtshilfe

(1) Der Landesbeauftragte für den Datenschutz übermittelt den Aufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union Informationen und leistet Amtshilfe, soweit dies für das einheitliche Umsetzen und Anwenden der Richtlinie (EU) 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Der Landesbeauftragte für den Datenschutz ergreift alle geeigneten Maßnahmen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingehen nachzukommen.

(3) Der Landesbeauftragte für den Datenschutz darf Amtshilfeersuchen nur ablehnen, wenn

1. er für den Gegenstand des Ersuchens oder für die Maßnahmen, die er durchführen soll, nicht zuständig ist oder

2. das Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) Der Landesbeauftragte für den Datenschutz informiert die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Er erläutert im Fall des Absatzes 3 die Gründe für das Ablehnen des Ersuchens.

(5) Der Landesbeauftragte für den Datenschutz übermittelt die Informationen, um die er von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format.

(6) Der Landesbeauftragte für den Datenschutz erledigt Amtshilfeersuchen kostenfrei, soweit er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates das Erstatten entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen des Landesbeauftragten für den Datenschutz enthält alle erforderlichen Informationen. Zu diesen Informationen gehören insbesondere der Zweck und die Begründung des Ersuchens. Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

Abschnitt 8
Rechtsbehelfe

§ 78
Beschwerde

(1) Die betroffene Person hat, unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs, das Recht auf Beschwerde bei dem Landesbeauftragten für den Datenschutz, wenn sie der Ansicht ist, dass das Verarbeiten der sie betreffenden personenbezogenen Daten gegen die nach diesem Gesetz erlassenen Vorschriften verstößt.

(2) Ist eine Beschwerde nach Absatz 1 bei einer unzuständigen Behörde und nicht bei dem Landesbeauftragten für den Datenschutz eingereicht worden, ist die Beschwerde von der unzuständigen Behörde unverzüglich an den Landesbeauftragten für den Datenschutz weiterzuleiten. Die betroffene Person ist über das Weiterleiten der Beschwerde zu unterrichten.

(3) Der Landesbeauftragte für den Datenschutz leitet eine bei ihm eingelegte Beschwerde über das Verarbeiten personenbezogener Daten, das in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiter. In diesem Fall unterrichtet der Landesbeauftragte für den Datenschutz die betroffene Person über das Weiterleiten und unterstützt sie auf ihr Ersuchen weiterhin.

(4) Der Landesbeauftragten für den Datenschutz unterrichtet die betroffene Person über den Stand und das Ergebnis ihrer Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach § 79.

§ 79
Gerichtlicher Rechtsschutz gegen Entscheidungen des Landesbeauftragten für den Datenschutz

Die betroffene Person hat, unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs, das Recht auf gerichtlichen Rechtsschutz gegen eine sie betreffende rechtsverbindliche Entscheidung des Landesbeauftragten für den Datenschutz. Dies gilt auch, soweit sich der Landesbeauftragte für den Datenschutz nicht mit einer Beschwerde nach § 78 befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis einer solchen Beschwerde in Kenntnis setzt.

Abschnitt 9
Haftung und Sanktionen

§ 80
Recht auf Schadenersatz

(1) Haben die Justizvollzugsbehörden, ein Auftragsverarbeiter oder sonstiger Verantwortlicher einer betroffenen Person durch das Verarbeiten personenbezogener Daten, das nach diesem Gesetz oder nach anderen auf das Verarbeiten anwendbaren Vorschriften rechtswidrig war, vorsätzlich oder grob fahrlässig einen Schaden zugefügt, sind sie der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einem nicht automatisierten Verarbeiten der Schaden nicht auf ein Verschulden der Justizvollzugsbehörden zurückzuführen ist.

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

(3) Lässt sich bei einem automatisierten Verarbeiten personenbezogener Daten nicht ermitteln, welcher von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche oder sein Rechtsträger.

(4) Hat beim Entstehen des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

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

§ 81
Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein, einem Dritten gegenüber offenlegt und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten, die nicht allgemein zugäng-

lich sind, ohne hierzu berechtigt zu sein, verarbeitet oder durch unrichtige Angaben erschleicht.

(3) Der Versuch ist strafbar.

(4) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amtswegen für geboten hält. Antragsberechtigt sind die betroffene Person, die Justizvollzugsbehörde, der Auftragsverarbeiter, die beauftragte Stelle, der Aufgaben des Vollzuges zum Erledigen übertragen wurden und der Landesbeauftragte für den Datenschutz.

Abschnitt 10
Schlussvorschriften

§ 82
Übergangsvorschriften zum Anpassen automatisierter Verarbeitungssysteme

(1) Sofern das Anpassen der vor dem 6. Mai 2016 eingerichteten automatisierten Verarbeitungs- und Verbundsysteme an die Vorgaben dieses Gesetzes mit einem unverhältnismäßigen Aufwand verbunden ist, kann dies bis zum 6. Mai 2023 erfolgen und mit diesem Gesetz in Einklang gebracht werden.

(2) Die Frist des Absatzes 1 kann bei Eintreten oder Vorliegen außergewöhnlicher Umstände verlängert werden, wenn hierdurch sonst schwerwiegende Schwierigkeiten für den Betrieb der automatisierten Verarbeitungs- und Verbundsysteme entstehen würden. Die verlängerte Frist muss vor dem 6. Mai 2026 enden. Das Verlängern der Frist nach Satz 2 sowie die Gründe hierfür sind der Europäischen Kommission mitzuteilen.

§ 83
Anwenden weiterer Vorschriften

Für das Verarbeiten personenbezogener Daten durch Justizvollzugsbehörden zu anderen Zwecken als denen nach diesem Gesetz gelten die Verordnung (EU) 2016/679 und die hierzu erlassenen Vorschriften des Landes.

§ 84
Einschränken von Grundrechten

Durch dieses Gesetz wird das Grundrecht auf Schutz personenbezogener Daten im Sinne des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes und des Artikels 6 Abs. 1 Satz 1 der Verfassung des Landes Sachsen-Anhalt eingeschränkt.

§ 85
Sprachliche Gleichstellung

Personen- und Funktionsbezeichnungen in diesem Gesetz gelten jeweils in männlicher und weiblicher Form.

Artikel 2
Änderung des Justizvollzugsgesetzbuches Sachsen-Anhalt

Das Justizvollzugsgesetzbuch Sachsen-Anhalt vom 18. Dezember 2015 (GVBl. LSA S. 66) wird wie folgt geändert:

1. Die Überschrift erhält folgende Fassung:

   „Erstes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Vollzug der Freiheitsstrafe, der Jugendstrafe, der Untersuchungshaft und des Strafarrestes - (Erstes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - JVollzGB I LSA)“.

2. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angaben zu Abschnitt 23 werden gestrichen.

      „Abschnitt 23 (weggefallen)“.

   b) Die Angabe zu Abschnitt 24 erhält folgende Fassung:

      „Abschnitt 23
      Schlussbestimmungen“.

   c) Die Angaben zu den §§ 164 bis 168 erhalten folgende Fassung:

      „§ 123 Übergangsbestimmungen
      § 124 Berichtspflicht
      § 125 Verhältnis zu Bundesrecht
      § 126 Einschränkung von Grundrechten
      § 127 Sprachliche Gleichstellung“.

3. In § 1 Abs. 2 wird die Angabe „329 Abs. 4 Satz 1“ durch die Angabe „329 Abs. 3“ ersetzt.

4. § 34 wird wie folgt geändert:

   a) In Nummer 3 wird das Wort „oder“ gestrichen.

   b) In Nummer 4 wird der Punkt am Ende durch das Wort „oder“ ersetzt.

   c) Nach Nummer 4 wird folgende Nummer 5 angefügt:
      „5. in den Fällen des § 25 Abs. 5 des Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt.“

5. In § 35 Abs. 1 Satz 1 wird die Angabe „§ 147“ durch die Angabe „§ 22 Abs. 3 des Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt“ ersetzt.

6. In § 36 Abs. 3 wird die Angabe „§ 145“ durch die Angabe „§ 31 Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt ersetzt.

7. In § 37 Abs. 1 Satz 5 wird die Angabe „§ 145“ durch die Angabe „§ 31 des Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt“ ersetzt.

8. § 109 wird wie folgt geändert:

   a) Absatz 2 wird aufgehoben.

   b) Absatz 3 wird Absatz 2.

9. Abschnitt 23 wird aufgehoben.

10. Abschnitt 24 wird Abschnitt 23.

11. Die §§ 164 bis 168 werden die §§ 123 bis 127.

Artikel 3
Änderung des Sicherungsverwahrungsvollzugsgesetzes Sachsen-Anhalt

Das Sicherungsverwahrungsverwahrungsvollzugsgesetz Sachsen-Anhalt vom 13. Mai 2013 (GVBl. LSA S. 206), geändert durch Artikel 2 des Gesetzes vom 18. Dezember 2015 (GVBl. LSA S. 666, 710), wird wie folgt geändert:

1. Die Überschrift erhält folgende Fassung:

   „Zweites Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Vollzug der Sicherungsverwahrung - (Zweites Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - JVollzGB II LSA)“.

2. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu Teil 1 erhält folgende Fassung:

      „Teil 1 (weggefallen)“.

   b) Die Angaben zu den §§ 73 und 74 erhalten folgende Fassung:

      „§ 73 (weggefallen)
      § 74 (weggefallen)“.

   c) Die Angabe zu Abschnitt 20 erhält folgende Fassung:

      „Abschnitt 20 (weggefallen)“.

   d) Die Angabe zu § 108 erhält folgende Fassung:

      „§ 108 (weggefallen)“.

e) Die Angabe zu Teil 4 erhält folgende Fassung:

„Abschnitt 20
Schlussbestimmungen“.

f) Die Angabe zu § 129“ erhält folgende Fassung:

„§ 129 (weggefallen)“.

3. Die Angabe „Teil 1 Vollzug der Sicherungsverwahrung“ wird gestrichen.

4. § 22 wird wie folgt geändert:

a) In Nummer 2 wird das Wort „oder“ am Ende gestrichen.

b) In Nummer 3 wird der Punkt am Ende durch das Wort „oder“ ersetzt.

c) Nach Nummer 3 wird folgende Nummer 4 angefügt:

„4. in den Fällen des § 25 Abs. 5 des Vierten Buches Justizvollzugsgesetzbuches Sachsen-Anhalt“.

5. In § 23 Abs. 1 Satz 1 werden nach dem Wort „lassen“ die Wörter „und den Anordnungen zur Identitätsfeststellung nach § 25 des Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt Folge leistet“ angefügt.

6. § 24 wird wie folgt geändert:

a) Absatz 2 Satz 3 wird aufgehoben.

b) Nach Absatz 3 wird folgender Absatz 4 angefügt:

„(4) Eine Aufzeichnung der optischen und akustischen Überwachung findet nur nach Maßgabe des § 31 Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt statt.“

7. § 25 Abs. 1 wird wie folgt geändert:

a) Nach Satz 3 folgender neuer Satz 4 eingefügt:

„Die Unterhaltung kann zeitversetzt überwacht und nach Maßgabe des § 31 Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt weiterverarbeitet werden.“

b) Der bisherige Satz 4 wird Satz 5.

8. Die §§ 73 und 74 werden aufgehoben.

9. § 76 wird wie folgt geändert:

   a) Die Absatzbezeichnung „(1)“ wird gestrichen.

   b) Absatz 2 wird aufgehoben.

10. § 98 wird wie folgt geändert:

   a) Die Absatzbezeichnung „(1)“ wird gestrichen.

   b) Absatz 2 wird aufgehoben.

11. § 107 Abs. 2 Satz 3 wird aufgehoben.

12. Abschnitt 20 wird aufgehoben.

13. Die Überschrift „Teil 4 Schlussbestimmungen“ wird durch die Überschrift „Abschnitt 20 Schlussbestimmungen“ ersetzt.

14. § 129 wird aufgehoben.

15. § 132 wird wie folgt geändert:

   a) Absatz 1 wird aufgehoben.

   b) Die Absatzbezeichnung „(2)“ wird gestrichen.

   c) Absatz 3 wird aufgehoben.

Artikel 4
Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.

(2) Artikel 1 § 16 tritt am 6. Mai 2023 in Kraft.

Begründung

A. Allgemeiner Teil

1. Gesetzgeberischer Handlungsbedarf

Das Europäische Parlament und der Rat der Europäischen Union haben am 27. April 2016 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 ff.), im Folgenden: „Richtlinie (EU) 2016/680“, erlassen. Die Richtlinie (EU) 2016/680 ist zwingend in nationales Recht umzusetzen. Das betrifft auch den Bereich des Justizvollzuges in Sachsen-Anhalt.

Der Justizvollzug, einschließlich der Sicherungsverwahrung, des Jugendarrestes, der Untersuchungshaft und der ihnen gleichgestellten Freiheitsentziehungen, fällt unter den Begriff der Strafvollstreckung und unter den Schutz vor und dem Abwehren von Gefahren für die öffentliche Sicherheit gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680. Das Einordnen des Justizvollzuges unter den Begriff der Strafvollstreckung ist dem deutschen Rechtssystem immanent. So wird 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 ein europarechtliches Betrachten führt zum Einordnen des Justizvollzuges unter den Begriff der Strafvollstreckung im Sinne der Richtlinie (EU) 2016/680. In zahlreichen europäischen Ländern werden begriffliche Unterscheidungen nicht vorgenommen, sondern beide Rechtsmaterien in einheitlichen Gesetzen geregelt. Auch ein an Sinn und Zweck der Richtlinie (EU 2016/680 orientiertes Betrachten führt zu diesem Ergebnis. Der sensible Bereich der Strafrechtspflege soll gerade der Richtlinie (EU) 2016/680 und nicht der am 25. Mai 2016 in Kraft getretenen 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. Mai 2016, S. 1 ff.) - im Folgenden „Verordnung (EU) 2016/679“ - unterfallen.

Dies soll den Mitgliedstaaten der europäischen Union bei Umsetzen der Richtlinie (EU) 2016/680 größere Handlungs- und Gestaltungsspielräume eröffnen und gilt auch für den Justizvollzug, der, als zeitlich letzter Abschnitt eines Strafverfahrens und als Dienstleister des Gewährleistens des sicheren Durchführens eines Strafverfahrens, ein wesentlicher Teil der Strafrechtspflege ist. Davon werden auch Sanktionen wie die Sicherungsverwahrung und der Jugendarrest erfasst, 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 dem geordneten Durchführen eines Strafverfahrens oder dem Abwehren von Gefahren für die öffentliche Sicherheit und Ordnung.

Der Anwendungsbereich der Richtlinie (EU) 2016/680 ist damit für den Bereich des Justizvollzuges eröffnet und verdrängt insoweit den Anwendungsbereich der Verordnung (EU) 2016/679.

Das vollständige Umsetzen der Richtlinie (EU) 2016/680 im Bereich des Justizvollzuges des Landes macht das umfassende Überarbeiten des bereichsspezifischen Datenschutzes und das Anpassen aller Justizvollzugsgesetze des Landes notwendig.

Der Schutz personenbezogener Daten betroffener Personen im Justizvollzug ist gegenwärtig bereichsspezifisch im Justizvollzugsgesetzbuch Sachsen-Anhalt (JVollzGB LSA) geregelt. Im Sicherungsverwahrungsvollzugsgesetz von Sachsen-Anhalt (SVVollzG LSA) finden sich Verweise auf das JVollzGB LSA (vgl. § 72 SVVollzG LSA). Diese Verweise sind aufzuheben, weil, unabhängig von der Richtlinie (EU) 2016/680, aufgrund der Verordnung (EU) 2016/679 ein vollständiges Neufassen des allgemeinen Datenschutzrechtes in Sachsen-Anhalt folgen wird, das im Anwendungsbereich der Richtlinie (EU) 2016/680 für den Justizvollzug weiterhin keine eigenen Regelungen enthalten wird.

Soweit im Justizvollzug hingegen anderweitige Rechtsmaterie zu vollziehen ist, paradigmatisch wäre insofern das beamtenrechtliche Dienstrecht einschließlich des Personalaktenrechtes zu nennen, vollzieht sich diese Rechtsanwendung außerhalb des sachlichen Anwendungsbereichs gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680. Das hat aus unionsrechtlicher Sicht die Folge, dass bei Vorliegen der weiteren Voraussetzungen der sachliche Anwendungsbereich der Verordnung (EU) 2016/679 eröffnet ist (vgl. Artikel 9 Absatz 1 Satz 2 der Richtlinie (EU 2016/680 für das Weiterverarbeiten von im sachlichen Anwendungsbereich der Richtlinie (EU 2016/680 erhobenen personenbezogenen Daten). Das Landesrecht setzt dies dahingehend um, dass sich der allgemeine datenschutzrechtliche Rahmen aus den Bestimmungen der Verordnung (EU) 2016/679, einschließlich der hierzu erlassenen Regelungen, ergibt.

2. Ziel

Es wird der Entwurf eines Gesetzes zum vollständigen Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen des bereichsspezifischen Datenschutzes im Justizvollzug und der Justizvollzugsgesetze des Landes vorgelegt (Gesetzentwurf).

Der Gesetzentwurf enthält in Artikel 1 - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (JVollzGB IV LSA) - eine Vollregelung des für den gesamten Justizvollzug (Strafvollzug, Jugendstrafvollzug, Untersuchungshaftvollzug, Jugendarrestvollzug und Vollzug der Sicherungsverwahrung) des Landes geltenden Datenschutzrechts, die weit überwiegend ohne externe Verweisungen auskommt, unter dem Ausschöpfen der bestehenden Regelungsspielräume bewährte Strukturen erhält, die Pflichten der Verantwortlichen konkretisiert, die bisherigen datenschutzrechtlichen Standards in ein neues eigenständiges Gesetz zum

Datenschutz im Justizvollzug des Landes überführt und zugleich die Vorgaben der Richtlinie (EU) 2016/680 vollständig in bereichsspezifisches Landesrecht umsetzt. Dies soll dem hohen Stellenwert des Datenschutzes im Justizvollzug und den Besonderheiten des Justizvollzuges im erforderlichen Umfang Rechnung tragen, die sehr komplexe Materie „Datenschutz“ anwendungsfreundlicher gestalten und so die Rechtssicherheit beim Anwender deutlich erhöhen.

Diese Verfahrensweise entspricht auch dem beabsichtigten Vorgehen des überwiegenden Teils der Länder, die auf der Grundlage des Musterentwurfes für ein Justizvollzugsdatenschutzgesetz, ebenfalls die Einführung eigenständiger Gesetze für den Datenschutz im Justizvollzug planen.

Der Strafvollzugsausschuss der Länder hat auf seiner 125. Tagung beschlossen, dass die Richtlinie (EU) 2016/680 für das Verarbeiten personenbezogener Daten für Zwecke des Justizvollzuges gilt und setzte eine länderübergreifende Arbeitsgruppe unter Federführung der Länder Berlin, Brandenburg und Schleswig-Holstein mit dem Auftrag ein, einen umfassenden Musterentwurf zum Umsetzen der Richtlinie (EU) 2016/680 im Justizvollzug zu erarbeiten. Unter Berücksichtigung der bisher hierzu in den Ländern bereits existierenden gesetzlichen Grundlagen erhielt die Arbeitsgruppe zudem den Auftrag, auch Bestimmungen zum Datenabgleich des Justizvollzuges mit den Behörden mit Sicherheitsaufgaben zu erarbeiten.

Auf seiner 126. Tagung hat der Strafvollzugsausschuss der Länder beschlossen, dass die Arbeitsgruppe auch den Informationsaustausch zwischen den Behörden mit Sicherheitsaufgaben und der Justiz in den Musterentwurf aufnehmen und Verbesserungen des Datenaustausches und der Zusammenarbeit zwischen den Justizvollzugsbehörden der Bundesländer und den Mitgliedstaaten der Europäischen Union bei sicherheitsrelevanten Gefangenen prüfen soll.

Die Konferenz der Justizministerinnen und Justizminister hat im November 2017 beschlossen, den länderübergreifenden Informations- und Datenaustausch der Justizvollzugsbehörden weiter zu entwickeln. Zudem wurde der Strafvollzugsausschuss der Länder beauftragt, in der von ihm eingesetzten Arbeitsgruppe Wege auch zu prüfen, ob das Austauschen vollzugsspezifischer Erkenntnisse über Gefangene aus Vorinhaftierungen in anderen Bundesländern verbessert werden kann.

Der Strafvollzugsausschuss der Länder hat auf seiner 127. Tagung den Musterentwurf zur Kenntnis genommen und hält die zum Umsetzen der Richtlinie (EU) 2016/680 erarbeiteten Bestimmungen für eine geeignete Grundlage zum Erarbeiten entsprechender Landesregelungen. Zudem hat er die von der Arbeitsgruppe vorgestellten Regelungen zum Datenabgleich mit den Behörden mit Sicherheitsaufgaben, welche nach Diskussion der bisher bestehenden landesgesetzlichen Bestimmungen und entsprechender Entwürfe erarbeitet worden sind, zur Kenntnis genommen und die Arbeitsgruppe beauftragt, Vorschläge zu der bisher im Musterentwurf ausgesparten Frage, ob das Austauschen vollzugsspezifischer Erkenntnisse über Gefangene aus Vorinhaftierungen in anderen Bundesländern verbessert werden kann, zu erarbeiten.

Der Gesetzentwurf berücksichtigt die wesentlichen Inhalte des Musterentwurfes zum Umsetzen der Richtlinie (EU) 2016/680 und Entwürfe anderer Länder zum bereichsspezifischen Datenschutz im Justizvollzug. Er orientiert sich zudem an den aktuellen

Novellierungen des Datenschutzrechts außerhalb des Justizvollzuges des Landes [vgl. Entwurf eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zum Regeln der Datenschutzaufsicht im Bereich des Verfassungsschutzes)].

Artikel 1 des Gesetzentwurf - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (JVollzGB IV LSA) - enthält u. a. Vorschriften über die allgemeinen Grundsätze des Verarbeitens personenbezogener Daten, die Rechtsgrundlagen einzelner Formen des Verarbeitens personenbezogener Daten, die Rechte betroffenen Personen, die Pflichten der Justizvollzugsbehörden und etwaiger Auftragsverarbeiter, das Bestellen behördlicher Datenschutzbeauftragter bei den Justizvollzugsbehörden und Regelungen über Schadensersatz und Sanktionen beim rechtswidrigen Verarbeiten personenbezogener Daten. Neu aufgenommen werden einige für die Vollzugspraxis erforderliche Regelungen, unter anderem Vorschriften zum Durchführen einer Sicherheitsanfrage über Gefangene und anstaltsfremde Personen, deren Ziel es ist, extremistische Einstellungen der betroffenen Personen zu erkennen, die zunächst nicht erkennbar sind. Eine Sicherheitsanfrage kann dabei durch eine auch technikgestützte Anfrage der Justizvollzugsbehörden beispielsweise beim Landeskriminalamt und dem Verfassungsschutz des Landes erfolgen. Die bislang in den einzelnen Justizvollzugsgesetzen des Landes Sachsen-Anhalt enthaltenen Abschnitte mit Vorschriften zum Datenschutz werden aufgehoben.

Artikel 2 und 3 des Gesetzentwurfes nehmen hierzu die erforderlichen Änderungen und korrespondierenden Anpassungen in den Justizvollzugsgesetzen vor. Damit werden alle von der Richtlinie (EU) 2016/680 geforderten Regelungen entsprechend deren inhaltlicher Vorgaben erlassen. Weil ein vollständiges bereichsspezifisches Umsetzen der Richtlinie (EU) 2016/680 im Justizvollzug erfolgt, sind Verweisungen in allgemeines Datenschutzrecht des Landes nicht erforderlich.

Artikel 4 des Gesetzentwurfes sieht das Inkrafttreten des Gesetzes vor. Mit Blick auf das erforderliche, umfassende Umstellen und Anpassen, der im Justizvollzug bereits verwendeten automatisierten Verarbeitungssysteme, wurde von der in Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 zu den Protokollierungspflichten eröffneten Option Gebrauch gemacht. Das in § 16 des Gesetzentwurfes enthaltene, verpflichtende Protokollieren einzelner Vorgänge des Verarbeitens personenbezogener Daten gilt erst frühestens ab dem 6. Mai 2023 und tritt demzufolge auch erst zu diesem Zeitpunkt in Kraft.

Insgesamt werden mit dem Gesetzentwurf alle Justizvollzugsgesetze des Landes Sachsen-Anhalt, einschließlich des neuen Gesetzes zum Datenschutz im Justizvollzug, geordnet und formell in die neue Systematik von vier Büchern des Justizvollzugsgesetzbuches Sachsen-Anhalt überführt, wobei alle Bücher - Erstes, Zweites, Drittes und Viertes Buch - des Justizvollzugsgesetzbuches Sachsen-Anhalt [JVollzGB I (Vollzug der Freiheitsstrafe, Jugendstrafe, Untersuchungshaft, Strafarrest), JVollzGB II (Vollzug der Sicherungsverwahrung), JVollzGB III (Vollzug des Jugendarrestes) und JVollzGB IV LSA (Datenschutz im Justizvollzug) weiterhin materiellrechtlich eigenständige Regelungswerke darstellen.

3. Grundzüge des Vierten Buches Justizvollzugsgesetzbuch Sachsen-Anhalt

3.1 Allgemeine Bestimmungen für das Verarbeiten personenbezogener Daten

Der Gesetzentwurf hebt in seinen allgemeinen Bestimmungen die zentralen Grundsätze für ein rechtmäßiges Verarbeiten personenbezogener Daten im Justizvollzug hervor, das zu einem bestimmten Zweck im Rahmen der jeweiligen Aufgabenwahrnehmung der Justizvollzugsbehörden und nach den Grundsätzen der Erforderlichkeit und der Datensparsamkeit zu erfolgen hat. Die Justizvollzugsbehörden dürfen Daten nur verarbeiten, wenn das Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder die Gefangenen oder andere betroffene Personen in das Verarbeiten ihrer personenbezogenen Daten einwilligen. Der Entwurf erkennt damit an, dass auch ein Gefangener über seine personenbezogenen Daten in erster Linie selbst bestimmen darf, soweit dies mit den Aufgaben des Vollzuges in Einklang zu bringen ist. Die Betonung des Einwilligens entspricht dem Ziel der Vollzugsgesetze, die Selbstverantwortung zu stärken. Der Gesetzentwurf betont den hohen Stellenwert des Datengeheimnisses, dem gerade im Vollzug mit den oft einschneidenden Folgen für die Lebensführung der Gefangenen und der Wirkung in der Öffentlichkeit eine wichtige Schutzfunktion zufällt. Dementsprechend sind alle Personen, die Zugang zu personenbezogenen Daten im Justizvollzug haben, auf das Einhalten des Datengeheimnisses förmlich zu verpflichten.

Der Gesetzentwurf regelt an zentraler Stelle außerdem die Verantwortung für das Erheben personenbezogener Daten und trägt damit den Bestimmungen der Richtlinie (EU) 2016/680 Rechnung, die klare Verantwortlichkeiten für die Einhaltung der datenschutzrechtlichen Bestimmungen zum Schutz der Rechte der betroffenen Personen verlangt.

3.2 Rechtsgrundlagen für das Verarbeiten personenbezogener Daten

Der Gesetzentwurf legt in dem zentralen Abschnitt die allgemeinen Rechtsgrundlagen für das Verarbeiten personenbezogener Daten fest. Um das bisherige hohe datenschutzrechtliche Schutzniveau beizubehalten, eine möglichst hohe Anwenderfreundlichkeit und Rechtssicherheit zu erzielen, greift der Gesetzentwurf zwar auf den neuen zentralen Verarbeitungsbegriff der Richtlinie (EU) 2016/680 zurück, setzt aber dennoch weit überwiegend das bewährte begriffliche Unterscheiden der einzelnen Verarbeitungsvorgänge fort. Ausgehend von den möglichen Datenverarbeitungsvorgängen legt der Gesetzentwurf zunächst die Voraussetzungen für das rechtmäßige Erheben personenbezogener Daten fest. Auch hier gilt wie im bisherigen Recht der Grundsatz des direkten Erhebens, wonach die erforderlichen Daten bei der betroffenen Person selbst und nur im Ausnahmefall bei Dritten erhoben werden sollen. In Einklang mit der Richtlinie (EU) 2016/680 sieht der Gesetzentwurf aber eine Einschränkung dieses Grundsatzes für das Erheben bei anderen öffentlichen Stellen vor. Dafür enthält der Gesetzentwurf neue Bestimmungen, welche die Rechte der Gefangenen klar regeln.

Die Richtlinie (EU) 2016/680 enthält unterschiedliche Anforderungen für die Zulässigkeit des Erhebens personenbezogener Daten, je nachdem, ob es sich um personenbezogene Daten oder um personenbezogene Daten besonderer Kategorien handelt. Letztere dürfen nur erhoben und verarbeitet werden, wenn dies zum Erreichen

des jeweiligen Verarbeitungszwecks unbedingt erforderlich ist. Diese Anforderungen an den Erforderlichkeitsmaßstab setzt der Gesetzentwurf in zahlreichen Bestimmungen um.

Eine entscheidende Bedeutung misst der Gesetzentwurf der Zweckbindung beim Verarbeiten personenbezogener Daten im Justizvollzug bei. Erhobene Daten dürfen grundsätzlich zu vollzuglichen Zwecken verarbeitet werden. Sollen Daten zu anderen als nach diesem Gesetz anerkannten Zwecken verarbeitet oder Dritten gegenüber offengelegt werden, liegt eine Zweckänderung vor, für die weitere gesetzliche Anforderungen gelten. Auch insoweit enthält die Richtlinie (EU) 2016/680 Vorgaben für die nationalen Rechtsvorschriften. Außerdem sind die Anforderungen aus der verfassungsgerichtlichen Rechtsprechung zum Bundeskriminalamtsgesetz (vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) umzusetzen. Aufgrund der vielfältigen Aufgaben des Vollzuges und seiner Vernetzung mit anderen staatlichen Stellen, die mit den Justizvollzugsbehörden zusammenwirken, wird der häufigste Fall einer Zweckänderung das Offenlegen personenbezogener Daten gegenüber öffentlichen Stellen sein, das ausführlich in Abschnitt 4, Unterabschnitte 3 und 4 des Gesetzentwurfes geregelt wird.

Die Vorschriften enthalten besondere Bestimmungen beispielsweise bei Verlegungen, Überstellungen und Vorinhaftierungen von Gefangenen und umfasst auch den Austausch personenbezogenen mit anderen Ländern. Dies entspricht dem Bedürfnis, sicherheitsrelevante Informationen der Justizvollzugsbehörden für vollzugliche Zwecke nutzen zu können, unabhängig davon, in welchem Bundesland die Gefangenen inhaftiert worden sind und setzt den Beschluss der Konferenz der Justizministerinnen und Justizminister der Länder vom 9. November 2017 um, den Austausch personenbezogener Daten im Justizvollzug zwischen den Ländern zu verbessern.

Im Übrigen werden bewährte Bestimmungen über die Informationsgewährung übernommen und im neuen Recht getrennt nach Opfern und Dritten geregelt. Dadurch soll der Opferschutz hervorgehoben und weiter akzentuiert werden Für das Offenlegen gegenüber nicht öffentlichen Stellen wurde im Gesetzentwurf eine eigene gesetzliche Befugnisnorm eingefügt, die die wichtigsten Anwendungsfälle aus der Praxis aufnimmt und die unübersichtliche Vorgängernorm des § 132 JVollzGB LSA anwenderfreundlich auflöst.

3.3 Besondere Bedingungen beim Verarbeiten personenbezogener Daten

Um den besonderen Bedingungen beim Verarbeiten personenbezogener Daten, auch mit Blick auf das Umsetzen der Richtlinie (EU) 2016/680 Rechnung zu tragen, enthält der Gesetzentwurf (Abschnitt 4) besondere Bedingungen - Auftragsverarbeiter, Funktionsübertragung, Verarbeiten nach Weisung, Gemeinsame Verantwortliche, Elektronische Akte, Zentrales Datei-, Buchhaltungs- und Abrechnungssystemsystem Einrichten automatisierter Verfahren, Verantwortung und Verordnungsermächtigung - für das Verarbeiten personenbezogener Daten.

3.4 Informationsaustausch zwischen den Justizvollzugsbehörden, den Justizbehörden und den Behörden mit Sicherheitsaufgaben im Rahmen von Fallkonferenzen

Der Gesetzentwurf enthält zudem erstmals die notwendigen Rechtsgrundlagen zum Verarbeiten personenbezogener Daten im Rahmen von sog. Fallkonferenzen, wo unterschiedliche Stellen aus Gründen der Entlassungsvorbereitung bei gefährlichen Gefangenen an einem Tisch zusammenkommen. Die Justizvollzugsbehörden dürfen Fallkonferenzen, je nachdem, welcher vollzugliche Zweck verfolgt oder welcher Gefahr entgegengewirkt werden soll, mit den Behörden mit Sicherheitsaufgaben (bspw. mit den Polizeibehörden des Bundes und der Länder oder dem Verfassungsschutz des Bundes und der Länder) unter Einbeziehung von Organen der Rechtspflege wie den Vollstreckungsbehörden, den Sozialen Diensten der Justiz oder forensischen Ambulanzen durchführen. Das gegenseitige Offenlegen personenbezogener Daten der Gefangenen dient gerade in diesen Fällen vorwiegend dem Zweck der Gefahrenabwehr. Aus diesem Grund sind für die Wissenserweiterung unter den Behörden die verfassungsrechtlichen Vorgaben, wie sie in der Rechtsprechung des Bundesverfassungsgerichts Ausdruck finden, zu beachten. Der Gesetzentwurf setzt auch insoweit die neuere verfassungsgerichtliche Rechtsprechung zur Antiterrordatei (BVerfG, Urteil des Ersten Senats vom 24. April 2013, 1 BvR 1215/07) und zum Bundeskriminalamtgesetz (BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) um.

3.5 Rechte der betroffenen Personen

Der Gesetzentwurf enthält außerdem im Umsetzen der Richtlinie (EU) 2016/680 in § 67 eine zentrale Vorschrift, die die Rechte der betroffenen Personen ausweist. Der Gesetzentwurf benennt dadurch eindeutige subjektiv-öffentliche Rechte, mit denen die betroffenen Personen Benachrichtigungen und Auskünfte über das Verarbeiten ihrer personenbezogenen Daten und demzufolge auch das Durchsetzen der Ansprüche auf das Berichtigen, Löschen und Vernichten oder Einschränken des Verarbeitens ihrer personenbezogenen Daten verlangen können.

3.6 Technische Schutzanforderungen und Protokollieren des Verarbeitens

Die Richtlinie (EU) 2016/680 verlangt Garantien, mit denen die Datenschutzgrundsätze zum Schutz der Rechte der Gefangenen und anderer betroffener Personen umgesetzt werden. Der Gesetzentwurf sieht daher in Anlehnung an die bisherige Rechtslage das Umsetzen des Standard-Datenschutzmodells vor, das um weitere technische Schutzstandards ergänzt wird. Die Eintrittswahrscheinlichkeit und die Schwere der mit dem Verarbeiten personenbezogener Daten verbundenen Risiken für das Recht auf informationelle Selbstbestimmung der betroffenen Personen sind auf der Grundlage eines Sicherheitskonzeptes der Justizvollzugsbehörden zu ermitteln und zu dokumentieren.

3.7 Prüfen, Löschfristen und Einschränken des Verarbeitens

Der Gesetzentwurf setzt die neuen Vorgaben der Richtlinie (EU) 2016/680 für das Prüfen der Notwendigkeit des Weiterverarbeitens, zur Angabe angemessener Löschfristen und das Einschränken des Verarbeitens personenbezogener Daten um. Per-

sonenbezogene Daten über Gefangene sind fünf Jahre nach dem Entlassen der Gefangenen zu löschen und zu vernichten. Im Vollzug der Jugendstrafe verkürzt sich diese Frist auf drei Jahre und beim Jugendarrest auf zwei Jahre. An die Stelle des Löschens und Vernichtens personenbezogener Daten kann das Einschränken ihres Verarbeitens treten, wenn die personenbezogenen Daten für fest umrissene Zwecke weiter aufbewahrt werden müssen. Personenbezogene Daten Dritter sind grundsätzlich zu löschen und zu vernichten, soweit sie für vollzugliche Zwecke nicht mehr erforderlich sind. Es wird weiterhin sichergestellt, dass die Gefangenenpersonalakten solange aufbewahrt werden dürfen, wie es die Verordnung zur Ausführung des Gesetzes zur Aufbewahrung von Schriftgut der Justiz im Land Sachsen-Anhalt (Justizaufbewahrungsverordnung - JAufbVO) vom 16. Juni 2009, zuletzt geändert durch Verordnung vom 13. April 2015 (GVBl. LSA S. 90) oder andere Archivvorschriften es verlangen.

3.8 Offenlegen durch Einsehen von Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern

Mit § 42 des Gesetzentwurfes wurde eine neue Vorschrift aufgenommen, die den Mitgliedern einer Delegation des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT) das Recht einräumt, während eines Anstaltsbesuches in Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter einsehe zu dürfen, soweit dies für das Erfüllen der Aufgaben des Ausschusses erforderlich ist. Damit wird einer Forderung des CPT aus dem Jahr 2016 entsprochen, Maßnahmen zu ergreifen, damit Besuchsdelegationen des Ausschusses künftig unbeschränkt Personal- und Krankenakten von Gefangenen einsehen dürfen.
Aus Gründen der Klarstellung wurde geregelt, dass das identische Recht zum Einsehen von Akten im Rahmen von Anstaltsbesuchen auch für Mitglieder einer durch das Übereinkommen der Vereinten Nationen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe legitimierten Stelle gilt, auch wenn hierfür bereits eine Rechtsgrundlage in Artikel 14 Absatz 1 Buchstabe b und Artikel 20 Buchstabe b des Fakultativprotokolls zum Übereinkommen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe besteht.

B. Besonderer Teil

Zu Artikel 1 - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - Datenschutz im Justizvollzug - (JVollzGB IV LSA)

Die Bestimmungen dieses Gesetzes gehen als bereichsspezifische Sonderregelungen für den Datenschutz im Justizvollzug des Landes im Bereich der Richtlinie (EU) 2016/680 auch weiterhin dem Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt - DSG LSA) in der Fassung der Bekanntmachung vom 13. Januar 2016, zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Februar 2018 (GVBl. LSA S. 10) - vgl. § 3 Absatz 3 Satz 1 DSG LSA - und den Regelungen des Entwurfes eines Gesetzes zum Anpassen des Datenschutzrechtes in Sachsen-Anhalt an das Recht der Europäischen Union (DSAnpG EU LSA) sowie des Entwurfes eines Gesetzes zum Umsetzen der Richtlinie (EU) 2016/680 und zum Anpassen von bereichsspezifischen Datenschutzvorschriften an die Richtli-

nie (EU) 2016/680 und zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes (Drs. 7/3207) vor.

Zu Abschnitt 1 - Allgemeine Bestimmungen

Zu § 1 Anwendungsbereich

Die Vorschrift beschreibt den Anwendungsbereich des Gesetzes. Nach Nr. 7 ist dieses Gesetz auch auf die Haft nach § 127b Absatz 2, § 230 Absatz 2, §§ 236, 329 Absatz 3, § 412 Satz 1 und § 453c der Strafprozessordnung und nach Nr. 8 auf das einstweilige Unterbringen nach § 275a Absatz 6 Strafprozessordnung anwendbar. Auf die Zivilhaft ist dieses Gesetz nicht anwendbar. Hier gilt die Verordnung (EU) 2016/679 in Verbindung mit den einschlägigen Vorschriften des Strafvollzugsgesetzes (StVollzG) in der jeweiligen Fassung und den Vorschriften des Bundes zum Anpassen von Bundesrecht an die Verordnung (EU) 2016/679 unmittelbar. Für Regelungen des Verarbeitens personenbezogener Daten, die nicht in den Anwendungsbereich der Richtlinie oder des Unionsrechts fallen, gelten die Verordnung (EU) 2016/679 und die hierzu erlassenen Vorschriften.

Zu § 2 Vollzugliche Zwecke

Um die Rechtmäßigkeit des Verarbeitens personenbezogener Daten jederzeit zu gewährleisten, müssen die Zwecke des Verarbeitens eindeutig festgelegt sein (vgl. Erwägungsgrund 29 der Richtlinie (EU) 2016/680). Vor diesem Hintergrund definiert § 2 die konkreten, von den Justizvollzugsbehörden des Landes regelmäßig zu erreichenden vollzuglichen Zwecke und setzt damit auch Artikel 8 Absatz 2 der Richtlinie (EU) 2016/680 um, wonach im Recht der Mitgliedstaaten der europäischen Union die Zwecke des Verarbeitens personenbezogener Daten anzugeben sind. Erfolgt das Verarbeiten personenbezogener Daten zu einem der genannten Zwecke, unterfällt es stets dem Anwendungsbereich dieses Gesetzes.

Der umfassende, in den Nummern 1 bis 14 jedoch nicht abschließend enthaltene Katalog soll die Rechtsanwendung vereinfachen und damit die Rechtssicherheit aller im Justizvollzug handelnden Personen erhöhen. Dies trägt erheblich dazu bei, dass in dem sensiblen Bereich des Justizvollzuges dem Schutz personenbezogener Daten der betroffenen Person nicht nur ein besonders hoher Stellenwert eingeräumt wird, sondern dieser auch aufrechterhalten, sichergestellt und rechtssicher durchgesetzt werden kann. Alle in den Nummern 1 bis 14 aufgezählten vollzuglichen Zwecke dienen damit den Justizvollzugsbehörden unmittelbar dem Erfüllen ihrer Aufgaben im Rahmen der Strafvollstreckung im engeren Sinne. Das Erreichen der Vollzugsziele der Gefangenen kann je nach Art der einzelnen Freiheitsentziehung (Freiheitsstrafe, Jugendstrafe, Untersuchungshaft, Jugendarrest oder Sicherungsverwahrung) unterschiedlich sein. Im Jugendarrestvollzug umfasst dies auch den Zweck, den Jugendlichen das von ihnen begangene Unrecht und ihre Verantwortung hierfür bewusst zu machen Hilfen für eine Lebensführung ohne Straftaten aufzuzeigen. Der vollzugliche Zweck der „Erreichen des Vollzugsziels“ nimmt auf das Ziel der Freiheitsentziehung Bezug, wie es sich aus dem jeweils geltenden Vollzugsgesetz ergibt. Der Zweck des Erreichens des Vollzugsziels umfasst beispielswiese auch die Gesundheitsfürsorge, die Beschäftigung sowie alle weiteren mit der Freiheitsentziehung in unmittelbarem Zusammenhang stehenden Aspekte.

Auch das Verarbeiten personenbezogener Daten der ehrenamtlichen oder anderer an der Behandlung und Betreuung der Gefangenen mitwirkenden Personen und ihre Tätigkeit im Vollzug dient der Fortentwicklung der vollzuglichen Behandlungsmaßnahmen und fällt daher unter das Erreichen des Vollzugsziels der Gefangenen, soweit nicht im konkreten Fall ein anderer vollzuglicher Zweck einschlägig ist.

Das Erreichen der jeweiligen Vollzugsziele steht auch in unmittelbarem Zusammenhang mit dem Vorbereiten und Durchführen von nachsorgenden Maßnahmen, die an das Entlassen der Gefangenen anknüpfen. Durch einen Austausch personenbezogener Daten zwischen den beteiligten öffentlichen und nicht öffentlichen Stellen soll der reibungslose Übergang in die Freiheit sowie die Zeit nach dem Entlassen der Gefangenen für diesen erleichtert werden, so dass auch dieser Zweck als vollzuglicher Zweck im Sinne dieses Gesetzes erfasst ist.

Die Justizvollzugsbehörden müssen sich regelmäßig in gerichtlichen Verfahren und gegenüber den Strafvollstreckungsbehörden u. a. zum Vollzugsverhalten und zum Behandlungs- und Betreuungsstand der Gefangenen erklären. Vollzuglicher Zweck ist daher auch das Erfüllen der den Justizvollzugsbehörden durch Gesetz oder auf Grund eines Gesetzes übertragenen sonstigen Aufgaben durch das Mitwirken in entsprechenden Verfahren, insbesondere durch das regelmäßige Abgeben von Stellungnahmen.

Personenbezogenen Daten werden auch zum Erstellen von Statistiken, insbesondere zum Evaluieren der vollzuglichen Maßnahmen verarbeitet, soweit ihr Anonymisieren oder Pseudonymisieren nicht möglich ist. Dieser allein aus dem Erreichen der Vollzugsziele der Gefangenen abgeleitete Verarbeitungszweck wird nunmehr ausdrücklich als vollzuglicher Zweck im Sinne dieses Gesetzes aufgeführt.

Nummer 15 enthält als Generalklausel eine Aufzählung von Auffangtatbeständen, u. a. den vollzuglichen Zweck der Resozialisierung, also die Befähigung des Gefangenen in Zukunft ein Leben in sozialer Verantwortung ohne Straftaten zu führen. Dieser Vollzugszweck ist sowohl völker- als auch europarechtlich verankert (vgl. Regel Nr. 88 der VN-Mindestgrund-sätze für die Behandlung der Gefangenen, „Nelson-Mandela-Regeln“ und Nr. 102.1 der Europäischen Strafvollzugsgrundsätze) als auch auf nationaler Ebene verfassungsrechtlich geboten. Des Weiteren ist auch der vollzugliche Zweck des Schutzes der Allgemeinheit vor weiteren Straftaten der Gefangenen enthalten, der sich sowohl unmittelbar auf die Haftzeit, als auch auf die Zeit nach dem Entlassen der Gefangenen bezieht (Legalprognose).

Die vollzuglichen Zwecke der Resozialisierung der Gefangenen und des Schutzes der Allgemeinheit vor weiteren Straftaten der Gefangenen stehen dabei immer in unmittelbarem Zusammenhang. Nur eine gelungene Resozialisierung gewährleistet zugleich auch den umfassenden Schutz der Allgemeinheit. Beides dient letztlich auch der Sicherheit der Bevölkerung des Landes. Der Staat kommt dieser Schutzpflicht in ganz besonderem Maße nach, in dem er die Resozialisierung von den Gefangenen fordert, aber auch fördert. Auch der aufgeführte vollzugliche Zweck des Schutzes von Leib, Leben, Freiheit und Vermögen der Bediensteten und der Gefangenen, sowie des Vermögens des Landes durch das Aufrechterhalten der Sicherheit und Ordnung innerhalb der Anstalten. dient dem Aufrechterhalten von Sicherheit und Ordnung im Justizvollzug und steht ebenfalls im Einklang und unmittelbarem Zusammenhang mit dem Ziel der Resozialisierung. Der ebenfalls enthaltene vollzugli-

che Zweck des Verhinderns des Befreiens und Entweichens der Gefangenen dient dem Durchsetzen des staatlichen Strafanspruchs gegenüber den Gefangenen. Gleiches gilt für den vollzuglichen Zweck des Vermeidens einer Nichtrückkehr und des Missbrauchs von Lockerungen oder anderen vollzugsöffnenden Maßnahmen, wobei hier auch die Resozialisierung der Gefangenen wieder wirksam wird, weil die Gefangenen stufenweise an ein Leben in Freiheit herangeführt und erprobt werden sollen, und in den Fällen ihrer unerlaubten Abwesenheit aus den Anstalten und ihrem Wiederergreifen nach dem Entweichen oder nach der unerlaubten Abwesenheit.

Im Untersuchungshaftvollzug und den gleichgestellten Freiheitsentziehungen kommt dem vollzuglichen Zweck der Resozialisierung keine eigenständige Bedeutung zu. Hier ist es das vorrangige inhaltliche Ziel der Justizvollzugsbehörden, durch ihr Mitwirken beim Umsetzen und Durchsetzen von Anordnungen der Strafvollstreckungsbehörden und des gesetzlichen Richters bei den Strafgerichten, jederzeit das Durchführen eines sicheren und geordneten Strafverfahrens zu gewährleisten.

Zu § 3 Begriffsbestimmungen

§ 3 enthält die Begriffsbestimmungen, die für das Verständnis dieses Gesetzes und seiner Systematik wesentlich sind. Sie dienen zum Teil dem Umsetzen von Artikel 3 der Richtlinie (EU) 2016/680.

Nummer 1 definiert den Begriff „Gefangene“ als Personen, an denen Freiheitsentziehungen nach § 1 vollzogen werden. Personen, gegen die Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft vollstreckt wird, werden nicht erfasst. Für sie gelten die Bestimmungen des Strafvollzugsgesetzes (§§ 179 ff. StVollzG).

Nummer 2 definiert den Begriff der „Anstalten“ und stellt damit klar, dass damit alle Einrichtungen des Justizvollzuges umfasst werden sollen, in denen Freiheitsentziehungen nach § 1 vollzogen werden können.

Nummer 3 definiert den Begriff „Justizvollzugsbehörde“ und stellt damit sicher, dass alle Einrichtungen des Justizvollzuges, in denen personenbezogene Daten betroffener Personen verarbeitet werden können, auch ausdrücklich vom Anwendungsbereich dieses Gesetzes erfasst werden und ggf. auch Verantwortlicher (z. B. IT-Leitstelle für den Justizvollzug oder das für den Justizvollzug zuständige Ministerium) sein kann.

Nummer 4 definiert den Begriff „personenbezogenen Daten“ als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und führt auch den Begriff „betroffene Person“ ein. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren vgl. Erwägungsgrund 21 der Richtlinie (EU) 2016/680.

Nummer 5 definiert den Begriff „Verarbeiten“ mit oder ohne Hilfe automatisierter Verfahren und benennt Fallbeispiele (vgl. Erwägungsgrund 34 der Richtlinie (EU) 2016/680).

Das Gesetz behält das in Abschnitt 22 des JVollzGB LSA enthaltene, differenzierte Trennen der einzelnen Vorgänge des Verarbeitens personenbezogener Daten bei. Vor diesem Hintergrund definiert Nummer 6 den Begriff „Weiterverarbeiten“ durch das Negativabgrenzen zu Nummer 5.

Nummer 7 definiert den Begriff „Einschränken des Verarbeitens“, Nummer 8 „Profiling“ im Sinne der Richtlinie (EU) 2016/680. Nummer 9 definiert den Begriff „Anonymisieren“, Nummer 10 das „Pseudonymisieren“ und Nummer 11 übernimmt den Begriff „Verschlüsseln“ aus dem DSG LSA.

Die Nummern 12 bis 16 definieren in dieser Reihenfolge die Begriffe „Dateisystem“, „Verantwortliche“, „Auftragsverarbeiter“, „Empfänger“ und „Verletzen des Schutzes personenbezogener Daten“ im Sinne der Richtlinie (EU) 2016/680. Nummer 17 definiert den Begriff „personenbezogene Daten besonderer Kategorien“ und zählt hierzu in den Buchstaben a bis e die Begriffe „genetische Daten“, „biometrische Daten“, „Gesundheitsdaten“ und „Daten zum Sexualleben oder zur sexuellen Orientierung“ auf. Bei der hier gewählten Formulierung handelt es sich im Verhältnis zu dem in der Richtlinie (EU) 2016/680 verwendeten Begriffspaar „besondere Kategorien personenbezogener Daten“ um eine sprachliche Anpassung, die klarstellt, dass es um das Verarbeiten personenbezogener Daten einer betroffenen Person und nicht um das Verarbeiten von „Kategorien“ geht. In den Nummern 18 bis 20 werden die Begriffe aus Nummer Buchstabe a bis c - „genetische Daten“, „biometrische Daten“ und „Gesundheitsdaten“ selbst erläutert und in Nummer 21 der Begriff „internationale Organisation“ definiert.

Der Begriff „Einwilligen“ wird in der Richtlinie (EU) 2016/680 selbst nicht näher definiert. Die in Nummer 22 aufgenommene Definition entspricht der Definition in Artikel 4 Nummer 11 der Verordnung (EU) 2016/679. Ein Bekunden des Willens der betroffenen Person ist im Sinne dieser Begriffsbestimmung in informierter Weise erfolgt, wenn sie im Vorfeld vollständig über alle relevanten Umstände aufgeklärt worden ist. Nummer 23 definiert den Begriff „anstaltsfremde Person“. Die Definitionen der öffentlichen und nicht öffentlichen Stellen in den Nummern 24 und 25 wurden aus § 2 Absatz 1, 2 und 4 des Bundesdatenschutzgesetzes übernommen. Ergänzend wurden in Nummer 24 c) die Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Mitgliedstaates der Europäischen Union aufgenommen, um zu verdeutlichen, dass nicht nur inländische öffentliche Stellen, sondern auch die öffentlichen Stellen anderer Mitgliedstaaten der Europäischen Union von der Definition umfasst sind und ein Offenlegen personenbezogener Daten gegenüber diesen grundsätzlich möglich ist.

Dies entspricht auch Erwägungsgrund Nummer 93 der Richtlinie (EU) 2016/680, wonach die Grundrechte und die Grundfreiheiten der betroffenen Personen zu schützen sind, aber auch der ungehinderte und direkte Austausch personenbezogener Daten der betroffenen Person im Verkehr zwischen den Behörden innerhalb der Europäischen Union zu gewährleisten ist. Aus diesem Grund enthält bereits die Zielbestimmung von Artikel 1 Absatz 2 Buchstabe b der Richtlinie (EU) 2016/680 die Grundlage für einen direkten Austausch personenbezogener Daten zwischen den Justizvollzugsbehörden der Mitgliedstaaten der Europäischen Union. Nummer 26 übernimmt den Begriff „Aufsichtsbehörde“ aus Artikel 3 Nummer 15 der Richtlinie (EU) 2016/680.

Zu Abschnitt 2 - Grundsätze des Verarbeitens personenbezogener Daten

Zu § 4 Allgemeine Grundsätze

Die Vorschrift dient dem Umsetzen von Artikel 4 Absatz 1 der Richtlinie (EU) 2016/680. Sie führt allgemeine Grundsätze des Verarbeitens personenbezogener Daten, die in Teilen an mehreren Stellen dieses Gesetzes noch einmal aufgenommen und konkretisiert werden, an zentraler Stelle zusammen. Absatz 1 hebt das Recht der betroffenen Personen auf informationelle Selbstbestimmung besonders hervor, welches durch dieses Gesetz oder einer anderen aufgrund Gesetzes erlassenen Rechtsvorschrift eingeschränkt werden kann.

Zu § 5 Andere Zwecke

Satz 1 setzt Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 um und stellt klar, dass die Justizvollzugsbehörden als Behörden mit Gesamtaufgaben personenbezogene Daten so lange und so weit zu anderen Zwecken weiterverarbeiten dürfen, so lange es sich bei diesen anderen Zwecken um vollzugliche Zwecke handelt und das Weiterverarbeiten erforderlich und verhältnismäßig ist. Dabei wird von der vom EU Gesetzgeber in Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 eröffneten Möglichkeit Gebrauch gemacht, personenbezogene Daten auch für andere vollzugliche Zwecke zu verarbeiten, wobei das Verarbeiten innerhalb der Bandbreite aller zur Verfügung stehenden vollzuglichen Zwecke nicht als Zweckänderung im Sinne dieses Gesetzes gilt. Satz 2 betrifft das Weiterverarbeiten personenbezogener Daten zu anderen in § 1 genannten und damit nach diesem Gesetz anerkannten Zwecken. Dies ist insbesondere zulässig, wenn es in diesem Gesetz oder einer anderen Rechtsvorschrift vorgesehen ist.

Zu § 6 Archivarische, wissenschaftliche oder statistische Zwecke

Die Vorschrift setzt Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 um. Die Justizvollzugsbehörden dürfen personenbezogene Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken verarbeiten, solange das Verarbeiten personenbezogene Daten unter die in § 1 genannten Zwecke fällt. Als Beispiel kann hier die kriminologische Forschung angeführt werden. Voraussetzung hierfür ist das Vorliegen geeigneter Vorkehrungen zugunsten der Rechtsgüter betroffener Personen. Hierzu können insbesondere das, gemessen am konkreten Forschungszweck, so zeitnah wie möglich erfolgende Anonymisieren personenbezogener Daten oder das räumliche und organisatorische Abtrennen der Forschung betreibenden Stellen gehören. Diese Vorkehrungen werden in einschlägigen Vorschriften dieses Gesetzes weiter ausdifferenziert.

Zu § 7 Unterscheiden verschiedener Kategorien von betroffenen Personen

Die Vorschrift dient dem Umsetzen von Artikel 6 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen des vorgesehenen Unterscheidens beim Verarbeiten personenbezogener Daten, etwa dem Unterscheiden entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Sicherheit personenbezogener Daten werden an späterer Stelle in diesem Gesetz aufgegriffen und konkretisiert.

Zu § 8 Unterscheiden zwischen auf Fakten basierenden und auf persönlichen zu Einschätzungen beruhenden personenbezogenen Daten

Die Vorschrift dient dem Umsetzen von Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen des vorgesehenen Unterscheidens personenbezogener Daten bei deren Verarbeiten, etwa dem Unterscheiden entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen zur Sicherheit personenbezogener Daten werden an späterer Stelle in diesem Gesetz aufgegriffen und konkretisiert.

Zu § 9 Automatisiertes Entscheiden im Einzelfall

Die Vorschrift setzt Artikel 11 der Richtlinie (EU) 2016/680 um und regelt das Verbot automatisierter, insbesondere auf Profiling basierender Einzelentscheidungen. Bei der in Absatz 1 genannten, nur unter bestimmten Umständen zulässigen „Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat“ dürfte es sich regelmäßig um einen Verwaltungsakt handeln. Interne Zwischenfestlegungen oder -auswertungen, die nur Ergebnis automatisierter Prozesse sind, fallen nicht hierunter.

Zu § 10 Überprüfen und Fristen

Die Vorschrift dient dem Umsetzen von Artikel 5 der Richtlinie (EU) 2016/680.

Zu § 11 Einwilligen der betroffenen Person

Die Vorschrift entspricht grds. § 125 JVollzGB LSA und stellt klar, dass im Justizvollzug auch das Einwilligen in das Verarbeiten personenbezogener Daten rechtserheblich sein kann, unabhängig davon, ob es durch Gefangene oder andere betroffene Personen erfolgt.

Entsprechendes lässt sich auch dem Erwägungsgrund Nummer 35 zur Richtlinie (EU) 2016/680 entnehmen, wonach das Einwilligen auch im Geltungsbereich der Richtlinie (EU) 2016/680 Grundlage des Verarbeitens personenbezogener Daten sein kann.

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

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

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

Absatz 4 orientiert sich an § 51 Absatz 4 des Bundesdatenschutzgesetzes. Das Einwilligen ist gemäß Satz 1 nur dann tragfähige Grundlage für das Verarbeiten personenbezogener Daten, wenn es auf der freien Entscheidung der Gefangenen oder einer anderen im Justizvollzug betroffenen Person beruht. Bei der Beurteilung, ob das Einwilligen freiwillig erteilt wurde, sind nach den allgemeinen Grundsätzen die Umstände des Einzelfalls maßgeblich, was in Absatz 1 Satz 2 zum Ausdruck kommt.

Dabei werden auch die besonderen Umstände der Freiheitsentziehung zu berücksichtigen sein. Die Vorschrift des Bundesdatenschutzgesetzes wurde hier noch dahingehend ergänzt, dass bei den Umständen des Einwilligens im Anwendungsbereich dieses Gesetzes insbesondere auch die besondere Situation der Freiheitsentziehung zu berücksichtigen ist. Diese beinhaltet regelmäßig ein besonderes Machtgefälle zwischen den Verantwortlichen des Verarbeitens personenbezogener Daten und betroffenen Personen. Von einem freiwilligen Erteilen ist aber regelmäßig dann auszugehen, wenn dieses besondere Machtgefälle das Entscheiden der betroffenen Personen 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.

Nach Erwägungsgrund Nummer 35 der Richtlinie (EU) 2016/680 kann von einem Einwilligen nur ausgegangen werden, wenn eine echte Wahlfreiheit der betroffenen Person vorliegt. Eine solche Wahlfreiheit soll nicht bestehen, wenn eine Behörde die betroffene Person auch anweisen kann, einer rechtlichen Verpflichtung zum Dulden des Erhebens personenbezogener Daten oder einem Mitwirken an diesem Erheben nachzukommen. Zugleich nennt Erwägungsgrund Nummer 35 aber auch Konstellationen, auch explizit für den Bereich der Strafvollstreckung (DNA-Tests, Aufenthaltsüberwachung mit elektronischer Fußfessel), in denen betroffene Personen in das Verarbeiten ihrer personenbezogenen Daten einwilligen können. Auch wenn in der Richtlinie (EU) 2016/680 außerhalb der Erwägungsgründe das Einwilligen - anders als in der Verordnung (EU) 2016/679 - nicht mehr erwähnt wird, ist es daher als Rechtsgrundlage des Verarbeitens personenbezogenen Daten möglich. Dies entspricht auch der Wertung des Bundesgesetzgebers, der in § 46 Nummer 17 und in § 51 des Bundesdatenschutzgesetzes, gesetzliche Regelungen für das Einwilligen geschaffen hat. in denen betroffene Personen in das Verarbeiten personenbezogener Daten wirksam einwilligen können.

Der Schutz personenbezogener Daten besonderer Kategorien stellt auch zusätzliche Anforderungen an die Wirksamkeit des Einwilligens, so dass Absatz 5 den Schutzgedanken des Artikels 10 der Richtlinie (EU) 2016/680 übernimmt. Die Vorschrift entspricht § 51 Absatz 5 des Bundesdatenschutzgesetzes, in den die Regelung des § 4a Absatz 3 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 2097) übernommen worden ist.

Nach Absatz 6 verbleibt bei dem Grundsatz, dass das Einwilligen nicht die Geschäftsfähigkeit betroffener Personen im Sinne der bürgerlich-rechtlichen Vorschriften voraussetzt.

Die Rechtsnatur des Einwilligens als rechtsgeschäftliche Erklärung oder als tatsächliches Einverständnis mit dem Eingriff in das Persönlichkeitsrecht ist umstritten (zum Streitstand s. Plath, BDSG/Verordnung (EU) 2016/679, 2. Auflage 2016, § 4 a BDSG, Rn. 7). Für die Wirksamkeit des Einwilligens wird zumindest die tatsächliche Einsichtsfähigkeit betroffener Personen vorliegen müssen. Bei Fehlen gegenteiliger Anhaltspunkte werden die Justizvollzugsbehörden regelmäßig vom Vorliegen der tatsächlichen Einsichtsfähigkeit ausgehen können. Diese Frage ist jeweils einzelfallbezogen zu beurteilen. Die gesetzlichen Vertreter (Eltern - §§ 1626 und 1629 BGB -, Vormünder - § 1793 BGB -, Betreuer - § 1902 BGB -, soweit dies zu ihrem Aufgabenkreis gehört, sowie Pfleger - § 1909 BGB -, soweit sich dies aus dem Text der Bestellung ergibt) treten in die Rechte der von ihnen vertretenen Gefangenen ein,

wenn diese nicht die für eine Entscheidung notwendige Einsichtsfähigkeit besitzen und vollzugliche oder andere nach diesem Gesetz anerkannte Zwecke hierdurch nicht gefährdet werden. Ihr Einbeziehen kann aber häufig für das Erreichen der nach diesem Gesetz anerkannten Zwecke erforderlich sein.

Die Bestimmung überträgt daher den Rechtsgedanken aus § 67 des Jugendgerichtsgesetzes (JGG) auf die datenschutzrechtlichen Bestimmungen im Justizvollzug, indem gesetzliche Vertreter hinsichtlich der genannten Rechte den Gefangenen gleichgestellt werden. Die Einschränkung, wonach vollzugliche Aufgaben hierdurch nicht gefährdet werden dürfen, dient dem Vermeiden des Missbrauchs.

Zu Abschnitt 3 - Sicherheit personenbezogener Daten

Zu § 12 Datengeheimnis

Absatz 1 Satz 1 entspricht § 150 Absatz 2 JVollzGB LSA und betrifft den Umgang Bediensteter mit personenbezogenen Daten. Auch im Justizvollzug gilt der Grundsatz, dass jeder Bedienstete nur auf solche personenbezogenen Daten zugreifen darf, die er für zum Erfüllen seiner Aufgaben braucht. Satz 2 übernimmt den Gedanken aus § 126 Satz 1 JVollzGB LSA und verdeutlicht die besondere Pflicht der Bediensteten zur Verschwiegenheit. Die Vorschrift richtet sich an alle unmittelbar in den Justizvollzugsbehörden beschäftigten Personen, unabhängig davon, ob die Tätigkeit mit Blick auf die 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. Satz 3 entspricht den §§ 126 Satz 2 und 135 Absatz 1 JVollzGB LSA und stellt sicher, dass Mitarbeiter nicht öffentlicher Stellen über ihre Pflicht zur Verschwiegenheit belehrt und auf das gewissenhafte Erfüllen 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.

Absatz 2 entspricht dem § 135 Absatz 2 und Absatz 3 dem § 135 Absatz 3 JVollzGB LSA.

In Absatz 4 werden die Regelungen aus § 151 JVollzGB LSA übernommen. Satz 1 erlaubt in engen Grenzen das Kenntlichmachen personenbezogener Daten von Gefangenen innerhalb der Anstalt. Personenbezogene Daten besonderer Kategorien dürfen nach Satz 2 nicht allgemein kenntlich gemacht werden.

Absatz 5 entspricht § 150 Absatz 1 JVollzGB LSA und dient dem sicheren Umgang mit personenbezogenen Daten in Akten, um so einen unbefugten Zugang und Gebrauch auszuschließen. Satz 2 stellt für das Führen von Akten im Justizvollzug besondere Schutzvorkehrungen auf, um sicherzustellen, dass sich das Einsehen in die dort niedergelegten personenbezogenen Daten auf die hierzu berechtigten Bediensteten beschränkt und verlangt, dass für besonders sensible Teilbereiche besondere Akten anzulegen sind. Aufzeichnungen der Ärzte und Psychologen über medizinische Behandlungen oder über Therapien sind getrennt von anderen Akten zu führen und aufzubewahren und unterliegen nur dem Zugriff der jeweiligen Ärzte und Psychologen. Gleichzeitig wird bestimmt, dass die Gefangenenpersonalakten in Teil- oder Unterbänden untergliedert werden sollen (etwa für Gutachten oder Disziplinar-

verfahren) damit auch so ein differenzierter Zugriff auf bestimmte Informationen ermöglicht wird.

Absatz 6 stellt als Abschluss der Neuregelung durch die Übernahme von § 126 Satz 3 JVollzGB LSA klar, dass das Datengeheimnis und die dazu korrespondierenden Pflichten auch nicht durch das Beenden der Tätigkeit enden.

Zu § 13 Technische und organisatorische Maßnahmen

Die Vorschrift setzt Artikel 19, 20 und 29 der Richtlinie (EU) 2016/680 um, welche die Vorgaben zu den Pflichten des Verantwortlichen, zum Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen sowie zur Sicherheit des Verarbeitens personenbezogener Daten betreffen und führt diese als Sicherheitsvorschriften des Datenschutzes im Justizvollzug an zentraler Stelle zusammen.

Absatz 1 entspricht im Wesentlichen dem Wortlaut von Artikel 20 Absatz 2 der Richtlinie (EU) 2016/680. Die Justizvollzugsbehörden haben sicherzustellen, dass durch Voreinstellungen jeweils nur die personenbezogenen Daten verarbeitet werden, deren Verarbeiten nach dem jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

In Absatz 2 werden Artikel 19, Artikel 20 Absatz 1 und Artikel 29 Absatz 1 der Richtlinie (EU) 2016/680 zusammengeführt und umgesetzt.

Absatz 3 enthält einen Anforderungskatalog, der dem Standarddatenschutzmodell entspricht und geeignet ist, die Datenschutzgrundsätze, insbesondere den des Datenminimierens wirksam umzusetzen und sicherstellt, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden.

Die Gewährleistungsziele des Standarddatenschutzmodells lassen sich den Anforderungen der Richtlinie (EU) 2016/680 zuordnen (vgl. Schlehahn, DuD 2018, 32, 36). Sie setzen neben den Artikeln 19, 20 und 29 Absatz 1 außerdem die Artikel 4, 5, 8 bis 14, 16 bis 18, 22, 24, 25, 28, 30 und 31 der Richtlinie (EU) 2016/680 um. Das Umsetzen der Maßnahmen kann jede Justizvollzugsbehörde eigenverantwortlich festlegen. Erfolgt das Verarbeiten personenbezogener Daten über das elektronische Buchhaltungs- und Abrechnungssystem im Strafvollzug (BASIS-WEB) wird das Umsetzen der erforderlichen organisatorischen und technischen Maßnahmen regelmäßig durch das Teilnehmen an diesem System erfüllt sein. BASIS-WEB ermöglicht alle Funktionalitäten, die für das Umsetzen der genannten Maßnahmen erforderlich sind, beispielsweise ein komplexes Rollen- und Rechtesystem. Das tatsächliche Zuordnen der einzelnen Rechte und Rollen bleibt insoweit Aufgabe der zuständigen Behördenleitungen.

Absatz 4 dient dem Umsetzen von Artikel 29 Absatz 2 der Richtlinie (EU) 2016/680. Satz 1 benennt die Ziele, die im Hinblick auf das automatisierte Verarbeiten personenbezogener Daten durch das Etablieren geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen. Nach Satz 2 können die Zwecke der Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle und Zugriffskontrolle insbesondere durch das Verwenden von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

Absatz 5 sieht, 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), sondern das Durchführen einer Datenschutzfolgenabschätzung vor. Da das bisherige Schutzniveau nicht unterschritten werden soll, sollte eine Datenschutzfolgenabschätzung bereits im Rahmen des Fortschreibens der bestehenden Sicherheitskonzepte in den Anstalten stattfinden. Die Vorschrift setzt die Vorgaben aus Artikel 20 Absatz 1 und Artikel 29 Absatz 1 der Richtlinie (EU) 2016/680 um, wonach der für das Verarbeiten personenbezogener Daten die Verantwortlichen die Eintrittswahrscheinlichkeit und die Schwere der mit dem Verarbeiten personenbezogener Daten verbundenen Risiken zu bewerten und auf dieser Grundlage die erforderlichen technischen und organisatorischen Maßnahmen ergreifen.

Absatz 6 trägt der Anforderung aus Artikel 19 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 Rechnung, wonach die getroffenen Maßnahmen erforderlichenfalls überprüft und aktualisiert werden müssen. Dabei sind im Rahmen der Angemessenheit auch die mit der Maßnahme verbundenen Kosten zu berücksichtigen („Kosten-Nutzen-Analyse“).

Zu § 14 Datenschutzfolgenabschätzung

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

Absatz 1 dient dem Umsetzen von Artikel 27 der Richtlinie (EU) 2016/680. Die Datenschutzfolgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes. Die Voraussetzungen zum Durchführen einer Datenschutzfolgenabschätzung können nur unvollkommen gesetzlich konkret ausgestaltet werden. So lässt sich dennoch feststellen, dass hinsichtlich des Umfangs des Verarbeitens personenbezogener Daten nicht das Einzelverarbeiten, sondern lediglich das Verwenden maßgeblicher Systeme und Verfahren zum Verarbeiten personenbezogener Daten mithilfe einer Datenschutzfolgenabschätzung vorab in den Blick genommen werden müssen. Insoweit lässt sich, abseits der prozeduralen Verbindung, eine Vergleichbarkeit mit den Voraussetzungen des Durchführens eines Anhörens des Landesbeauftragten für den Datenschutz begründen. Kriterien für die Entscheidung, ob das vorgesehene Verarbeiten personenbezogener Daten qualitativ erhöhte Risiken für die Rechtsgüter betroffener Person in sich birgt, können beispielsweise der Kreis betroffener Personen, die Art der zum Erheben personenbezogener Daten eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit dem Verarbeiten verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein. Die Konkretisierung der in Absatz 1 genannten Voraussetzungen obliegt letztlich der vollzuglichen Praxis. Bei diesem Konkretisierungsvorgang wird allerdings zu beachten sein, dass die entstehenden Aufwände angemessen und beherrschbar bleiben müssen. Ferner ist festzuhalten, dass das Erfordernis einer Datenschutzfolgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden gilt.

Absatz 2 Absatz 2 nimmt Artikel 35 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 und Absatz 3 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 Datenschutzfolgenabschätzung fest und konkretisiert die in Artikel 27

Absatz 2 der Richtlinie (EU) 2016/680 enthaltenen allgemeinen Angaben unter Übernahme der Angaben aus Artikel 35 Absatz 7 der Verordnung (EU) 2016/679.

Entgegen der Regelung in § 67 des Bundesdatenschutzgesetzes enthält die Bestimmung keine Verpflichtung der Verantwortlichen zum Durchführung einer Überprüfung, ob das Verarbeiten personenbezogener Daten den Maßgaben folgt, die sich aus der Datenschutzfolgenabschätzung ergeben haben. Diese Verpflichtung gibt die Richtlinie (EU) 2016/680 gerade nicht vor.

Zu § 15 Verzeichnis von Verarbeitungstätigkeiten

Die Vorschrift dient dem Umsetzen von Artikel 24 der Richtlinie (EU) 2016/680 und verpflichtet die Justizvollzugsbehörden und Auftragsverarbeiter, wie schon jetzt § 14 Absatz 3 DSG LSA, zum Führen eines Verzeichnisses über die bei ihnen durchgeführten Tätigkeiten zum Verarbeiten personenbezogener Daten. Dieses in Teilen über den bisherigen Umfang nach § 14 Absatz 3 DSG LSA hinausgehende Verzeichnis dient vor allem dem Landesbeauftragten für den Datenschutz dazu, einen Überblick über das bei den Verantwortlichen durchgeführte Verarbeiten personenbezogene Daten zu erhalten. Dies ermöglicht es ihm, seine Aufgaben und Befugnisse im Hinblick auf den jeweiligen Verantwortlichen zielgerichtet, effizient und verhältnismäßig auszurichten und zu nutzen. Die Beteiligung des Landesbeauftragten für den Datenschutz wird arrondiert und ergänzt durch die interne Beratungs- und Kontrolltätigkeit des behördlichen Datenschutzbeauftragten und die Regelung zum umfassenden Zugang zu personenbezogenen Daten und den Vorgängen ihres Verarbeitens.

In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit „Kategorien von Datenverarbeitungstätigkeiten“ stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Vorgänge des Verarbeitens personenbezogener Daten bezieht, sondern auf sinnvoll abgrenzbare und kategorisierbare Teile des bei den Justizvollzugsbehörden durchgeführten Verarbeitens personenbezogener Daten bezieht. Es kann sich anbieten, die nach Satz 1 Nummer 2 aufzunehmenden Angaben zu den Zwecken des Verarbeitens an den gesetzlichen Aufgabenzuschreibungen der betreffenden öffentlichen Stelle auszurichten. Satz 2 übernimmt die bisher in § 14 Absatz 4 Nummer 1 DSG LSA enthaltene Regelung.

Absatz 2 verpflichtet auch Auftragsverarbeiter, ein Verzeichnis, wenngleich in geringerem Umfang, auch für das Verarbeiten personenbezogene Daten zu führen.

In Absatz 3 werden Aussagen zur Form des Verzeichnisses und dessen Führen getroffen. Die bisherige Regelung in § 14 Absatz 3 DSG LSA wird fortgeschrieben. Damit wird auch für die Zukunft bestimmt, dass jedenfalls bei automatisierten Verfahren je Dateisystem ein Verzeichniseintrag zu erstellen ist.

Nach Absatz 4 ist das Verzeichnis und seine Aktualisierungen dem Landesbeauftragten für den Datenschutz auf Anfrage zur Verfügung zu stellen.

Zu § 16 Protokollieren des Verarbeitens personenbezogener Daten

Die Vorschrift dient dem Umsetzen von Artikel 25 der Richtlinie (EU) 2016/680, statuiert die umfassende Pflicht der Justizvollzugsbehörden und des Auftragsverarbeiters

zum Protokollieren des jeweils unter seiner Verantwortung durchgeführten Verarbeitens personenbezogener Daten und ermöglicht so die Kontrolle der Rechtmäßigkeit der Vorgänge des Verarbeitens personenbezogener Daten der betroffenen Person. Absatz 1 regelt in Umsetzung von Artikel 25 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 eine Pflicht zum Protokollieren von bestimmten Vorgänge des Verarbeitens personenbezogener Daten in automatisierten Verarbeitungssystemen. Die Vorgaben der Richtlinie (EU) 2016/680 wurden im Katalog in Nummer 2 um das Speichern personenbezogener Daten und in Nummer 7 um das Einschränken des Verarbeitens personenbezogener Daten ergänzt. Die Regelung erfasst unter anderem auch das Protokollieren des automatisierten Übertragens an Schnittstellen von Verfahren zu anderen Verfahren sowie Verarbeitungsvorgängen durch den Administrator. Ebenfalls erfasst wird das Protokollieren „lesender Zugriffe“, also, wenn Informationen aus dem Verarbeitungssystem i. S. des Artikels 25 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 abgefragt werden (vgl. Herbst-Kühling/Buchner, DS-GVO/BDSG, Art. 4 DS-GVO Rn. 27; Schaffland/Wiltfang, DS-GVO/BDSG, Art. 4 DS-GVO Rn. 74; a. A. vgl. Schild - BeckOK Datenschutzrecht, Art. 4 DS-GVO Rn. 47; Ernst in Paal/Pauly, DS-GVO/BDSG, Art. 4 DS-GVO Rn. 28). Absatz 2 enthält konkrete Vorgaben an 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 werden muss und sich daraus die Begründung für die Verarbeitungsvorgänge ableiten lassen sollte. Das Protokollieren „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 des Abfragens oder Offenlegens personenbezogener Daten 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 dem Aufrechterhalten der Datensicherheit verwendet werden. Das Protokollieren dieser Daten 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 EuGHs 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 des Verarbeitens personenbezogener Daten nachzuvollziehen. Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) ausgeführt, durch technische und organisatorische Maßnahmen müsse sichergestellt sein, dass die Protokolldaten der oder dem Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und das Protokollieren 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.

In Absatz 5 wird festgelegt, dass die Protokolle dem Datenschutzbeauftragten und dem Landesbeauftragten für den Datenschutz zum Zweck der Datenschutzkontrolle zur Verfügung stehen müssen. Die Vorschrift setzt Artikel 25 Absatz 3 der Richtlinie (EU) 2016/680 um.

Zu § 17 Melden von Verstößen

Die Vorschrift dient dem Umsetzen von Artikel 48 der Richtlinie (EU) 2016/680. Die Justizvollzugsbehörden haben im Zusammenhang mit dem Melden von Verstößen sowohl interne Meldungen als auch Hinweise betroffener Personen oder sonstiger Dritter in den Blick zu nehmen. Für beide Stränge bietet sich als Kontakt- und Beratungsstelle sowohl der Leiter der Justizvollzugsbehörde oder eine von ihm hierzu beauftrage Person oder der behördliche Datenschutzbeauftragte selbst an.

Zu Abschnitt 4 - Rechtsgrundlagen des Verarbeitens personenbezogener Daten

Abschnitt 4 enthält als zentraler Abschnitt die Rechtsgrundlagen der einzelnen Vorgänge des Verarbeitens personenbezogener Daten und trennt im Wesentlichen die einzelnen Vorgänge des Erhebens, des Weiterverarbeitens, des Offenlegens, des Löschens und Vernichtens, des Einschränkens und des Berichtigens personenbezogener Daten betroffener Personen voneinander ab. Durch die Vielfalt der Vorschriften werden die Zwecke, Verbote und Gebote entsprechend den Richtlinienvorgaben so eindeutig formuliert, dass es dem Rechtsanwender ermöglicht wird, eine differenzierte, übersichtliche und sichere Handhabung des komplexen Datenschutzbereiches vorzunehmen und gerade im sensiblen Bereich „Justizvollzug“ das hohe Schutzniveau, das der Gesetzgeber bereits mit Verabschiedung des JVollzGB LSA im Bereich des Datenschutzes im Justizvollzug eingeführt hat, statuiert und manifestiert wird.

Zu Unterabschnitt 1 - Erheben personenbezogener Daten

Zu § 18 Zulässigkeit des Erhebens personenbezogener Daten

Die Vorschrift entspricht mit sprachlichen Anpassungen an die Richtlinie (EU) 2016/680 dem § 127 JVollzGB LSA und enthält den Grundsatz der Zulässigkeit des Erhebens personenbezogener Daten. Nach Absatz 1 ist das Erheben personenbezogener Daten zulässig, soweit dies für die in § 1 in Verbindung mit § 2 definierten vollzuglichen Zwecke erforderlich ist.

Absatz 2 trägt der besonderen Schutzbedürftigkeit personenbezogener Daten besonderer Kategorien Rechnung. Die damit verbundene gesteigerte Persönlichkeitsrelevanz, wie sie auch das Bundesverfassungsgericht betont (BVerfGE 115, 320,348), und die damit verbundene gesteigerte Intensität von Eingriffen in das Persönlichkeitsrecht betroffener Personen, lassen das Verarbeiten de personenbezogenen Daten nur unter engen Voraussetzungen zu. Die Fallgruppen des Absatzes 2 knüpfen

an die bisherige Regelung des § 127 Absatz 2 JVollzGB LSA an und setzen Artikel 10 Buchstabe a) bis c) der Richtlinie (EU) 2016/680 um.

Zu § 19 Erheben personenbezogener Daten bei der betroffenen Person

Die Vorschrift entspricht mit sprachlichen Anpassungen an die Richtlinie (EU) 2016/680 dem § 128 JVollzGB LSA und enthält den Grundsatz der Zulässigkeit des Erhebens personenbezogener Daten bei der betroffenen Person selbst.

Absatz 1 behält den Grundsatz des direkten Erhebens personenbezogener Daten bei und ist damit unmittelbar Ausfluss des Grundrechts auf informationelle Selbstbestimmung, da die betroffene Person wissen können soll, wer sich für ihre personenbezogenen Daten interessiert.

Nach Absatz 2 trägt die, die personenbezogenen Daten erhebende Stelle die Verantwortung dafür, dass die betroffene Person über den Zweck des Erhebens ihrer personenbezogenen Daten und ihre dazu korrespondierenden Rechte in Kenntnis gesetzt werden. Nur so können sie im Rahmen der ihnen eingeräumten Möglichkeiten selbstbestimmt über den Umgang mit ihren personenbezogenen Daten entscheiden, darauf Einfluss nehmen oder sich informieren.

Absatz 3 regelt die Voraussetzungen, unter denen auch ohne Kenntnis, also ohne Mitwirken der betroffenen Person, ausnahmsweise das Erheben personenbezogener Daten zulässig ist, nämlich dann, wenn keine Anhaltspunkte vorliegen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Insofern haben die Justizvollzugsbehörden eine Abwägung vorzunehmen. Als Beispiele kommen hier u. a. die durch Bedienstete geführten Beobachtungsbögen bei suizidgefährdeten Gefangenen in Betracht sowie Arbeitsplatzkontrollen im offenen Vollzug bei Freigängern.

Zu § 20 Erheben personenbezogener Daten über Gefangene bei Dritten

Die Vorschrift entspricht, mit redaktionellen und sprachlichen Anpassungen an die Richtlinie (EU) 2016/680 sowie der Erweiterung des Kataloges in Absatz 1 um die Nummern 7 und 8, dem § 129 JVollzGB LSA, enthält den Grundsatz der Zulässigkeit des Erhebens personenbezogener Daten über Gefangene bei Dritten und setzt somit auch Artikel 6 der Richtlinie (EU) 2016/680 um.

Absatz 1 nennt die Voraussetzungen für das Erheben personenbezogener Daten über einwilligungsfähige Gefangene ohne deren Kenntnis und Mitwirken bei Dritten. Diese Art des Erhebens personenbezogener Daten greift stärker in die Rechte der Gefangenen ein als dies beim Erheben bei ihnen selbst der Fall wäre. Aus diesem Grunde bindet Absatz 1 diese Art des Erhebens an die strengen, im Justizvollzug aber auch erforderlichen Voraussetzungen, der Nummern 1 bis 8.

Absatz 2 erweitert die Befugnis zum Erheben personenbezogener Daten um die Möglichkeit, diese auch ohne Kenntnis der Gefangenen bei ihren gesetzlichen Vertretern zu erheben, wenn sie nicht die für das Einwilligen notwendige Einsichtsfähigkeit besitzen. Im Hinblick auf die personenbezogenen Daten besonderer Kategorien müssen ggf. kumulativ zusätzlich die Voraussetzungen des § 18 Absatz 2 vorliegen.

Aufgrund der Tatsache, dass das Erheben personenbezogener Daten bei Dritten in der Regel ohne das Mitwirken und damit ohne Kenntnis der Gefangenen einen starken Eingriff in die Rechtsposition der Gefangenen bedeutet, müssen die Justizvollzugsbehörden nicht öffentliche Stellen nach Absatz 3 darüber aufklären, aufgrund welcher Rechtsvorschrift eine Auskunftsverpflichtung besteht, andernfalls auf die Freiwilligkeit der Auskunft. Nur so ist sichergestellt, dass die nicht öffentlichen Stellen in eigener Verantwortung entscheiden können, ob und in welchem Umfang sie eine Auskunft erteilen wollen oder nicht erteilen.

Zu § 21 Erheben personenbezogener Daten über Personen, die keine Gefangenen sind

Die Vorschrift entspricht, mit redaktionellen und sprachlichen Anpassungen an die Richtlinie (EU) 2016/680, dem § 130 JVollzGB LSA und regelt in Satz 1 das Erheben personenbezogener Daten über Personen, welche keine Gefangenen sind, wie beispielsweise Angehörige, Freunde oder andere nahestehende Personen. Gleichzeitig wird Artikel 6 der Richtlinie (EU) 2016/680 umgesetzt. Zum Erreichen 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 betroffener Personen gesprochen werden. Die Vorschrift ermöglicht sowohl das Erheben personenbezogener Daten bei den Gefangenen als auch das Erheben personenbezogener Daten bei Dritten oder Stellen außerhalb des Justizvollzuges. Sie enthält damit ein weiteres Durchbrechen des Grundsatzes des Direkterhebens bei der betroffenen Person, bindet das Erheben personenbezogener Daten aber an enge, aber auch erforderliche Voraussetzungen. Aufgrund der Tatsache, dass das Erheben personenbezogener Daten für das Erreichen der vollzuglichen Zwecke unbedingt erforderlich ist und gleichzeitig das Abwägen mit den schutzwürdigen Interessen der betroffenen Person erfolgt, ist gewährleistet, dass sich die Eingriffe in die Rechte Dritter im Rahmen der Verhältnismäßigkeit bewegen.

Im Hinblick auf die personenbezogenen Daten besonderer Kategorien müssen ggf. kumulativ noch die Voraussetzungen des § 18 Absatz 2 vorliegen. Nach Satz 2 hat der Vollzug nichtöffentliche Stellen darüber aufzuklären, aufgrund welcher Rechtsvorschrift sie zu einer Auskunft verpflichtet sind, andernfalls auf die Freiwilligkeit der erbetenen Auskunft hinzuweisen. Nur so ist sichergestellt, dass die nichtöffentlichen Stellen in eigener Verantwortung entscheiden können, ob sie eine Auskunft erteilen wollen oder nicht erteilen.

Zu § 22 Identifizieren von Gefangenen und anstaltsfremden Personen

Das zweifelsfreie Klären der Identität eines Gefangenen und einer anstaltsfremden Person ist für den Justizvollzug notwendig, um Identitätsverwechselungen 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 Vollzugs- und Eingliederungsplanung zu gewährleisten, bedarf es des zweifelsfreien Feststellens der Identität von Gefangenen. Darüber hinaus ist das zweifelsfreie Feststellen der Identität aller Gefangenen notwendig, um die Sicherheit und Ordnung der Anstalten zu gewährleisten. Zahlreiche Maßnahmen zu deren Aufrechterhalten, Durchsetzen und Wiederherstellen wie beispielsweise das regelmäßige Überprüfen der Gefangenen nach § 24 oder das Austauschen personenbezoge-

ner Daten mit den Behörden mit Sicherheitsaufgaben setzen voraus, dass die Identität der betroffenen Person zweifelsfrei geklärt ist. Darüber hinaus dient das Erheben personenbezogener Daten zum Feststellen der Identität des Gefangenen der Sicherung des Vollzuges, indem namentlich etwa das Fahnden und Wiederergreifen von Gefangenen im Fall der Flucht ermöglicht werden. Auch gilt es, irrtümliche Entlassungen zu verhindern. Schließlich sollen die Justizvollzugsbediensteten alle Gefangenen identifizieren können, um so einen sicheren und reibungslosen Vollzugsalltag zu gewährleisten. Absatz 1 regelt deshalb die zulässigen erkennungsdienstlichen Maßnahmen, um die Identität des Gefangenen feststellen zu können. Verbleiben Zweifel, erfolgt nach Absatz 2 ein Abgleich mit dem Landeskriminalamt, dem Bundeskriminalamt, oder dem Bundesamt für Migration und Flüchtlinge auf Grundlage der erhobenen personenbezogenen Daten.

Absatz 1 regelt abschließend die zulässigen erkennungsdienstlichen Maßnahmen zum Erheben von personenbezogener Daten der Gefangenen. Dies ist zulässig zu vollzuglichen Zwecken. Insoweit wird § 2 Nummer 2 des Gesetzes in Bezug genommen. Als vollzuglicher Zweck hervorgehoben wird das Gewährleisten der Sicherheit und Ordnung der Anstalten. Als weiterer Zweck wird das Feststellen der Identität des Gefangenen genannt, die letztlich aber den vorgenannten Zwecken gleichsam als Sekundärzweck dient.

Aus der Fassung „sind […] zulässig“ ergibt sich, dass die Justizvollzugsbehörden 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 „zu vollzuglichen Zwecken“ durchgeführt werden dürfen, kann die Ermessensentscheidung auf eine Vielzahl von Gründen gestützt werden. Zumindest das Aufnehmen 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. Das Begrenzen auf Gefangene mit einer bestimmten Mindestvollzugsdauer ist im Gesetz nicht angelegt. Im Rahmen der Ermessensausübung ist der Grundsatz der Erforderlichkeit zu beachten. Das Erheben der personenbezogenen 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) oder das Anfertigen neuer Lichtbilder gerechtfertigt ist. Aus der Natur der Regelung 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 jedoch ermessensleitende Standardisierungen für den Vollzugsalltag nicht aus.

Das Aufnehmen 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 ihrem technischen Herstellen 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 „biometrischen Daten“, wenn sie mit speziellen technischen Mitteln verarbeitet werden. Lichtbilder werden folglich nicht per se den besonderen Regelungen biometrischer Daten unterwor-

fen, sondern nur dann, wenn sie genutzt werden, um aus ihnen physische, physiologische oder verhaltenstypische 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 Gesichtsfelderkennung dem Absatz 1 Nummer 4. Die Schriftprobe eines Gefangenen unterfällt der Nummer 4 nicht. Absatz 1 Nummer 5 erlaubt das Erheben biometrischer Merkmale. Zu den körperlichen biometrischen Merkmalen gehören beispielsweise die Gesichtsform, die Augennetzhaut, die Stimme, die Handgeometrie oder die Venenstruktur. Das biometrische Erheben 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 regelmäßig und erfolgreich angewendet. Auch wenn es sich um sehr sensible personenbezogene Daten handelt, kann der Einsatz im erforderlichen Umfang für die betroffene Person 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. Diese personenbezogenen Daten dürfen nur mit Kenntnis des Gefangenen erhoben werden. Insoweit wird der Verhältnismäßigkeitsgrundsatz konkretisiert.

Handelt es sich bei den personenbezogenen Daten um solche besonderer Kategorien, ist § 18 Absatz 2 zu beachten. Das Erheben dieser personenbezogenen Daten muss zu den zugelassenen Zwecken unbedingt erforderlich, also im konkreten Einzelfall unerlässlich sein. Das Abgleichen personenbezogener Daten nach Absatz 2 darf nur erfolgen, wenn Zweifel an der Identität eines Gefangenen bestehen und die Maßnahme zu deren Feststellen erforderlich ist.

Die personenbezogenen Daten, die zum Feststellen der Identität offengelegt werden dürfen, ergeben sich abschließend aus Absatz 1 und § 24 Absatz 3. In der Folge dürfen nur Grunddaten wie beispielsweise Nachname, Geburtsname, Vorname, Geburtsdatum, Geschlecht, Geburtsort, Geburtsland, Staatsangehörigkeit, Aliaspersonen, zum Feststellen der Identität gefertigte Lichtbilder, Finger- und Handflächenabdrücke, festgestellte äußere körperliche Merkmale, Messungen, biometrische Merkmale von Fingern, Händen, Gesicht, Augen, der Stimme und die erfasste Unterschrift offengelegt werden. Als Schwelle legt Absatz 2 Satz 1 „Zweifel an der Identität“ eines Gefangenen fest. Damit orientiert sich die Vorschrift an der Rechtsprechung des Bundesverfassungsgerichts, wonach das Offenlegen von Grunddaten ausschließlich zum Zweck des Feststellens der Identität nicht zu beanstanden ist, wenn es sich um Einzelabfragen handelt und ein konkreter Anlass für das Offenlegen personenbezogener Daten besteht (vgl. BVerfG, Urteil des Ersten Senats vom 24. April 2013 - 1 BvR 1215/07, Randnummern 192 ff.). Als Empfänger nennt Absatz 2 Satz 1 das Landeskriminalamt. Dieses Vorgehen soll einheitlich in allen Ländern etabliert werden. Die Regelung wirkt insoweit als Befugnisnorm für das Landeskriminalamt. Sie ermächtigt sowohl zum Abgleichen personenbezogener Daten als auch zum Offen-

legen des Ergebnisses an die Justizvollzugsbehörden zum Zweck des Identifizierens. Das Weiterverarbeiten der offengelegten personenbezogenen Daten wird durch Absatz 1 Satz 2 folglich auf das Identifizieren der Gefangenen beschränkt. Zu einem darüberhinausgehenden Austauschen von ermittlungs- oder handlungsleitenden Informationen ermächtigt Absatz 2 nicht. Hierfür bedarf es eines Vorgehens nach Maßgabe anderer Bestimmungen. Handelt es sich bei den personenbezogenen Daten um solche besonderer Kategorien, ist deren Weiterverarbeiten für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligen der betroffenen Personen nur zulässig, soweit dies zu einem der in § 29 Absatz 2 genannten Zwecke unbedingt erforderlich ist.

Satz 3 erweitert den Kreis der Behörden, gegenüber denen personenbezogene Daten zum Zweck des Feststellens der Identität offengelegt und die um einen Datenabgleich ersucht werden dürfen auf das Bundeskriminalamt und auf das Bundesamt für Migration und Flüchtlinge. Da es sich bei um eine landesrechtliche Regelung handelt, muss die Befugnis zum Datenabgleich und zum Offenlegen des Ergebnisses des Datenabgleichs an die Justizvollzugsbehörden aus dem jeweiligen Fachrecht der Bundesbehörden folgen.

Zum Gewährleisten der Sicherheit und Ordnung der Anstalten, namentlich um die Kontrolle von Besuchsverboten und der Verhinderung des Entweichens durch das Verwechseln und Austauschen von Gefangenen mit anderen Personen (z. B. Besucher) zu ermöglichen, sieht Absatz 3, der dem § 147 Absatz 1 JVollzGB LSA entspricht, zum Feststellen der Identität, neben der Angabe der Personalien und dem Nachweis durch amtliche Ausweise, die Möglichkeit vor, unter engen Voraussetzungen die genannten biometrischen Merkmale von vollzugsfremden Personen zu erheben.

Die Anstalt ist eine zum Feststellen der Identität berechtigte Behörde im Sinne von § 2 Abs. 2 des Personalausweisgesetzes (PAuswG) und kann nach § 1 Abs. 1 S. 3 und 4 PAuswG u. a. das Hinterlegen des Personalausweises, für die Dauer des Aufenthaltes in einer Anstalt verlangen und der betroffenen Person ermöglichen, nach § 18 Abs. 1 S. 1 PAuswG ihren Personalausweis dazu zu verwenden, ihre Identität gegenüber der Anstalt auch elektronisch nachzuweisen. Das Erheben biometrischer Merkmale stellt einen nicht unerheblichen Eingriff in die informationelle Selbstbestimmung dar und darf nach Abs. 3 Nr. 2 nur erfolgen, soweit dies zum Verhindern des Verwechselns und des Austauschens von Gefangenen, insbesondere beim Verlassen der Anstalten mit anderen Personen erforderlich und soweit es sich um personenbezogene Daten besonderer Kategorien handelt, unbedingt erforderlich, also unerlässlich, ist.

Zu § 23 Sicherheitsrelevante Erkenntnisse über Gefangene und anstaltsfremde Personen

Der Justizvollzug wird zunehmend als Teil der Sicherheitsarchitektur der Länder verstanden. Namentlich der Umgang mit extremistischen Gefangenen und Gefangenen, die der organisierten Kriminalität zuzuordnen sind, stellt die Behörden mit Sicherheitsaufgaben und die Justizvollzugsbehörden vor besondere Herausforderungen.

Der Informationsaustausch mit den Behörden mit Sicherheitsaufgaben ist hierbei von zentraler Bedeutung, um die Sicherheit der Anstalten zu gewährleisten, um eine auf

den einzelnen Gefangenen und seine Bedürfnisse abgestimmte Vollzugs- und Eingliederungsplanung zu ermöglichen, um weitergehende Radikalisierungen und Gefährdungen der Vollzugsziele bei anderen Gefangenen zu verhindern und um die Behörden mit Sicherheitsaufgaben bei fortbestehender Gefahr in das Vorbereiten des Entlassens wirksam einbinden zu können. Namentlich zu nennen sind insoweit das Unterbringen von Gefangenen in einer anderen Abteilung, das Verlegen und Überstellen der Gefangenen, das Veranlassen des Teilnehmens an Deradikalisierungsprogrammen, das Kontrollieren von Besuchen und des Schriftverkehrs und die unter dem Einbeziehen der Behörden mit Sicherheitsaufgaben erfolgende Eingliederungsplanung und in Fallkonferenzen.

Die §§ 23 ff. sind in einem systematischen Zusammenhang, insbesondere mit den §§ 22, 29 bis 38 zu lesen. Diese ermöglichen es den Justizvollzugsbehörden, die Identität von Gefangenen und anstaltsfremden Personen sicher festzustellen. Speziell die §§ 23 ff. ermöglichen dann den Austausch personenbezogener Daten mit den Behörden mit Sicherheitsaufgaben, um weitere Informationen beispielsweise zum jeweiligen Gefangenen zu erlangen und gegebenenfalls eine hierauf abgestimmte Vollzugsplanung vornehmen zu können. Es besteht insofern ein gestufter Dreiklang aus dem Feststellen der Identität, gegebenenfalls durchzuführender Sicherheitsanfrage und Fallkonferenz bei fortbestehender Gefährlichkeit. Daneben besteht die Möglichkeit des punktuellen Informationsaustauschs nach den §§ 29 und 34.

Nach Satz 1 prüfen die Justizvollzugsbehörden nach Maßgabe der §§ 24 und 25, ob sicherheitsrelevante Erkenntnisse über Gefangene und anstaltsfremde Personen, die Zugang zu den Justizvollzugsanstalten begehren, vorliegen. Satz 1 ist als programmatischer Auftrag vor allem an die Anstalten zu verstehen, bei Gefangenen und anstaltsfremden Personen stets eine sicherheitsbezogene Überprüfung nach § 24 und § 25 vorzunehmen. Davon unberührt bleibt, dass § 24 und § 25 ein Absehen von einem Überprüfen zulassen können, zum Beispiel, wenn die Sicherheitsanfrage im Ermessen der Justizvollzugsbehörden steht. Der Begriff der anstaltsfremden Person ist in § 3 Nummer 23 definiert.

Satz 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 Prüfkompetenz der Anstalten aus dem nachfolgenden § 25 wird dahingehend erweitert, dass nach Satz 3 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 § 24 Überprüfen von Gefangenen

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

Die „drohende Gefahr“ begründet die Schwelle für den mit der Sicherheitsanfrage verbundeneren Eingriff in das Recht auf informationelle Selbstbestimmung der Gefangenen.

Die Gefahrenprognose muss tatsachengestützt sein und darf sich nicht auf Vermutungen und allgemeine Erfahrungssätze stützen. Sie ist der konkreten Gefahr im polizeirechtlichen Sinne vorgelagert. Nicht das Verletzen des Schutzgutes „Sicherheit der Anstalten“ muss drohen, sondern eine Gefahr hierfür („Gefahr der Gefahr“). Es müssen folglich tatsächliche Anhaltspunkte für das Entstehen einer konkreten Gefahr für die Sicherheit der Anstalten bestehen. Der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehbar sein, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für die Sicherheit der Anstalten hindeuten. Ausreichend ist, dass ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, aus dem heraus die Verletzung der Sicherheit der Anstalten resultieren könnte. Nur relativ diffuse Anhaltspunkte für mögliche Gefahren sind 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. In der Folge ist auch ein Offenlegen personenbezogener Daten, um überhaupt erst herauszufinden, ob eine Gefahr droht, ausgeschlossen. Die Sicherheitsanfrage erfolgt mit Blick darauf, dass der Gefangene sich nicht freiwillig im Justizvollzug aufhält, nicht verdachtsunabhängig. 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“) Justizbehörden und Behörden mit Sicherheitsaufgaben bei Vorliegen einer drohenden Gefahr für die Sicherheit der Anstalten um Auskunft zu ersuchen. Zweck der Sicherheitsanfrage und des damit zusammenhängenden Datentransfers ist also der Schutz der Sicherheit der Anstalten vor einer drohenden Gefahr.

Zu den Behörden mit Sicherheitsaufgaben im Sinne dieser 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 Behörden mit Sicherheitsaufgaben in den Mitgliedstaaten der Europäischen Union. Beispiele für Justizbehörden sind Gerichte oder die Staatsanwaltschaften. Nach Satz 2 Nummer 1 dürfen die Justizvollzugsbehörden insbesondere eine Auskunft nach § 41 Absatz 1 Nummer 1 des Bundeszentralregistergesetzes (BZRG) anfordern. Nach Absatz 1 Satz 2 Nummer 2 und 3 dürfen auch sicherheitsrelevante Erkenntnisse der Polizeibehörden des Bundes und der Länder und der Verfassungsschutz des Landes angefragt werden. Entsprechend dem „Doppeltürmodell“ des Datenschutzrechtes gibt Absatz 1 Satz 1 und 2 nur die Befugnis zu einer Abfrage personenbezogener Daten. Satz 3 konkretisiert den Begriff der drohenden Gefahr nach 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 Freiheitsentziehung nicht zugrunde liegen sowie ein

Vollzugsverhalten bei früheren Freiheitsstrafen angesprochen. Demgegenüber ist eine drohende Gefahr für die Sicherheit der Anstalten nach den Erfahrungen des Justizvollzuges 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. Insoweit wirkt die Bestimmung auch konkretisierend bezogen auf Anfragen bei den Polizeibehörden des Bundes und der Länder nach Satz 1.

Absatz 3 regelt das mit der Sicherheitsanfrage im Zusammenhang stehende Offenlegen personenbezogener Daten durch die Justizvollzugsbehörden gegenüber den angefragten Stellen. Das Ersuchen muss nach Absatz 3 Satz 1 die personenbezogenen Daten, insbesondere die gesicherten Identitätsdaten umfassen. Absatz 3 ist insoweit in einem Zusammenhang mit den Normen dieses Gesetzes (z. B. § 22) zu lesen, die es den Justizvollzugsbehörden ermöglichen, die Identität eines Gefangenen sicher festzustellen. Über die Identitätsdaten hinaus sollen bekannt gewordene Aliaspersonalien, die voraussichtliche Vollzugsdauer sowie das Aktenzeichen der der Vollstreckung zugrundeliegenden Entscheidung mitgeteilt werden, um den angefragten Behörden eine sachhaltige Auskunft zu ermöglichen. Bei dem Offenlegen personenbezogener Daten nach Absatz 3 ist der enge Zweck des Offenlegens dieser personenbezogenen Daten, die Anfrage nach sicherheitsrelevanten Erkenntnissen, zu berücksichtigen.

Nach Absatz 4 teilen die beteiligten Behörden den Justizvollzugsbehörden ihre sicherheitsrelevanten Erkenntnisse über die Gefangenen mit.

Der Begriff der „sicherheitsrelevanten Erkenntnisse“ ist in § 23 näher bestimmt. Für die Polizei- und Verfassungsschutzbehörden des jeweiligen Landes bedeutet diese Norm eine Befugnis zum Offenlegen personenbezogener Daten an die jeweiligen Justizvollzugsbehörden. Mangels Gesetzgebungskompetenz ist die Bestimmung für sonstige Behörden als bloßer Programmsatz zu verstehen. Die Befugnis zum Offenlegen personenbezogener Daten muss aus dem jeweils einschlägigen 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 Anstalten ergeben, steht es im Ermessen der Justizvollzugsbehörden („dürfen“), zusätzliche Auskünfte oder Unterlagen bei den Justizbehörden und Behörden mit Sicherheitsaufgaben 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 Justizbehörden und Behörden mit Sicherheitsaufgaben begründet Absatz 5 keine Befugnis zum Offenlegen personenbezogener Daten. Diese müssen in den dortigen jeweils einschlägigen Fachgesetzen geregelt sein.

Absatz 6 bestimmt, dass die personenbezogenen Daten in gesonderten Akten oder Dateisystemen zu führen, das heißt zu verarbeiten sind. Hintergrund ist der besondere Schutz dieser personenbezogenen 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 Justizvollzugsbehörden zuvörderst dafür benötigt, Sicherheitsrisiken vor Ort aufzudecken und ihnen entgegentreten zu können. Stellt sich aber heraus, dass Gefangene etwa besondere Radikalisierungstendenzen oder besondere Gewaltproblematiken aufweisen, müssen die Anstalten in der Lage sein, die Gefangenen nicht nur zum Schutz Dritter sicher zu verwahren, sondern die Erkenntnisse auch im Besonderen für die weitere Vollzugs- und Eingliederungsplanung nutzen zu dürfen, nicht nur, um den Gefangenen zu helfen, sondern auch, um den Sicherheitsgefahren nachhaltig begegnen zu können. Beispielhaft zu nennen ist das Vermitteln der Gefangenen in spezifische Maßnahmenangebote zur Deradikalisierung oder zum Auseinandersetzen mit einer Gewaltproblematik. Es entspricht einer der wichtigsten Aufgabe des Justizvollzuges, die Allgemeinheit vor weiteren Straftaten der Gefangenen zu schützen, indem gefährlichen Gefangenen auf diese Klientel abgestimmte Behandlungsprogramme angeboten werden. Hierfür müssen die Justizvollzugsbehörden die im Rahmen der Sicherheitsanfrage gewonnenen Erkenntnisse weiterverarbeiten dürfen.

Zu § 25 Überprüfen von anstaltsfremden Personen

Absatz 1 Satz 1 statuiert den Grundsatz, dass anstaltsfremde Personen nur dann in den Anstalten tätig werden dürfen, wenn keine Sicherheitsbedenken bestehen. Der Begriff der anstaltsfremden Person ist in § 2 Nummer 20. 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 zu den Anstalten begehren. Beispielhaft zu nennen sind insoweit Handwerksbetriebe oder der Anstaltskaufmann. Beispiele für nicht berufliche Tätigkeiten sind das Ableisten eines freiwilligen Praktikums oder Tätigkeiten im Rahmen eines Ehrenamtes. Auch Honorarkräfte oder Mitarbeiter externer Organisationen und Vereine unterfallen der Regelung. Ein Schlechterstellen anstaltsfremder Personen oder gar Misstrauen ist damit in keiner Weise verbunden, da auch für die Justizvollzugsbediensteten selbst entsprechendes gilt. Im Ergebnis werden die anstaltsfremden Bediensteten den Justizvollzugsbediensteten insoweit gleichgestellt. Steht eine Person zu den Justizvollzugsbehörden in einem Dienst- oder Arbeitsverhältnis oder soll sie im Auftrag einer anderen Behörde in den Anstalten tätig werden, geht dieses Gesetz von der Fiktion aus, dass keine Sicherheitsbedenken bestehen. Personen, die zu den Justizvollzugsbehörden nicht in einem Dienst- oder Arbeitsverhältnis stehen und die Anstalten aber im Auftrag einer anderen Behörde aufsuchen sind beispielsweise Bewährungshelfer, Polizeibeamte oder Referendare.

Absatz 1 Satz 2 stellt klar, dass für den Regelfall („soll“) eine Zuverlässigkeitsprüfung durchzuführen ist. Die Zuverlässigkeitsprüfung soll zur Aufrechterhaltung der Sicherheit der Anstalten erfolgen. Eine Ausnahme von der regelhaft durchzuführenden Zuverlässigkeitsprüfung ist demnach immer dann angezeigt, wenn eine Gefährdung der Sicherheit der Anstalten fernliegend erscheint. Beispielhaft zu nennen sind solche anstaltsfremden Personen, die aufgrund ihrer Stellung und ihrer langjährigen Mitarbeit im Vollzug den Anstalten gut bekannt sind und denen die Anstalten aus guten Gründen bereits Vertrauen entgegenbringt. Weitere Beispiele sind die Mitarbeiter privater landeseigener Unternehmen, Bewerber, die zu Vorstellungsgesprächen in die Anstalten kommen oder Vertreter von Unternehmen, die zu Vertragsverhandlungen

dort anwesend sind. Die Zuverlässigkeitsprüfung erfolgt mit dem Einwilligen der betroffenen Person.

Es bedarf daher ihrer zuvor erteilten Zustimmung. Um eine fundierte Entscheidung betroffenen Person zu ermöglichen, sind insbesondere der Anlass der Zuverlässigkeitsprüfung, ihr möglicher Umfang und die etwaigen Folgen einer verweigerten Zustimmung mitzuteilen.

Absatz 1 Satz 3 gibt Justizvollzugsbehörden die Befugnis zum Abfragen personenbezogener Daten. Hierin eingeschlossen ist die Befugnis zum Offenlegen solcher personenbezogenen Daten, die für eine Zuverlässigkeitsüberprüfung von Polizei- und Verfassungsschutzbehörden notwendig sind, wie insbesondere der Identitätsdaten der anstaltsfremden Person. Das Abfragen bei Drittbehörden steht im Ermessen der Justizvollzugsbehörden („dürfen“). Bei der Ermessensentscheidung und dem Abfragen ist der enge Zweck der Zuverlässigkeitsprüfung, die Sicherheit der Anstalten zu gewährleisten, zu berücksichtigen. Absatz 1 Satz 3 gibt nur die Befugnis zum Abfragen personenbezogener Daten und zum Offenlegen der hierfür notwendigen Informationen. Gemäß dem „Doppeltürmodell“ des Datenschutzes muss die Befugnis der Drittbehörden zum Offenlegen personenbezogener Daten an die Justizvollzugsbehörden aus dem jeweils einschlägigen Fachrecht folgen.

Absatz 1 Satz 4 konkretisiert den Verhältnismäßigkeitsgrundsatz und erklärt, dass in Eilfällen an die Stelle der Zuverlässigkeitsprüfung das Beaufsichtigen der anstaltsfremden Person treten soll. Auch hiervon darf im Ausnahmefall abgewichen werden („soll“), wenn eine Gefährdung der Sicherheit der Anstalten 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 zum Austausch personenbezogener Daten nach Absatz 1 Satz 3. Danach soll von einem Austausch personenbezogener Daten abgesehen werden, wenn aufgrund des Anlasses, der Art, des Umfangs oder der Dauer des Aufenthalts oder der Tätigkeit in einer Anstalt eine Gefahr für die Sicherheit der Anstalten fernliegend ist. Der im Austausch personenbezogener Daten liegende Eingriff in das Grundrecht auf informationelle Selbstbestimmung der anstaltsfremden Person ist insoweit mit der prognostisch festzustellenden Gefahr für die Sicherheit der Anstalten abzuwägen. Zu berücksichtigen ist hierbei etwa, ob die anstaltsfremde Person Kontakt zu Gefangenen hat und bei Ehrenamtlichen, mit welchem konkreten Angebot sie in die Anstalten kommen. Bei einer unklaren Ausgangslage darf der Austausch personenbezogener Daten weiterhin erfolgen, da in diesem Fall eine Gefahr für die Sicherheit der Anstalten 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 das Zulassen zum Besuch von Gefangenen und der Anstalten zum Gegenstand. Letzteres umfasst beispielsweise Maßnahmen der Resozialisierungs- und Öffentlichkeitsarbeit, etwa den Anstaltsbesuch, um Theaterveranstaltungen der Gefangenen beizuwohnen. Anders als bei der Tätigkeit anstaltsfremder Personen steht hier nicht erst der Austausch personenbezogener Daten mit 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 des Gefangenen folgende Resozialisierungsziel. Zu berücksichtigen ist insoweit, dass der Zuverlässigkeitsprüfung eine abschreckende Wirkung zukommen kann.

Die Ermessensentscheidung für eine Zuverlässigkeitsüberprüfung von Anstaltsbesuchern setzt voraus, dass tatsächliche Anhaltspunkte für eine drohende Gefahr der Sicherheit der Anstalten 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 das Verletzen des Schutzgutes „Sicherheit der Anstalten“ muss drohen, sondern eine Gefahr hierfür („Gefahr der Gefahr“). Tatsächliche Anhaltspunkte für eine drohende Gefahr der Sicherheit der Anstalten können insbesondere auch darin begründet sein, dass sicherheitsrelevante Erkenntnisse über einen Gefangenen vorliegen, der Besucht werden soll. Die drohende Gefahr muss also nicht notwendigerweise vom 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 Anstalten als fernliegend ausgeschlossen werden kann. Hintergrund der Regelungssystematik ist, dass der Zugang anstaltsfremder Personen zu den Anstalten, um dort tätig zu werden, regelmäßig freiwillig erfolgt.

Ein Tätigwerden in den Anstalten, insbesondere aus beruflichen Gründen, gibt darüber hinaus die Möglichkeit zu besonders weitgehenden Einblicken in die Abläufe der Anstalten und ist daher in erhöhtem Maße gefahrgeneigt. Bei Besuchen nach Absatz 3 stehen demgegenüber Grundrechtspositionen der Gefangenen und anderer betroffener Personen 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 Anstalten vergleichsweise weniger gefährdet ist.

Die Zuverlässigkeitsüberprüfung von Besuchern hat zu erfolgen, wenn diese einwilligen. Es bedarf daher ihrer zuvor erteilten Zustimmung. Um eine fundierte Entscheidung 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 zum Abfragen personenbezogener Daten bei Drittbehörden. Diese steht im Ermessen der Justizvollzugsbehörden und ist auf den engen Zweck des Offenlegens personenbezogener Daten, die Zuverlässigkeitsüberprüfung, beschränkt. Das Offenlegen personenbezogener Daten durch die Justizvollzugsbehörden zum Zweck der Zuverlässigkeitsprüfung dürfte sich daher regelmäßig auf die Identitätsdaten des Besuchers beschränken.

Absatz 3 Satz 3 erweitert die Befugnis zum Offenlegen personenbezogener Daten an die Polizeibehörden und die Verfassungsschutzbehörden auf die Informationen, ob und für welchen Gefangenen das Zulassen zum Besuch begehrt wird.

Absatz 4 konkretisiert den Verhältnismäßigkeitsgrundsatz und nimmt Verteidiger, Beistände, Rechtsanwälte, Notare und die im Rahmen des Überwachens des Schriftwechsels der Gefangenen gesetzlich privilegierte Personen und Stellen von der Zuverlässigkeitsüberprüfung im Rahmen von Gefangenenbesuchen aus. Die geschützte Kommunikation des 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 von der betroffenen Person verweigert wird oder sich sicherheitsrelevante Erkenntnisse ergeben. Der betroffenen Person wird nicht oder nur unter Beschränkungen der Zutritt zu den Anstalten gewährt. Bei der Entscheidung sind die Grundrechtspositionen der betroffenen Person 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 Anstalten abzuwägen. Der Begriff der „sicherheitsrelevanten Erkenntnisse“ in Absatz 5 Satz 1 verweist auf § 23 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 das Wiederholen der Zuverlässigkeitsüberprüfung. Diese hat im Regelfall zu erfolgen („soll“), wenn neue sicherheitsrelevante Erkenntnisse nach § 23 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 Anstalten 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.

Zu § 26 Optisch-elektronisches Beobachten

Die Vorschrift führt den Regelungsgehalt der §§ 141 bis 143 JVollzGB LSA zusammen und regelt die Voraussetzungen des optisch-elektronischen Beobachten in den Anstalten.

Das Erheben personenbezogener Daten durch optisch-elektronisches Beobachten stellt einen besonders intensiven Eingriff in das informationelle Selbstbestimmungsrecht dar, da die betroffenen Personen grundsätzlich keine Möglichkeit haben, sich diesen Maßnahmen zu entziehen. Absatz 1 Satz 1 bindet ihren Einsatz deshalb ausdrücklich an den dort aufgeführten Katalog von Erlaubnistatbeständen, der um die Tatbestände des § 30 Absatz 1 Nummern 1 und 2 DSG LSA in der Fassung der Bekanntmachung vom 13. Januar 2016 erweitert und konkretisiert wurde. Beim optisch-

elektronischen Beobachten der Außengrenzen von Anstalten kann es dazu kommen, dass auch außerhalb des Anstaltsgeländes liegende Flächen miterfasst werden.

Soweit es sich hierbei um öffentlich zugängliche Räume handelt, können diese ausnahmsweise optisch-elektronisch beobachtet werden. Dazu gehören u. a. die effektive das Sicherstellen und Wahrnehmen des Hausrechtes, damit das Verletzen des Hausrechtes von außerhalb, z. B. Beschmieren, Beschädigen oder Zerstören von baulichen (z. B. Mauer, Zaun) oder technischen Einrichtungen (z.B. Kameras, Zaundetektion) der Anstalten, rechtzeitig vorgebeugt, und Schäden für den Landeshaushalt wirksam abgewendet werden kann. Insoweit besteht eine Duldungspflicht der Personen, die sich in Kenntnis des optisch-elektronischen Beobachtens des unmittelbaren Vorfeldes der Anstalten dort bewegen. Dabei sind die jedoch die Belange betroffener Personen, das Hausrecht der Anstaltsleiter und die Notwendigkeit, die Sicherheit der Anstalten zu gewährleisten, nach den in der Vorschrift genannten Maßstäben gegeneinander abzuwägen und in ein angemessenes Verhältnis zu dem jeweils einschlägigen Schutzzweck zu bringen.

Absatz 1 Satz 2 schließt die bisher bestehende Regelungslücke und schafft die notwendige Rechtsgrundlage für ein optisch-elektronisches Beobachten in den Fahrzeugen des Transportes von Gefangenen, soweit die Voraussetzungen des Satzes 1 vorliegen. Damit wird dem Bedürfnis der vollzuglichen Praxis in den Ländern, insbesondere bei Umlauf der Gefangenen über die Ländergrenzen hinaus und der technischen Ausstattung neuer Gefangenentransportwagen im erforderlichen Umfang Rechnung getragen und sichergestellt, dass auch während des Transportes der Gefangenen, diese durch die Bediensteten mit einer sie schützenden, ständigen und unmittelbare Beaufsichtigung mittels optisch-elektronischem Beobachten erfolgen kann, ohne das Bedienstete, insbesondere bei gefährlichen Gefangenen, in unmittelbar die Sicherheit der Bediensteten gefährdende Situationen gelangen und an ihrer Gesundheit geschädigt werden.

Absatz 2 stellt sicher, dass betroffene Personen Kenntnis vom optisch-elektronischen Beobachten nehmen können. Da betroffene Personen aus allen Kulturkreisen und Gesellschaftsschichten kommen und nicht immer alle in der Lage sind, die deutsche Sprache gleich zu verstehen, kann die Verpflichtung der Justizvollzugsbehörden auch dadurch erfüllt werden, dass sowohl sprachliche als auch nichtsprachliche Hinweise dafür sorgen, dass die Personen in eindeutig erkennbarer Weise Kenntnis von der Tatsache und auch von der Reichweite, also des konkreten räumlichen Erstreckens des optisch-elektronischen Beobachtens, haben. Der generelle Hinweis, beispielsweise, das optisch-elektronische Beobachten erstrecke sich auf das gesamte Anstaltsgelände, reicht hierfür nicht aus.

Vor diesem Hintergrund und zur einheitlichen und transparenten Umsetzung optisch-elektronischen Beobachtens in den Anstalten verlangt Absatz 3 ein individuelles, einheitliches Konzept in jeder Anstalt, das auch als Teil der bestehenden Sicherheitskonzepte der Anstalten geführt werden kann und beinhaltet dessen regelmäßiges Überprüfen, Anpassen und laufendes Fortschreiben an die sich verändernden Verhältnisse.

Zu § 27 Optisch-elektronisches Beobachten in Räumen oder Bereichen zum Unterbringen der Gefangenen

Die Vorschrift entspricht grds. § 144 JVollzGB LSA und modifiziert diesen. Die Regelungen zum Weiterverarbeiten finden nun als eigenständige Vorschriften in § 31 ihren Niederschlag.

Absatz 1 stellt klar, dass das Erheben personenbezogener Daten durch optisch-elektronisches Beobachten in Räumen oder Bereichen zum Unterbringen der Gefangenen grundsätzlich verboten ist, da hier den Gefangenen die einzige Rückzugsmöglichkeit verbleibt und sie in diesem Zusammenhang grundsätzlich auch einen Anspruch auf eine unbeobachtete Privatsphäre haben. Das Verbot bezieht sich im Einzelnen im Vollzug der Untersuchungshaft, der Freiheitsstrafe, der Jugendstrafe, des Strafarrestes und den Freiheitsentziehungen nach § 1 Nummer 7 und 8 auf die Hafträume der Gefangenen, im Vollzug des Unterbringens in der Sicherungsverwahrung auf die Unterkunftsbereiche der Untergebrachten und im Jugendarrest auf die Räume zum Unterbringen der Arrestanten zur Ruhezeit. Ausnahmsweise ist jedoch unter den Voraussetzungen der Nummern 1 und 2 das optisch-elektronische Beobachten zulässig. Nummer 1 erfasst dabei den Katalog der besonderen Sicherungsmaßnahmen (vgl. § 89 JVollzGB LSA und § 77 SVVollzG LSA) und sichert diesen auf der Ebene des Schutzes personenbezogener Daten der Gefangenen ab. Optisch-elektronisches Beobachten kann in einem solchen Fall gegenüber einer Sitzwache durch Bedienstete der geringere Eingriff in die Privatsphäre der Gefangenen sein. Nummer 2 greift den Katalog der Nummer 1 auf und lässt optisch-elektronisches Beobachten unter engen Voraussetzungen vorübergehend zu. Die Regelung dient insbesondere als Schutzvorschrift für die Justizvollzugsbediensteten, die im Rahmen und für die Dauer ihres Einsatzes zur Abwehr der in Nummer 1 genannten Gefahren gefährlichen Gefangenen auch in Hafträumen gegenübertreten müssen und ihre Gesundheit gefährden. Sie umfasst auch, soweit von der Technik unveränderlich vorgegeben, das gleichzeitig mit dem optisch-elektronischen Beobachten zu Beweiszwecken einhergehende Erheben personenbezogener Daten in Form des gesprochenen Wortes.

Die Regelung entfaltet damit, neben ihrer individuellen Schutzwirkung, auch eine spezial- und generalpräventive Wirkung für Gefangene und Justizvollzugsbedienstete. Sie trägt so ganz erheblich zum Erhöhen der Sicherheit und Ordnung in den Anstalten bei. Wegen des starken Eingriffs in das Recht auf informationelle Selbstbestimmung bedarf es hier klarer formeller Anwendungsvorgaben, beispielsweise das ausdrückliche schriftliche Anordnen des Anstaltsleiters. Dies gilt auch für das dokumentierte Begründen aller in diesem Zusammenhang stehenden Entscheidungen. Diese und weitere Vorgaben sind beispielhaft Absatz 2 enthalten.

Absatz 3 bestimmt, dass Gefangene über den Umstand des optisch-elektronischen Beobachtens in Kenntnis zu setzen sind und diese 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 können oder durch technische Maßnahmen dafür Sorge getragen wird, dass diese Bereiche im Rahmen des optisch-elektronischen Beobachtens nicht sichtbar sind. Dies kann beispielsweise durch aus-

reichendes Verpixeln erreicht werden, wobei das Verpixeln in unterschiedlichen Graden möglich und zulässig ist. Nur in besonderen Ausnahmefällen, beispielsweise bei akuter Selbstverletzungs- oder Suizidgefahr, kann im Einzelfall hiervon eine Rückausnahme gemacht werden und wieder das uneingeschränkte Überwachen der Gefangenen durch optisch-elektronisches Beobachten erfolgen. Dies ist in der schriftlichen Anordnung festzuhalten und zu begründen. Die Regelungen 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 trägt mit seiner Unterbrechungsregelung dem Erforderlichkeitsgrundsatz Rechnung, dient aber auch dem Schutz besonderer Vertrauensverhältnisse. Bei der Anwesenheit Dritter wird das optisch-elektronische Beobachten regelmäßig nicht erforderlich sein. Das optisch-elektronische Beobachten ist z. B. für Gespräche der Gefangenen mit ihren Verteidigern ausgeschlossen. Durch das kurzzeitige und absehbare Unterbrechen werden die Anstalten außerdem personell entlastet. Zum Fortsetzen des optisch-elektronischen Beobachtens zum gleichen Zweck und beim Fortbestehen der ursprünglich rechtfertigenden Voraussetzungen ist kein neues Anordnen optisch-elektronischen Beobachtens erforderlich.

Zu § 28 Auslesen von Datenspeichern

Die Vorschrift entspricht grds. § 146 JVollzGB LSA und modifiziert diesen zu einer Vorschrift des Erhebens personenbezogener Daten. Die bisher in Absatz 2 enthaltene Regelung zum Weiterverarbeiten findet nun als eigenständige Vorschrift in § 33 ihren Niederschlag.

Absatz 1 gestattet unter engen Voraussetzungen das Auslesen von elektronischen Daten-speichern sowie von elektronischen Geräten mit Datenspeichern. Nach dem derzeitigen Stand der Technik sind hiervon vor u. a. Computer, Notebooks, Tablet-PCs, Mobiltelefone, Smartphones, USB-Sticks, (SSD) Festplatten, Speicherkarten erfasst. Das Auslesen dieser Datenspeicher dient vornehmlich dem Aufklären subkulturell organisierter Strukturen, dem Verhindern des Weiterleitens oder des Bekanntmachens der darauf möglicherweise gespeicherten Daten der Anstalten (z.B. Bilder sicherheitsrelevanter Einrichtungen) und damit unzulässiger Absprachen in Strafprozessen oder im Justizvollzug selbst, um sich gegen die Justizvollzugsbediensteten verdeckt organisieren und geschlossen begegnen zu können. Sie trägt so ganz erheblich zur Aufrechterhaltung der Sicherheit der Anstalten bei. Insbesondere vor diesem Hintergrund wurde der bisher in § 146 Absatz 1 Satz 1 JVollzGB LSA enthaltene Zusatz („die ohne Erlaubnis in die Anstalt eingebracht wurden“) gestrichen, da er die Sicherheit und Ordnung der Anstalten erheblich gefährdet. Mit dem Zusatz würden aktuell die Fälle nicht erfasst, in denen Geräte mit Speichermöglichkeit zwar zulässig in die Anstalten eingebracht wurden (z. B. USB-Sticks und Festplatten im Schul- und Werkbereich), jedoch im Anschluss zweckwidrig zu den Zwecken verwendet werden, die die Sicherheit und Ordnung der Anstalt gefährden. Durch die Neuregelung werden diese Fälle nun erfasst. Dem Schutzbedürfnis betroffener Personen tragen die Justizvollzugsbehörden im Wege der Einzelfallentscheidung im Rahmen des Abwägens der widerstreitenden Interessen und dem Anwenden des Verhältnismäßigkeitsgrundsatzes hinreichend Rechnung. Zwar ist das Auslesen von Datenspeichern als solches kein Eingriff in das Telekommunikationsgeheimnis. Es greift aber in die Integrität und Vertraulichkeit informationstechnischer Systeme ein. Mit Blick auf die

Bedeutung des Eingriffs ist nur der Anstaltsleiter oder eine von ihm hierzu ausdrücklich beauftragte Person zur Anordnung befugt. Vor dem Auslesen bedarf es einer Interessenabwägung. Die Gründe müssen auf konkreten tatsächlichen Anhaltspunkten beruhen und in der Anordnung aus schriftlich festgehalten werden. Das Auslesen darf nur unter Beachten der Rechte der betroffenen Person erfolgen und ist möglichst auf die Inhalte zu beschränken, deren Kenntnis zum Aufrechterhalten der Sicherheit und Ordnung der Anstalt erforderlich ist.

Insbesondere ist es zu vermeiden, personenbezogene Daten aus dem absolut geschützten Bereich privater Lebensgestaltung auszulesen. Absatz 2 verbietet daher das Erheben personenbezogener Daten die in den Kernbereich der privaten Lebensgestaltung betroffener Personen fallen und ordnet deren Löschen und Vernichten an, soweit diese Daten versehentlich erhoben wurden.

Nach Absatz 3 sind die Gefangenen schon bei der Aufnahme in den Vollzug darüber zu belehren, dass Datenspeicher ausgelesen werden dürfen.

Zu Unterabschnitt 2 - Weiterverarbeiten personenbezogener Daten

Zu § 29 Zulässigkeit des Weiterverarbeitens personenbezogener Daten

§ 29 entspricht mit sprachlichen und redaktionellen Anpassungen § 131 JVollzGB LSA.

Absatz 1 entspricht § 131 Absatz 1 JVollzGB, bestimmt den Grundsatz, wonach die Justizvollzugsbehörden die zulässig von ihnen erhobenen personenbezogenen Daten auch zu den Zwecken, zu denen sie erhoben wurden, weiterverarbeiten dürfen und dient zudem dem Umsetzen des in Artikel 8 Absatz 1 der Richtlinie (EU) 2016/680 normierten Erforderlichkeitsprinzips. Der Begriff des Weiterbearbeitens entspricht grds. dem in § 131 JVollzGB LSA enthaltenen Begriffspaar des „Speicherns und Nutzens“. Der Begriff „Nutzen“ wird in der Richtlinie (EU) 2016/680 jedoch nicht mehr ausdrücklich erwähnt. Der dort verwandte Begriff „Verwenden“ ist für sich genommen nicht als Surrogat geeignet, so dass der Begriff des „Weiterverarbeitens“, der sich auch in der Verordnung (EU) 2016/679 wiederfindet, im Umsetzen der Richtlinie (EU) 2016/680 in § 3 Nummer 6 dieses Gesetzes definiert und vom Oberbegriff des „Verarbeitens“ in § 3 Nummer 5 negativ abgegrenzt wird.

Absatz 2 entspricht grds. § 131 Absatz 2 JVollzGB LSA und bestimmt die Voraussetzungen, unter denen das Weiterverarbeiten personenbezogener Daten durch die Justizvollzugsbehörden, auch ohne das Einwilligen der betroffenen Person, zu Zwecken zu denen sie nicht erhoben wurden, zulässig ist. Nach Nummer 1 ist das Weiterverarbeiten personenbezogener Daten zu einem anderen Zweck zulässig, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt. Die Nummer 2 lässt das Weiterverarbeiten personenbezogener Daten zu einem anderen Zweck zu, wenn die Voraussetzung des Erhebens personenbezogener Daten über Gefangene bei Dritten bzw. Personen, die nicht Gefangene sind, zulässig ist. Die Nummer 3 sieht auch das zulässige Weiterverarbeiten personenbezogener Daten unter anderem auch bei Verfahren des gerichtlichen Rechtsschutzes im Vollzug, der Wahrnehmung von Aufsichts- und Kontrollbefugnissen vor. Die Nummern 1 und 3 dienen damit auch dem Umsetzen von Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680. Die in den Num-

mern 4 bis 10 genannten Zwecke unterfallen ebenfalls dem in Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 genannten Zwecken.

Da sich das Weiterverarbeiten personenbezogener Daten besonderer Kategorien unmittelbar an ihr Erheben anschließt, gewährleistet Absatz 3 Satz 1 als eigene Ermächtigungsgrundlage durch das Verweisen auf den Katalog von Absatz 2, das Aufrechterhalten des Schutzniveaus und bestimmt die Zulässigkeit, soweit dies unbedingt erforderlich ist. Satz 2 enthält eine Ausnahme zugunsten personenbezogener Daten besonderer Kategorien, die einem Amts- oder Berufsgeheimnis unterfallen (insbesondere Gesundheitsdaten) und in einer, eine Verschwiegenheitsverpflichtung begründenden, amtlichen oder beruflichen Funktion überlassen wurden. Das Offenbaren dieser Daten richtet sich nach den §§ 57 ff. Die Regelung trägt damit Artikel 10 der Richtlinie (EU) 2016/680 Rechnung.

Absatz 4 entspricht mit sprachlichen Anpassungen dem § 131 Absatz 4 JVollzGB LSA und dient damit auch dem Umsetzen von Artikel 6 der Richtlinie (EU) 2016/680, wonach zwischen verschiedenen Kategorien betroffener Personen zu unterscheiden ist.

Absatz 5 entspricht § 131 Absatz 5 JVollzGB LSA.

Absatz 6 entspricht § 131 Absatz 6 JVollzGB LSA und enthält als bereichsspezifische Sonderregelung, beim Vorliegen der dort genannten Ausnahmetatbestände, die Befugnis, personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert oder genutzt werden, auch für andere Zwecke weiterzuverarbeiten.

Zu § 30 Weiterverarbeiten von Identifikationsmerkmalen; Gefangenenausweise

Absatz 1 entspricht mit sprachlichen Anpassungen § 140 Absatz 2 und 3 JVollzGB LSA und nennt die Voraussetzungen unter den das Weiterverarbeiten der nach § 22 erhobenen personenbezogener Daten der Gefangenen zulässig ist.

§ 37, und damit das Weiterverarbeiten der nach § 22 erhobenen personenbezogenen Daten im Rahmen von Fallkonferenzen, bleibt von der Regelung des Absatzes 1 unberührt. Gleichzeitig wird klargestellt, dass die erhobenen personenbezogenen Daten des Gefangenen nicht nur in Papierform in Gefangenenpersonalakten abgelegt, sondern auch in Gestalt personenbezogener Dateisystemen gespeichert werden dürfen. Dabei sind personenbezogener Daten 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 beispielsweise ein gesondertes Ablegen in der Gefangenenpersonalakte. Satz 2 Nummer 1 greift den Grundsatz der Zweckbindung auf und legt fest, dass die erhobenen Daten zu den Zwecken, zu denen sie erhoben wurden, weiterverarbeitet werden dürfen. Nummer 2 erlaubt das Weiterverarbeiten der nach § 22 erhobenen personenbezogener Daten zum Zweck des Identifizierens des entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen im Rahmen des Fahndens nach ihm und seines Festnehmens. Nummer 3 regelt das Weiterverarbeiten der nach § 22 erhobenen personenbezogener Daten für den Zweck des § 29 Absatz 2 Nummer 7 sowie zum Feststellen der Identität nach § 22.

Absatz 2 entspricht mit sprachlichen Anpassungen § 147 Absatz 2 JVollzGB LSA und nennt die Voraussetzungen, unter den das Weiterverarbeiten der nach § 22 Absatz 3 erhobenen personenbezogener Daten anstaltsfremder Personen zulässig ist. Die Nummer 2 wurde um die Möglichkeit ergänzt, die gewonnenen personenbezogenen Daten anstaltsfremder Personen auch zum Verfolgen von Ordnungswidrigkeiten nach § 115 OWiG offenlegen zu dürfen. Nach § 115 Absatz 1 OWiG handelt ordnungswidrig, wer unbefugt einem Gefangenen Sachen oder Nachrichten übermittelt oder sich von ihm übermitteln lässt oder sich mit einem Gefangenen, der sich innerhalb einer Vollzugsanstalt befindet, von außen durch Worte oder Zeichen verständigt. Das erforderliche Erweitern der Regelung dient damit auch dem Gewährleisten der Sicherheit und Ordnung der Anstalten.

Absatz 3 Satz 1 ermächtigt die Anstalten, die Gefangenen zu verpflichten, aus Gründen der Sicherheit oder Ordnung, einen Lichtbildausweis mit sich zu führen. Dies umfasst die Herstellung der Lichtbildausweise, die beim Entlassen der Gefangenen oder ihres Verlegens einzuziehen und zu vernichten sind. Satz 2 stellt sicher, dass auf einem Lichtbildausweis außer dem Bild nur solche personenbezogenen Daten gespeichert werden, die für das Gewährleisten von Sicherheit und Ordnung der Anstalten erforderlich sind.

Satz 3 ermöglicht es z. B. den Einrichtungen des offenen Vollzugs, Gefangene, die etwa außerhalb der Anstalten einem freien Beschäftigungsverhältnis nachgehen, beim Betreten und Verlassen der Anstalten auch mittels elektronischer Systeme zu erfassen.

Handelt es sich bei den erhobenen personenbezogenen Daten um solche besonderer Kategorien, ist ihr Weiterverarbeiten für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligen der betroffenen Person nur nach § 29 Absatz 3 zulässig. Das zweckändernde Weiterverarbeiten personenbezogener Daten nach § 30 Absatz 1 Nummer 2 und 3 und § 30 Absatz 2 muss folglich unbedingt erforderlich sein.

Zu § 31 Weiterverarbeiten personenbezogener Daten nach optisch-elektronischem Beobachten und akustisch-elektronischem Überwachen

Die Vorschrift entspricht § 145 JVollzGB LSA, enthält als Lex specialis in Absatz 1 Satz 1 die Befugnis, die durch optisch-elektronisches Beobachten erhobenen personenbezogenen Daten weiterzuverarbeiten, soweit und solange dies zum Erreichen vollzuglicher Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. In Satz 2 erfährt diese Befugnis mit Blick auf das Weiterverarbeiten personenbezogener Daten zu anderen als zu den erhobenen Zwecken das Beschränken auf die dort genannten Ziele. Die bisher enthaltene Frist von 48 Stunden hat sich in der Praxis nicht bewährt und ist zu streichen, da in vielen Fällen die Erkenntnisse, die ein Weiterverarbeiten personenbezogener Daten rechtfertigten, erst zu einem späteren Zeitpunkt bekannt wurden bzw. werden können und die Daten durch das zeitige Löschen und Vernichten unwiederbringlich verloren waren und wären. Das Löschen und Vernichten dieser personenbezogenen Daten richtet sich nach § 63 Absatz 4, wonach die maximale Löschfrist nunmehr einen Monat beträgt.

Absatz 2 entspricht § 145 Absatz 2 JVollzGB LSA und stellt die durch akustisch-elektronische Einrichtungen erhobenen personenbezogenen Daten denen eines optisch-elektronischen Beobachtens gleich. Erfasst sind hierbei alle mittels akustischen Überwachens gewonnenen Daten. Hierzu zählen auch die personenbezogenen Daten aus einem Überwachen des Telefonverkehrs nach den Justizvollzugsgesetzen (vgl. z. B. § 36 JVollzGB LSA).

Absatz 3 entspricht § 145 Absatz 5 JVollzGB LSA.

Absatz 4 entspricht § 145 Absatz 4 JVollzGB LSA und dient dem Schutz des Kernbereichs privater Lebensgestaltung. Er trägt der besonderen Lage, in der sich Gefangene befinden, Rechnung. Dem Kernbereich privater Lebensgestaltung 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 personenbezogenen Daten besteht ein absolutes Verbot ihres Verarbeitens, insbesondere dürfen sie nicht gespeichert werden. Durch präventive Maßnahmen ist sicherzustellen, dass das Verarbeiten dieser personenbezogenen Daten ausgeschlossen ist. Sollte es dennoch versehentlich zu einem Erheben oder dem Weiterverarbeiten dieser personenbezogenen Daten kommen, sind diese unverzüglich zu löschen. Satz 5 enthält davon eine den besonderen Vollzugserfordernissen gerecht werdende Ausnahme.

Handelt es sich um erhobene personenbezogenen Daten besonderer Kategorien ist ihr Weiterverarbeiten für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligen der betroffenen Person nur nach § 29 Absatz 3 zulässig. Das zweckändernde Weiterverarbeiten personenbezogener Daten nach § 31 muss folglich hierzu unbedingt erforderlich sein.

Zu § 32 Weiterverarbeiten personenbezogener Daten nach Beaufsichtigen, Überwachen und Kontrollieren

Die Vorschrift entspricht § 152 JVollzGB LSA. Erkenntnisse aus Maßnahmen zum Beaufsichtigen, Überwachen und Kontrollieren der Gefangenen und anderen betroffenen Personen unterliegen einem besonderen Schutz. Häufig stammen die Erkenntnisse aus einem zulässigen Eingriff in den Schutzbereich von Artikel 10 Absatz 1 GG. Der Schutzbereich von Artikel 10 GG umfasst auch die Informations- und Datenverarbeitungsprozesse, die sich an das Kenntnisnehmen von geschützten Kommunikationsdaten anschließen, sowie den Gebrauch dieser Kenntnisse (vgl. BVerfGE 100, 313, 359). Dabei stellt jedes Kenntnisnehmen, Aufzeichnen und Verwerten von Kommunikations-daten sowie das Auswerten des Inhalts und das sonstige Verwenden 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 und einen solchen Eingriff zu rechtfertigen, dürfen personenbezogene Daten nur unter den Voraussetzungen des Absatzes 1 verarbeitet werden. Missbräuchen ist durch besonderes Kennzeichnen der sensiblen Daten vorzubeugen.

Absatz 2 erweitert die privilegierten Zwecke von Satz 1 für die spezifischen Belange der Untersuchungshaft und den Freiheitsentziehungen nach § 1 Nummern 1, 7 und 8.

Soweit der Kernbereich der privaten Lebensgestaltung betroffen ist, dürfen personenbezogene Daten nicht verarbeitet werden. Absatz 3 Satz 1 nennt aus diesem Grund die Pflichten der Justizvollzugsbehörden zum Löschen und Vernichten personenbezogene Daten. Darüber hinaus besteht nach Satz 2 die Pflicht, das Erheben dieser personenbezogenen Daten und ihr Löschen und Vernichten zu dokumentieren, um das Einhalten dieser Vorgänge kontrollierbar zu machen und so der betroffenen Person effektiven Grundrechtsschutz zu ermöglichen. Satz 3 enthält davon eine den besonderen Erfordernissen des Vollzuges gerecht werdende Ausnahme.

Handelt es sich um erhobene personenbezogene Daten besonderer Kategorien ist ihr Weiterverarbeiten für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligen der betroffenen Person nur nach § 29 Absatz 3 zulässig. Das zweckändernde Weiterverarbeiten personenbezogener Daten nach § 32 muss hierzu unbedingt erforderlich, also unerlässlich, sein.

Zu § 33 Weiterverarbeiten personenbezogener Daten nach Auslesen von Datenspeichern

Die Vorschrift entspricht § 146 Absatz 2 JVollzGB LSA und nennt die Voraussetzungen zum Weiterverarbeiten personenbezogener Daten, die durch Auslesen von Datenspeichern erhoben wurden, wobei durch Verweis auf die Intentionen der §§ 29 und 37, die Zwecke richtlinienkonform konkretisiert wurden. Handelt es sich um erhobene personenbezogene Daten besonderer Kategorien ist ihr Weiterverarbeiten für Zwecke, zu denen sie nicht erhoben wurden, ohne Einwilligen der betroffenen Person nur nach § 29 Absatz 3 zulässig; es muss folglich unbedingt erforderlich, also unerlässlich, sein.

Zu Unterabschnitt 3 - Offenlegen personenbezogener Daten durch Übermitteln oder eine andere Art des Bereitstellens; Abfrage

In diesem Unterabschnitt wird das Offenlegen personenbezogener Daten durch Übermitteln oder eine andere Art ihres Bereitstellens geregelt. Dabei wurde bewusst der in der Richtlinie (EU) 2016/680 normierte Oberbegriff des „Offenlegens“ gewählt, weil das „Verbreiten“ personenbezogener Daten, also deren Veröffentlichen, explizit ausgeschlossen werden soll.

Zudem sollen weitere Formen des Offenlegens personenbezogener Daten an andere als die betroffenen Personen, beispielsweise das Bereitstellen personenbezogener Daten zum Einsehen von (elektronischen) Akten oder Dateisystemen in den Justizvollzugsbehörden, ausdrücklich erfasst werden sollen. Im Umsetzen der Richtlinie (EU) 2016/680 enthält Unterabschnitt 3, neben den modifizierten §§ 132 bis 134, 136 bis 139 und 140 Absatz 4 JVollzGB LSA, auch Neuregelungen zum Austauschen personenbezogener Daten mit den Behörden mit Sicherheitsaufgaben (einschließlich des Grundsatzes des hypothetischen Datenneuerhebens) und zum Offenlegen personenbezogener Daten durch Einsehen in die Personalakten, Gesundheitsakten und Krankenblättern der Gefangenen durch Mitglieder des CPT und der Nationalen Stelle zur Verhütung von Folter.

Zu § 34 Offenlegen personenbezogener Daten gegenüber öffentlichen Stellen

Absatz 1 entspricht im Wesentlichen § 132 Absatz 1, 3 und 4 JVollzGB LSA, fasst diese zusammen und ergänzt den Katalog um den Zweck des Offenlegens personenbezogener Daten gegenüber Jugendämtern zum Erfüllen deren Aufgaben.

Satz 1 regelt das Offenlegen personenbezogener Daten zu den Zwecken, zu denen sie erhoben worden sind, und stellt insbesondere die Rechtsgrundlage für den Austausch personenbezogener Daten zwischen den Justizvollzugsbehörden im Falle des Verlegens und Überstellens von Gefangenen oder bei Verwaltungsvorgängen, an denen mehrere Justizvollzugsbehörden beteiligt sind dar. Dies gilt namentlich auch für länderübergreifende Vorgänge. Voraussetzung ist, dass Empfänger personenbezogener Daten diese zum Erreichen vollzuglicher Zwecke benötigen. Der Begriff „vollzuglichen Zwecke“ ist in § 2 bestimmt. Der in Satz 1 normierte Erforderlichkeitsgrundsatz dient dem Umsetzen von Artikel 8 der Richtlinie (EU) 2016/680 und ist insoweit europarechtskonform auszulegen.

Satz 2 dient dem Umsetzen von Artikel 4 Absatz 2 und Artikel 9 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 (Grundsätze des zweckändernden Verarbeitens personenbezogener Daten) und ist in deren Anwendungsbereich europarechtskonform auszulegen. Unter den Voraussetzungen von Satz 2 dürfen personenbezogene Daten auch zu anderen Zwecken offengelegt werden. Eine „Rechtsvorschrift“ im Sinne von Nummer 1, welche das zweckändernde Offenlegen personenbezogener Daten gegenüber öffentlichen Stellen erlaubt, kann auch eine solche sein, die der Verordnung (EU) 2016/679 unterfällt. Hiermit wird der Tatsache Rechnung getragen, dass das vielfältige Verarbeiten personenbezogener Daten im Justizvollzug, je nach Zweck des Verarbeitens personenbezogener Daten, im Einzelfall entweder der Richtlinie (EU) 2016/680 oder der Verordnung (EU) 2016/679 unterfallen kann. Auch in letzterem Fall bedarf es einer gesetzlichen Ermächtigung zum Austausch personenbezogener Daten mit den zuständigen öffentlichen Stellen.

Das Offenlegen personenbezogener Daten für Gnadensachen nach Nummer 2 Buchstabe b) unterfällt nicht dem Unionsrecht. Die Vorschrift bedarf insoweit auch nicht der europarechtskonformen Auslegung. Das Offenlegen personenbezogener Daten für das Erfüllen von Aufgaben, die den für Sozialleistungen zuständigen Leistungsträgern durch Rechtsvorschriften übertragen worden sind (Nummer 2 Buchstabe d)), für dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldaten (Nummer 2 Buchstabe f)), für asyl- oder ausländerrechtliche Maßnahmen (Nummer 2 Buchstabe g)), zum Erfüllen von Aufgaben der Jugendämter (Nummer 2 Buchstabe h)), oder zum Durchführen der Besteuerung (Nummer 2 Buchstabe i)) unterfallen der Verordnung (EU) 2016/679 und nicht der Richtlinie (EU) 2016/680. Das Offenlegen personenbezogener Daten gegenüber öffentlichen Stellen zum Erfüllen von Aufgaben der forensischen Ambulanzen, für asylrechtliche Maßnahmen, zum Erfüllen der Aufgaben der Jugendämter und für Fallkonferenzen mit den Behörden mit Sicherheitsaufgaben wurde neu aufgenommen, um den entsprechenden Bedürfnissen der Praxis Rechnung zu tragen.

Satz 3 schränkt die Befugnis der Justizvollzugsbehörden zum Offenlegen personenbezogener Daten zugunsten Untersuchungsgefangener und der Gefangenen nach § 1 Nummern 7 und 8 ein, weil für sie die Unschuldsvermutung gilt. Deshalb muss vor dem Offenlegen personenbezogener Daten das Abwägen der schutzwürdigen In-

teressen stattfinden. Die Regelung dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680 (Unterscheiden verschiedener Kategorien betroffener Personen) und ist in deren Anwendungsbereich europarechtskonform auszulegen.

Absatz 2 entspricht § 132 Absatz 6 JVollzGB LSA und trägt dem Schutz personenbezogener Daten besonderer Kategorien Rechnung. Wegen der erhöhten Sensibilität dieser Daten dürfen diese ohne das Einwilligen der betroffenen Person nur in den genannten Fällen offengelegt werden. Die Möglichkeit des Offenlegens zulässig erhobener personenbezogener Daten besonderer Kategorien in Fallkonferenzen und gegenüber forensischen Ambulanzen wurde ergänzend eingefügt, um einem Bedürfnis der Praxis Rechnung zu tragen.

„Unbedingt erforderlich“ im Sinne des Absatzes 3 ist das Offenlegen personenbezogenen Daten besonderer Kategorien, wenn es im konkreten Einzelfall für das Erreichen des jeweiligen Zweckes unerlässlich ist.

Absatz 3 entspricht § 132 Absatz 7 JVollzGB LSA und trägt dem Umstand Rechnung, dass bei Personen, die keine Gefangenen sind, ein Eingriff durch die Justizvollzugsbehörden in ihr informationelles Selbstbestimmungsrecht besonderes Gewicht hat. Absatz 3 Satz 2 erweitert die Offenlegungsbefugnis der Justizvollzugsbehörden um die Möglichkeit, personenbezogene Daten Dritter offenzulegen, um das Fahnden nach und Festnehmen von entwichenen Gefangenen zu ermöglichen. Es handelt sich hier um eine bereichsspezifische Regelung. Bei den zulässig offengelegten personenbezogenen Daten handelt es sich regelmäßig nur um das Mitteilen von Namen und der Adresse(n) von Kontaktpersonen. Absatz 3 dient auch dem Umsetzen von Artikel 6 der Richtlinie (EU) 2016/680 (Unterscheiden verschiedener Kategorien betroffener Personen) und ist in deren Anwendungsbereich europarechtskonform auszulegen.

Absatz 4 entspricht § 132 Absatz 8 JVollzGB LSA und stellt eine für die Belange des Justizvollzuges praktikable und im Hinblick auf die Interessen und Rechte der betroffenen Personen dennoch verhältnismäßige Regelung dar. Die Regelung dient dem Umsetzen von Artikel 6 der Richtlinie (EU) 2016/680 (Unterscheiden verschiedener Kategorien betroffener Personen) und ist in deren Anwendungsbereich europarechtskonform auszulegen. Absatz 5 entspricht § 132 Absatz 10 JVollzGB LSA.

Zu § 35 Offenlegen personenbezogener Daten gegenüber nicht öffentlichen Stellen

Absatz 1 entspricht § 132 Absatz 2 JVollzGB LSA und erweitert in Nummer 2 den Katalog um den erforderlichen Zweck des Offenlegens personenbezogener Daten für das Inanspruchnehmen von Maßnahmen des Vorbereitens des Entlassens, des Übergehens in die Freiheit, des Schuldenregulierens und -tilgens, des Entlassens, des Wiedereingliederns, des nachgehenden Betreuens oder des freiwilligen Verbleibens.

Absatz 2 entspricht § 132 Absatz 5 JVollzGB LSA und erweitert diesen um den erforderlichen Zweck des Offenlegens personenbezogener Daten in Fallkonferenzen (§ 37).

Absatz 3 entspricht im Wesentlichen § 132 Absatz 6 JVollzGB LSA, trägt dem Schutz personenbezogener Daten besonderer Kategorien Rechnung und erweitert diesen um den erforderlichen Zweck des Offenlegens personenbezogener Daten in Fallkonferenzen (§ 37).

Absatz 4 entspricht durch den Verweis auf § 34 Absatz 3 bis 5 dem § 132 Absatz 7, 8 und 10 JVollzGB LSA.

Zu § 36 Weitere Voraussetzungen beim Offenlegen personenbezogener Daten gegenüber Behörden mit Sicherheitsaufgaben

Mit dem Urteil vom 20. April 2016 betreffend Regelungen des Bundeskriminalamtgesetzes (BKAG), hat das Bundesverfassungsgericht seine Rechtsprechung zum Erheben personenbezogener Daten und das Weitergeben dieser Daten zusammengefasst, konsolidiert und fortentwickelt (vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09, Rn 292 ff.). Der neue § 36 setzt den vom Bundesverfassungsgericht in der Entscheidung für den Austausch personenbezogener Daten mit den Behörden mit Sicherheitsaufgaben konkretisierten Grundsatz des hypothetischen Datenneuerhebens für den Bereich des Justizvollzuges des Landes um. Hintergrund ist die Erwägung, dass ein Austausch personenbezogener Daten nicht nur zwischen den verschiedenen Behörden mit Sicherheitsaufgaben des Bundes und der Länder, sondern regelmäßig auch zwischen den Behörden des Justizvollzuges und den Behörden mit Sicherheitsaufgaben stattfindet respektive stattfinden muss.

Die ausgetauschten bzw. auszutauschenden Informationen werden dabei oftmals durch eingriffs-intensive Überwachungsmaßnahmen wie Eingriffe in das Brief-, Post- und Fernmeldegeheimnis, das Überwachen des Zellenbereiches der Gefangenen oder das Auslesen gefundener Datenträger und Mobiltelefone erlangt. Umgekehrt werden Informationen gegenüber Justizvollzugsbehörden offengelegt und dort weiterverarbeitet, die die Behörden mit Sicherheitsaufgaben auf Grundlage mitunter schwerwiegender Grundrechtseingriffe erlangt haben. Das Bundesverfassungsgericht unterscheidet hinsichtlich des weiteren Verarbeitens erhobener personenbezogener Daten entsprechend den Grundsätzen der Zweckbindung und der Zweckänderung. Ein weiteres Verarbeiten erhobener personenbezogener Daten innerhalb der ursprünglichen Zwecksetzung kommt nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für das Erheben dieser Daten maßgeblich waren (vgl. BVerfG, a. a. O., Rn 279).

Da das Austauschen personenbezogener Daten mit den Behörden mit Sicherheitsaufgaben 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 des ursprünglichen Erhebens personenbezogener Daten durch das Weitergeben dieser Daten und das weitere Verarbeiten der Informationen zu anderen Zwecken vertieft wird. Dabei drohen die spezifischen Voraussetzungen, welche die Informationsgewinnung erlaubt haben, entwertet zu werden. Erlaubt der Gesetzgeber das weitere Verarbeiten personenbezogener Daten zu anderen Zwecken als denen des ursprünglichen Erhebens personenbezogener Daten, muss er folglich sicherstellen, dass dem Eingriffsgewicht des Erhebens personenbezogener Daten auch hinsichtlich des Weiterverarbeitens dieser Daten 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 des Erhebens personenbezogener Daten. Dabei unterscheidet das Bundesverfassungsgericht jeweils zwischen Gefahrentatbestand und Schutzgut einerseits und Tatverdacht und Straftatbestand andererseits. Voraussetzung für eine Zweckänderung ist jedenfalls, dass das Weiterverarbeiten personenbezogener Daten dem Schutz von Rechtsgütern oder dem Aufdecken von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihrem Neuerheben mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (Grundsatz des hypothetischen Datenneuerhebens). Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen eines Erhebens personenbezogener Daten hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend ist insoweit, dass sich aus den personenbezogenen Daten ein konkreter Ansatz ergibt (vgl. BVerfG, a. a. O., Rn 286 ff.). Der Gesetzgeber kann danach, bezogen auf das Weiterverarbeiten personenbezogener Daten durch Behörden mit Sicherheitsaufgaben, eine Zweckänderung grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ansätze zum Aufdecken von vergleichbar gewichtigen Straftaten oder zum Abwehren von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz das entsprechende Datenerheben zulässig ist (BVerfG, a. a. O., Rn 290). Anderes gilt für Informationen aus dem Überwachen von Wohnräumen oder dem Zugriff auf informationstechnische Systeme. Angesichts des besonderen Eingriffsgewichts dieser Maßnahmen muss für sie jedes Weiterverarbeiten dieser personenbezogenen Daten, wie bei beim Erheben selbst, auch durch eine dringende Gefahr oder eine im Einzelfall hinreichend konkretisierte Gefahr gerechtfertigt sein (BVerfG, a. a. O., Randnummer 291). Der verfassungsrechtliche Grundsatz des hypothetischen Datenneuerhebens wird für den Informationsaustausch mit den Behörden mit Sicherheitsaufgaben im neuen § 36 als allgemeiner Grundsatz definiert, der beim Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben und beim Erheben personenbezogener Daten bei diesen, unabhängig von der jeweiligen Eingriffsintensität des ursprünglichen Erhebens dieser Daten, zu beachten ist. Die Struktur der Vorschriften ist dabei an § 12 des neuen BKAG angelehnt. Hierdurch soll dem Petitum der Innenminister von einem Angleichen der Rechtsvorschriften verschiedener Behörden mit Sicherheitsaufgaben Rechnung getragen werden. Perspektivisch soll zudem ein weitgehender Gleichlauf der Verwaltungspraxis der Justizvollzugsbehörden und der Behörden mit Sicherheitsaufgaben beim Austausch personenbezogener Daten und in der Frage des hypothetischen Datenneuerhebens ermöglicht werden.

Absatz 1 übernimmt die Vorgaben des Bundesverfassungsgerichts an das zweckändernde Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben und führt damit den Grundsatz des hypothetischen Datenneuerheben in das Vierte Buch Justizvollzugsgesetzbuch Sachsen-Anhalt ein (vgl. BVerfG, a. a. O, Randnummern 288 bis 290). Die Vorschrift ist im Zusammenhang mit den Vorschriften zum Austausch personenbezogener Daten mit den Behörden mit Sicherheitsaufgaben zu lesen und begründet selbst keine Befugnis zum Offenlegen personenbezogener Daten.

Absatz 1 übernimmt auch die verfassungsrechtlichen Vorgaben dahingehend, dass das Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben 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 zum Erheben personenbezogener Daten gleichwertiger Rechtsgüterschutz sichergestellt ist. Darüber hinaus bedarf es im Einzelfall konkreter Ansätze zum Verhüten, Aufdecken, oder Verfolgen von Straftaten oder Ordnungswidrigkeiten oder zum Abwehren von in einem überschaubaren Zeitraum drohenden Gefahren.

Der Grundsatz des hypothetischen Datenneuerhebens wird hierbei eingeführt, ohne auf besonders eingriffsintensive Maßnahmen beschränkt zu sein.

Der Begriff der „Behörden mit Sicherheitsaufgaben“ umfasst die Polizeibehörden des Bundes und der Länder, den Verfassungsschutz des Bundes und der Länder sowie den Bundesnachrichtendienst und den militärischen Abschirmdienst. Gleiches gilt für die entsprechenden Behörden mit Sicherheitsaufgaben in den Mitgliedstaaten der Europäischen Union. Mit dem Offenlegen personenbezogener Daten „zum Zwecke der Gefahrenverhütung, zum Zwecke der Gefahrenabwehr, zum Verhindern oder Verfolgen von Ordnungswidrigkeiten, zum Verhindern oder Verfolgen von Straftaten oder zu den in § 29 Absatz 2 Nummer 4 genannten Zwecken“ ist die gesamte Tätigkeit der Behörden mit Sicherheitsaufgaben auf dem Zeitstrahl erfasst, vom Erstellen von Lagebildern durch den Verfassungsschutz über die klassische Gefahrenabwehr der Polizeibehörden bis zum Verfolgen von Straftaten und Ordnungswidrigkeiten.

Der Begriff „im Einzelfall konkrete Ansätze zum Verhüten, Aufdecken oder Verfolgen 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 das Offenlegen personenbezogener Daten rechtfertigt. Das Offenlegen personenbezogener Daten „ins Blaue hinein“ und allein getragen von der Hoffnung auf Erkenntnisse ist ausgeschlossen.

Der Begriff „im Einzelfall konkrete Ansätze […] zum Abwehren von in einem überschaubaren Zeitraum drohenden Gefahren […] für bedeutsame Rechtsgüter“ schließt das Offenlegen personenbezogener Daten „ins Blaue hinein“ und getragen allein von der Hoffnung auf Erkenntnisse 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 zu einem Schaden eines Schutzgutes kommt. Die „in einem überschaubaren Zeitraum drohende Gefahr“ ist der konkreten Gefahr im polizeirechtlichen Sinne folglich vorgelagert. Das Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben, um überhaupt erst herauszufinden, ob eine Gefahr droht, ist gleichwohl ausgeschlossen.

Mit der Formulierung „im Vergleich zum Erheben personenbezogener Daten gleichwertiger Rechtsgüterschutz“ wird normativ erfasst, dass sich das Gewicht des Grundrechtseingriffs des Weitergebens personenbezogener Daten am Grundrechtseingriff des Erhebens personenbezogener Daten zu orientieren hat. Die „Vergleichbarkeit“ folgt aus den rechtsgutsbezogenen Schwellen zum Erheben personenbezogener Daten 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, welches dem Erheben personenbezogener Daten zugrunde lag. Bei Informationen aus einer Strafverfolgungsmaßnahme bedarf die aufzuklärende Straftat des näheren Einordnens. Wenn zum Beispiel eine gegenwärtige Gefahr für Leib oder Leben vorausgesetzt wird, um das optisch-elektronische Beobachten eines Haftraums zu ermöglichen, dürften Zufallserkenntnisse aus einem solchen Beobachten 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 Schwelle des Erhebens personenbezogener Daten der Art der jeweiligen Maßnahme aber vergleichbar gewichtig. Anderes würde zum Beispiel beim Weiterverarbeiten solcher Informationen zum Verfolgen 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., Rn 100). Das Kriterium des gleichwertigen Rechtsgüterschutzes beim Erheben personenbezogener Daten und dem Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben stellt sich für die Justizvollzugsbehörden als vergleichsweise unproblematisch dar. Regelmäßig lassen die Justizvollzugsgesetze das Erheben personenbezogener Daten unter Voraussetzungen zu, die im Vergleich zu den Eingriffsschwellen der Polizeigesetze erheblich abgesenkt sind.

§ 41 JVollzGB LSA beispielsweise erlaubt das Überwachen des Schriftwechsels schon dann, wenn dies „aus Gründen der Sicherheit“ oder zum Abwehren einer „Gefährdung der Erreichung des Vollzugszieles“ erforderlich ist. Da der Grundrechtseingriff des Offenlegens personenbezogener Daten sich am Grundrechtseingriff des Erhebens personenbezogener Daten orientieren muss und weil die Voraussetzungen des Erhebens personenbezogener Daten bei deren Offenlegen fortwirken, sind die vergleichsweise niedrigen Schwellen des Erhebens personenbezogener Daten auch beim Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben zu berücksichtigen.

Die Schwellen zum Offenlegen personenbezogener Daten des § 36 Absatz 1 gewährleisten, dass es nicht zu einem Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben zum allgemeinen Unterstützen bei deren Aufgabenwahrnehmung kommt. Das Offenlegen personenbezogener Daten 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., Rn 293 ff.) unzulässig. Konkret bedeutsam ist dies beispielsweise mit Blick auf das Offenlegen personenbezogener Daten nach § 29 Absatz 2 Nummer 4 in Verbindung mit § 34 Absatz 1 Nummer 2 Buchstabe j), der isoliert betrachtet einen Austausch personenbezogener Daten an den Verfassungsschutz bereits zulässt, wenn dies für deren Aufgabenerfüllung erforderlich ist.

Absatz 2 regelt, dass die Vorgaben zum Offenlegen personenbezogener Daten gegenüber den Behörden mit Sicherheitsaufgaben umgekehrt auch gelten, wenn gegenüber den Justizvollzugsbehörden Informationen von diesen offengelegt werden. Insoweit werden die Vorgaben des Bundesverfassungsgerichts an das Offenlegen personenbezogener Daten durch die Behörden mit Sicherheitsaufgaben übernommen.

Das Kriterium des hypothetischen Datenneuerhebens ist zu beachten, wenn personenbezogene Daten erhoben werden „zum Zwecke der Gefahrenverhütung, zum Zwecke der Gefahrenabwehr, zum Verhindern oder Verfolgen von Ordnungswidrigkeiten oder zum Verhindern oder Verfolgen von Straftaten“. Angesprochen ist damit zuvörderst das Erheben personenbezogener Daten bei den Behörden mit Sicherheitsaufgaben zum Zwecke des Gewährleistens der Sicherheit der Anstalten. Auf dem Zeitstrahl wird der gesamte Bereich vom Verhindern des Eintritts einer Gefahrenlage über das Abwehren von Gefahren bis zum Verfolgen von Straftaten erfasst. Mit dem „Verhüten von Gefahren“ ist der Auftrag des Justizvollzuges erfasst, die Allgemeinheit vor weiteren Straftaten der Gefangenen 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 Anstalten, der Schutz der Allgemeinheit vor Straftaten der Gefangenen oder auch die Sicherung des Strafverfahrens in der Untersuchungshaft. Mit der Sicherheit der Anstalten sind zugleich gewichtige Rechtsgüter wie Leben, die Freiheit, die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung angesprochen, darüber hinaus die Gewährleistung eines resozialisierungsförderlichen Umfeldes. Das Austauschen personenbezogener Daten zwischen den Behörden mit Sicherheitsaufgaben zu den Justizvollzugsbehörden dürfte danach in weitem Umfang möglich sein. Absatz 2 gilt ebenso wie Absatz 1 nur für personenbezogene Daten. Werden seitens der Behörden mit Sicherheitsaufgaben also Informationen ohne Personenbezug übermittelt, beispielsweise zur Einschätzung eines Buches, findet § 36 keine Anwendung.

Absatz 3 trägt den besonderen Anforderungen des Bundesverfassungsgerichts an das zweckändernde Weiterverarbeiten personenbezogener 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 Behörden mit Sicherheitsaufgaben als auch für das Offenlegen von Informationen an die Behörden mit Sicherheitsaufgaben, da Absatz 2 auf Absatz 1 Bezug nimmt.

Das Offenlegen 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 Erhalten 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., Rn 183). Der Haftraum, Unterkunftsbereich oder Arrestraum eines Gefangenen unterfällt nicht dem Schutzbereich des Artikel 13 GG. Dementsprechend werden dort keine personenbezogenen Daten durch den „Einsatz technischer Mittel in oder aus Wohnungen“ gewonnen (vgl. BVerfG, Kammerbeschluss vom 30. Mai 1996 - 2 BvR 727/94). Das Offenlegen so gewonnener Informationen an Behörden mit Sicherheitsaufgaben unterfällt Absatz 3 Nummer 1 folglich nicht. Hinsichtlich des gleichwertigen Rechtsgüterschutzes des Erhebens personenbezogener Daten und des Offenlegens dieser personenbezogenen Daten ist indes zu beachten, dass die Achtung der Menschenwürde und insbesondere der Privat- und Intimsphäre als Ausdruck des allgemeinen Persönlichkeitsrechts auch bezüglich des Haftraum, Unterkunftsbereich oder Arrestraum eines Gefangenen angezeigt ist. Dabei ist anzuerkennen, dass der gesonderte Haftraum, Unterkunftsbereich oder Arrestraum für den Gefangenen 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 das Offenlegen 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 (i. V. m. Absatz 2) vor allem Anwendung finden, wenn es um das Empfangen entsprechender Daten durch die Behörden mit Sicherheitsaufgaben geht. Werden solche Informationen dann in einem nächsten Schritt vom Justizvollzug gegenüber anderen Behörden mit Sicherheitsaufgaben offengelegt, ist Absatz 3 Nummer 1 ebenfalls einschlägig. Das Offenlegen 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., Rn 213). Die Schutzgüter entsprechen denen des allgemeinen Polizeirechts für den verdeckten Eingriff in informationstechnische Systeme und sind entsprechend auszulegen. Gegenstand des Absatzes 3 Nummer 2 sind personenbezogene Daten, die durch den verdeckten Zugriff auf das Telekommunikationsendgerät der betroffenen Person 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 2. März 2006 - 2 BvR 2099/04 - , Rn 93 ff.). Anderes gilt für das Auslesen zum Beispiel über das Internet. Der praktische Anwendungsbereich des Absatzes 3 Nummer 2 dürfte für den Justizvollzug daher, vergleichbar dem Absatz 3 Nummer 1, gering sein.

Absatz 3 Nummer 2 dürfte (in Verbindung mit Absatz 2) vor allem Anwendung finden, wenn es um den Empfang entsprechender Daten durch die Behörden mit Sicher-

heitsaufgaben geht. Werden solche Informationen dann in einem nächsten Schritt vom Justizvollzug gegenüber anderen Behörden mit Sicherheitsaufgaben offengelegt, ist Absatz 3 Nummer 2 ebenfalls einschlägig.

Absatz 4 stellt klar, dass die Vorgaben der Zweckbindung und der Grundsatz des hypothetischen Datenneuerhebens nicht gelten, wenn die Grunddaten einer Person zu Identifizierungszwecken verwendet werden sollen. Dies entspricht der Rechtsprechung des Bundesverfassungsgerichts zum Abfragen und Verwenden von einfachen Grunddaten zum Zweck des Identifizierens (vgl. BVerfG, Urteil vom 24. April 2013 - 1 BvR 1215/07 -, Rn 193 ff.). Das Weiterverarbeiten dieser personenbezogenen Daten ist durch das bloße Verwenden von Grunddaten und Zweck des Identifizierens in doppelter Weise eng begrenzt, das Eingriffsgewicht des Offenlegens dieser Daten entsprechend reduziert. Weitere Daten, etwa die weiteren zu einer als „Treffer“ identifizierten Person gespeicherten Erkenntnisse, sind von Absatz 4 nicht erfasst; insoweit bleibt es bei den Vorgaben der Absätze 1 bis 3.

Zu § 37 Offenlegen personenbezogener Daten im Rahmen von Fallkonferenzen

Die Vorschrift hat Fallkonferenzen u. a. mit Behörden mit Sicherheitsaufgaben zum Gegenstand. Anders als dem punktuellen Austausch personenbezogener Daten wohnt diesen eine Dynamik insofern inne, als auf die jeweils ausgetauschten Informationen durch die empfangende Behörde unverzüglich reagiert und ihrerseits 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 einem Tätigwerden dem Betroffenen 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 Austausch personenbezogener Daten nach § 34. § 37 trägt somit der besonderen Eingriffstiefe Rechnung und schafft für Fallkonferenzen mit den Polizeibehörden des Bundes und der Länder und mit dem Verfassungsschutz der Länder sowie dem Bundesamt für Verfassungsschutz eine normenklare gesetzliche Grundlage mit qualifizierten Eingriffsschwellen für das gegenseitige Offenlegen personenbezogener Daten.

§ 37 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 Vorschrift orientiert sich insoweit an der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Trennungsprinzip. Danach unterliegen Regelungen, die den Austausch personenbezogener Daten der Polizeibehörden und Nachrichtendienste ermöglichen, hinsichtlich des Grundrechts auf informationelle Selbstbestimmung gesteigerten verfassungsrechtlichen Anforderun-

gen. Dass die Befugnisse des Verarbeitens personenbezogener Daten 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 zum Offenlegen personenbezogener Daten gegenüber den Polizeibehörden des Bundes und der Länder im Rahmen von Fallkonferenzen. Das Einberufen der Fallkonferenz steht im Ermessen der Justizvollzugsbehörden, wie aus der Formulierung „dürfen“ hervorgeht. Klarstellend wird hervorgehoben, dass Gegenstand des Offenlegens personenbezogener Daten auch der voraussichtliche Entlassungszeitpunkt, die voraussichtliche Entlassungsadresse sowie die Vollzugs- und Eingliederungspläne und auch personenbezogene Daten besonderer Kategorie sein können. Sofern biometrische Daten zum eindeutigen Identifizieren einer natürlichen Person ausgetauscht werden, erweitert § 37 Absatz 1 als spezielle Ermächtigungsnorm die Befugnisse nach §§ 30 und 38. Voraussetzung für das Offenlegen personenbezogener Daten ist, dass die Informationen zulässig erhoben wurden. Hiermit wird klargestellt, dass das unzulässige Erheben personenbezogener Daten zum Löschen und Vernichten personenbezogener Daten führen muss und deren Weiterverarbeiten im Rahmen einer Fallkonferenz ausgeschlossen ist. Als Offenlegungsschwelle nennt Absatz 1 Satz 1 tatsächliche Anhaltspunkte für die fortdauernde Gefährlichkeit des 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 des Gefangenen nach Absatz 1 Satz 1 Nummer 1 ist im Rahmen einer Gefahrenprognose für den Zeitpunkt der Entscheidung festzustellen. Die Prognose muss tatsachengestützt 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 betroffene Person aller Voraussicht nach in einem Zeitraum von nicht mehr als einem Jahr aus der Haft entlassen werden wird. Entscheidend ist die Vollzugsplanung im Zeitpunkt der Entscheidung. Die Vorschrift soll einer „Verpolizeilichung“ des Justizvollzuges entgegenwirken. Sie verdeutlicht die Ratio des Absatzes 1 Satz 1, einen Austausch personenbezogener Daten mit den Polizeibehörden und ein mit diesen abgestimmtes Vorgehen zu ermöglichen zum Zweck einer koordinierten Entlassungsvorbereitung.

Absatz 1 Satz 1 Nummer 3 verdeutlicht, dass der Informationsaustausch im Rahmen der Fallkonferenzen zum vorbeugenden Bekämpfen 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 der Gefangene weitere Straftaten begehen wird. Straftaten von erheblicher Bedeutung sind insbesondere Verbrechen sowie schwerwiegende Vergehen. Die Straftat muss nach mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu ge-

eignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Entscheidend ist die konkrete Betrachtung im Einzelfall. Die Gefahr von Bagatelldelikten genügt den Anforderungen einer Fallkonferenz nach § 37 nicht.

Absatz 1 Satz 2 erlaubt das Offenlegen personenbezogener Daten im Rahmen einer Fallkonferenz mit den Polizeibehörden des Bundes und der Länder zum Vorbereiten von Ausführungen, Vorführungen, Ausantwortungen, Überstellungen und Verlegungen. Die im Ermessen der Justizvollzugsbehörde stehende Fallkonferenz dient hier, also anders als im Satz 1, nicht dem koordinierten Vorbereiten der Entlassung, sondern soll die polizeiliche Absicherung der vorgenannten Vorgänge ermöglichen. Der im Vergleich zum Satz 1 begrenzte Zweck der Fallkonferenz ist beim Umfang des Offenlegens personenbezogener Daten zu berücksichtigen. Voraussetzung für eine Fallkonferenz nach Satz 2 ist die Gefahr von Entweichungen, Gewalttätigkeiten gegen Personen oder Sachen von bedeutendem Wert, deren Erhalten 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 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 von Regelfall kann eine Fallkonferenz ohne 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 diese der besonderen Begründung.

Absatz 1 Satz 4 ermächtigt die Justizvollzugsbehörden, unter den Voraussetzungen des § 37 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 gegenüber den Behörden mit Sicherheits-aufgaben offengelegt werden, umgekehrt aber nur wenige Informationen von den Behörden mit Sicherheitsaufgaben 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 Datenschutzrechts gibt Absatz 1 Satz 4 nur die Befugnis des Justizvollzuges zum Abfragen und Erheben personenbezogener Daten. Die Befugnis der Polizeibehörden des Bundes und der Länder zum Offenlegen personenbezogener Daten muss aus deren jeweils einschlägigen Fachrecht folgen.

Gehören die offengelegten personenbezogenen Daten zu besonderen Kategorien, ist deren Offenlegen gegenüber anderen öffentlichen Stellen nur unter den Voraussetzungen des § 29 Absatz 3 zulässig, wonach das Weiterverarbeiten dieser personenbezogenen Daten für die in § 29 Absatz 2 genannten Zwecke unbedingt erforderlich

sein muss. Gehören die offenzulegenden personenbezogenen Daten zu besonderen Kategorien personenbezogener Daten, ist deren Offenlegen gegenüber Polizeibehörden des Bundes und der Länder folglich nur dann zulässig, wenn dies zum Erfüllen der genannten Zwecke unbedingt erforderlich ist. Gleiches gilt für das Erheben solcher Daten bei den Polizeibehörden durch den Justizvollzug.

Absatz 2 Satz 1 ermächtigt die Justizvollzugsbehörden zum Offenlegen personenbezogener Daten gegenüber den Verfassungsschutzbehörden des Bundes und der Länder im Rahmen von Fallkonferenzen. Das Einberufen von Fallkonferenzen steht im Ermessen der Justizvollzugs-behörden, 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 zum Offenlegen personenbezogener Daten 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 des Verfassungsschutzes des Bundes und der Länder als Inlandsnachrichtendienste (Sammlung und Auswertung von Informationen) unterscheiden.

Polizeibehörden und der Verfassungsschutz 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 den Verfassungsschutz zugeschnittene Befugnisse zum Offenlegen personenbezogener Daten im Rahmen von Fallkonferenzen festlegt.

Nach Absatz 2 Satz 1 dürfen personenbezogene Daten einschließlich solche besonderer Kategorie gegenüber dem Verfassungsschutz des Bundes und der Länder offengelegt werden, wenn bestimmte Tatsachen den Verdacht für Bestrebungen nach § 29 Absatz 2 Nummer 4 begründen, eine damit im Zusammenhang stehende Gefahr für die Sicherheit der Anstalten 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 § 37 Absatz 2 Satz 1 Nummer 1 auf Tätigkeiten oder Bestrebungen nach § 29 Absatz 2 Nummer 4 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 des Verfassungsschutzes 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 des Verfassungsschutzes fallen, für das Offenlegen personenbezogener Daten unzureichend ist. Aufgrund der Tätigkeiten oder Bestrebungen muss entweder eine Gefahr für die Sicherheit der Anstalten oder das Erreichen 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 Anstalten 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 Anstalten und das Erreichen des Vollzugsziels. Ausgehend vom Vollzugsziel, den Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen, kann damit beispielsweise ein Austausch personenbezogener Daten mit dem Verfassungsschutz stattfinden, wenn aufgrund einer manifesten Radikalisierung Resozialisierungserfolge nicht festzustellen sind.

Die Gefahr für das Schutzgut „Vollzugsziel“ oder „Sicherheit der Anstalten“ muss „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 -, Rn 113). Ebenfalls unzureichend ist der Austausch personenbezogener Daten mit dem Verfassungsschutz, um überhaupt erst herauszufinden, ob eine drohende Gefahr vorliegt. Die drohende Gefahr ist Voraussetzung für die Fallkonferenz nach § 37 Absatz 2. Bedarf es insoweit einer weitergehenden Aufklärung des Sachverhalts, muss diese durch das Offenlegen nicht personenbezogener Informationen erfolgen.

Nach Absatz 2 Satz 1 Nummer 3 muss das Offenlegen personenbezogener Daten zum Verhindern einer Gefahr für die Sicherheit der Anstalten oder das Erreichen des Vollzugszieles unbedingt erforderlich, das heißt im konkreten Einzelfall unerlässlich sein. Dies ist im Rahmen des Ermessens der Justizvollzugsbehörde zu berücksichtigen und steht standardisierten Fallkonferenzen mit dem Verfassungsschutz entgegen.

Da es sich beim Verfassungsschutzbehörden, anders als bei den Polizeibehörden, nicht um Gefahrenabwehrbehörden handelt, übernimmt Absatz 2 Satz 1 nicht die Jahresfrist bis zum Entlassen des Satz 1 Satz 1 Nummer 2. Fallkonferenzen zum Informationsaustausch mit dem Verfassungsschutz nach Absatz 2 sind daher während des gesamten Vollzuges möglich.

Nach Absatz 2 Satz 2 sollen die Bewährungshilfe und die Führungsaufsichtsstellen an der Fallkonferenz beteiligt werden, sofern das Entlassen des Gefangenen in voraussichtlich nicht mehr als einem Jahr bevorsteht.

Dadurch soll sichergestellt werden, dass im Rahmen der Fallkonferenz eine Vielzahl von Einschätzungen Berücksichtigung findet, wenn das Vorbereiten der Entlassung des Gefangenen bereits in Rede steht. Beispielhaft zu nennen sind solche Informationen, die nicht in den originären Aufgabenbereich des Verfassungsschutzes gehören, wie beispielsweise Fragen der sozialen und beruflichen Wiedereingliederung. Als Ausnahme von Regelfall kann eine Fallkonferenz ohne Bewährungshilfe und Führungs-aufsichtsstelle stattfinden, wenn beispielsweise ganz überwiegend hochsensible personenbezogene Daten mit einem spezifischen Sicherheitsbezug ausge-

tauscht und hierüber weitergehend beraten werden soll. Im Rahmen des Ermessens der Justizvollzugsbehörden bedarf eine solche Entscheidung der besonderen Begründung.

Absatz 2 Satz 3 ermächtigt die Justizvollzugsbehörden, personenbezogene Daten vom Verfassungsschutz des Bundes und der Länder abzufragen und zu erheben. Er soll damit einer etwaigen „Schieflage“ von Justizvollzug und dem Verfassungsschutz entgegenwirken, wonach zwar eine Vielzahl von Informationen aus dem Justizvollzug heraus gegenüber den Behörden mit Sicherheitsaufgaben offengelegt werden, umgekehrt aber nur wenige Informationen von dort in den Justizvollzug gelangen. Die Regelung eröffnet den Justizvollzugsbehörden nun die Möglichkeit, beim Verfassungsschutz 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 zum Abfragen und Erheben personenbezogener Daten. Die Befugnis des Verfassungsschutzes des Bundes und der Länder zum Offenlegen personenbezogener Daten muss aus deren jeweils einschlägigen Fachrecht folgen.

Absatz 3 ermächtigt die Justizvollzugsbehörden zum gleichzeitigen Austausch personenbezogener Daten mit den Polizeibehörden des Bundes und der Länder und mit dem Verfassungsschutz des Bundes und der Länder im Rahmen von Fallkonferenzen. Das Einberufen der Fallkonferenzen steht im Ermessen der Justizvollzugsbehörden, wie aus der Formulierung „dürfen“ hervorgeht.

Bei den Schwellen zum Offenlegen personenbezogener Daten 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 Gefahrenabwehrbehörden und die Aufgaben des Verfassungsschutzes des Bundes und der Länder als Inlandsnachrichtendienste (Sammlung und Auswertung von Informationen) unterscheiden, gemeinsame Fallkonferenzen aber gerade auf einen dynamischen Informationsaustausch über die Behördengrenzen hinweg angelegt sind.

Ein Informationsaustausch zwischen den Behörden mit Sicherheitsaufgaben mit unterschiedlichen Aufgaben, der insbesondere auch den Austausch personenbezogener Daten zwischen den Polizeibehörden und anderen Behörden mit Sicherheitsaufgaben 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 dem Betroffenen gegenüber zur operativen Anwendung gebracht werden. Der Austausch personenbezogener Daten ist in einem solchen Fall nur ausnahmsweise zulässig. Voraussetzung für das Überwinden des informationellen Trennungsprinzips ist, dass der Zugriff auf und das Verarbeiten dieser personenbezogenen 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 vom 24. April 2013 - 1 BvR 1215/07 -, Rn. 112 ff., 201 ff.).

Absatz 3 Satz 1 Nummern 1 bis 3 konkretisieren die verfassungsrechtlichen Vorgaben an einen Austausch personenbezogener Daten unter Überwindung des informationellen Trennungsprinzips unter erlauben gemeinsame Fallkonferenzen von Justizvollzugsbehörden, Polizeibehörden und dem Verfassungsschutz, wenn kumulativ eine gegenwärtige Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalten im öffentlichen Interesse geboten ist, vorliegt, wenn der Verdacht für Tätigkeiten oder Bestrebungen nach § 29 Absatz 2 Nummer 4 begründen und wenn der Informationsaustausch zur Gefahrenabwehr unbedingt erforderlich ist. Die Gefahrenprognose und der Verdacht von Tätigkeiten und Bestrebungen nach § 29 Absatz 2 Nummer 4 muss tatsachengestützt sein. Vermutungen und allgemeine Erfahrungssätze sind unzureichend. Gegenwärtig ist eine Gefahr, bei der das Einwirken des schädigenden Ereignisses bereits begonnen hat oder bei der dieses Einwirken 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 § 29 Absatz 2 Nummer 4 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 zum Abwehren von Gefahren unbedingt erforderlich, wenn er im Einzelfall hierfür unerlässlich ist.

Absatz 3 Satz 2 erklärt Absatz 2 Satz 2 für entsprechend anwendbar. Auch bei gemeinsamen Fallkonferenzen mit den Polizeibehörden und dem Verfassungsschutz sollen also die Bewährungshilfe und die Führungsaufsichtsstellen beteiligt werden, sofern das Entlassen des Gefangenen in voraussichtlich nicht mehr als einem Jahr bevorsteht. Hierdurch soll sichergestellt werden, dass im Rahmen von Fallkonferenzen eine Vielzahl von Einschätzungen Berücksichtigung finden, wenn das Vorbereiten des Entlassens des Gefangenen bereits in Rede steht. Beispielhaft zu nennen sind solche Informationen, die nicht in den originären Aufgabenbereich der Behörden mit Sicherheitsaufgaben gehören, wie beispielsweise Fragen der sozialen und beruflichen Wiedereingliederung. Als Ausnahme von Regelfall kann eine Fallkonferenz ohne Bewährungshilfe und Führungsaufsichtsstelle stattfinden, wenn beispielsweise ganz überwiegend hochsensible personenbezogene Daten mit einem spezifischen Sicherheitsbezug ausgetauscht und hierüber weitergehend beraten werden soll.

Absatz 3 Satz 3 ermächtigt die Justizvollzugsbehörden, personenbezogene Daten vom Verfassungsschutz 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 Behörden mit Sicherheitsaufgaben entgegenwirken, wonach zwar eine Vielzahl von Informationen aus dem Justizvollzug heraus gegenüber den Behörden mit Sicherheitsaufgaben übermittelt offengelegt werden, umgekehrt aber nur wenige Informationen von dort in den Justizvollzug gelangen. Absatz 3 Satz 3 eröffnet den Justizvollzugsbehörden nun die Möglichkeit, beim Verfassungsschutz des Bundes und der Länder und bei den Polizeibehörden des Bundes und der Länder personenbezogene Informationen zu erheben, um ihren gesetzlichen Auftrag und das Voll-

zugsziel 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 Datenschutzrechts gibt Absatz 3 Satz 3 nur die Befugnis des Justizvollzuges zum Abfragen und Erheben personenbezogener Daten. Die Befugnis des Verfassungsschutzes des Bundes und der Länder und der Polizeibehörden des Bundes und der Länder zum Offenlegen personenbezogener Daten muss aus deren jeweils einschlägigen Fachrecht folgen.

Nach § 37 Absatz 4 sind die wesentlichen Ergebnisse der Fallkonferenz zu dokumentieren. Die Dokumentation muss sachhaltig genug sein, um den erfolgten Austausch personenbezogener Daten und das gegebenenfalls erfolgte Festlegen auf ein einvernehmliches Vorgehen dergestalt nachvollziehen zu können, dass nachträglicher Rechtsschutz und eine nachträgliche Datenschutzkontrolle möglich sind.

§ 37 Absatz 5 stellt klar, dass die Vollzugs- und Eingliederungsplanung den Justizvollzugs-behörden vorbehalten bleibt, ist in einem systematischen Zusammenhang mit den Absätzen 1 bis 3 zu lesen und soll einer „Verpolizeilichung“ und einer „Vernachrichtendienstlichung“ des Justizvollzuges entgegenwirken. Absatz 5 stellt auch klar, dass die Fallkonferenzen mit den Polizeibehörden und dem Verfassungsschutz 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 Behörden mit Sicherheitsaufgaben. Diese werden nur im konkreten Einzelfall und soweit im Rahmen von Fallkonferenzen beteiligt, als es ihren gesetzlichen Aufgaben entspricht und die jeweiligen Voraussetzungen zum Offenlegen personenbezogener Daten erfüllt sind.

Zu § 38 Offenlegen von Identifikationsmerkmalen

Die Vorschrift entspricht § 140 Absatz 4 JVollzGB LSA und wurde u. a. um das Einbeziehen der personenbezogenen Daten von anstaltsfremden Personen für deren notwendiges Offenlegen nach den Nummern 1 bis 4 erweitert. Damit wurde eine Regelungslücke, die bisher nur das Offenlegen der personenbezogenen Daten der Gefangenen ermöglichte, geschlossen.

Nummer 1 ist in einem Zusammenhang mit Nummer 2 zu lesen und nennt die zuständigen Empfänger im Falle des Fahndens nach einem Gefangenen und dessen Festnehmen.

Nummer 2 ist im Zusammenhang mit Nummer 4 zu lesen. Nummer 3 verweist hinsichtlich der Empfänger bei einem Offenlegen personenbezogener Daten zum Zweck des Identifizierens einer natürlichen Person auf die §§ 22 und 37 und deren Voraussetzungen.

Nummer 4 erfasst den Fall des Offenlegens der erhobenen personenbezogenen Daten auf Ersuchen einer öffentlichen Stelle, greift den Grundsatz des hypothetischen Datenneuerhebens auf und erlaubt das zweckändernde Offenlegen personenbezogener Daten an eine öffentliche Stelle auf deren Ersuchen, wenn das Neuerheben der entsprechenden personenbezogenen Daten durch die anfragende Stelle im konkreten Fall zulässig wäre.

Der letzte Halbsatz übernimmt den Regelungsgehalt von § 137 letzte Alternative JVollzGB LSA. So wird sichergestellt, dass die Behörden mit Sicherheitsaufgaben jederzeit beispielsweise ihrer Verpflichtung aus § 32 Abs. 1 BKAG mit personenbezogenen Daten, die sachlich richtig und auf dem neuesten Stand sind, nachkommen können. Dies trägt u. a. auch den Anforderungen von Artikel 4 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680 Rechnung.

Gehören die erhobenen personenbezogenen Daten zu besonderen Kategorien, ist deren Offenlegen gegenüber anderen öffentlichen Stellen nur unter den Voraussetzungen des § 29 Absatz 3 zulässig. Nach § 29 Absatz 3 muss das Weiterverarbeiten für die in § 29 Absatz 2 genannten Zwecke unbedingt erforderlich sein. Gehören die erhobenen personenbezogenen Daten zu besonderen Kategorien personenbezogener Daten, ist deren Offenlegen gegenüber anderen öffentlichen Stellen folglich nur dann zulässig, wenn dies zum Erfüllen der genannten Zwecke unbedingt erforderlich ist.

Zu § 39 Offenlegen personenbezogener Daten durch das Mitteilen von Haftverhältnissen

Absatz 1 regelt, in welchem Umfang die Justizvollzugsbehörden Auskunft über die genannten Haftverhältnisse geben dürfen. Auch hier erfolgt ein sachgerechtes Differenzieren zwischen öffentlichen und nichtöffentlichen Stellen. Bei Letzteren sind die Interessen des Gefangenen ausdrücklich in das Prüfen mit einzubeziehen. Die nicht öffentlichen Stellen müssen ihr Interesse glaubhaft darlegen, z.B. Darstellen einer Forderung und der beabsichtigten weiteren Schritte wie das gerichtliche Geltendmachen oder die Zwangsvollstreckung unter Vorlage des Titels. Die Justizvollzugsbehörden trifft hier keine Pflicht zum Überprüfen der Rechtmäßigkeit der angestrebten Maßnahmen.

Absatz 2 privilegiert Forderungen öffentlicher Stellen. Die öffentliche Hand soll wegen ihrer überragenden Bedeutung für die Daseinsvorsorge hinsichtlich von Auskünften über die Entlassungsadresse oder die Vermögensverhältnisse von Gefangenen den Opfern einer Straftat insoweit gleichgestellt werden.

Der besonderen Stellung der Untersuchungsgefangenen, sie gelten als unschuldig, und der in einer Haft gemäß § 1 Nummer 7 und 8 befindlichen Gefangenen ist auch im Rahmen des Mitteilens über ihre Haftverhältnisse an externe Stellen Rechnung zu tragen. Absatz 3 bestimmt deshalb, dass im Falle des Mitteilens über Haftverhältnisse nur die Angabe erfolgen darf, ob sich eine Person in der Anstalt in Untersuchungshaft oder wegen einer anderen Freiheitsentziehung nach § 1 Nummer 7 und 8 befindet.

Absatz 4 schreibt eine Interessenabwägung zwischen den Belangen der Auskunftsberechtigten und der Gefangenen vor. Im Falle eines unterbliebenen Anhörens der Gefangenen hat nicht nur eine Mitteilung, sondern auch die Angabe des offengelegten Inhalts zu erfolgen.

Absatz 5 trägt den besonderen Schutzinteressen der Empfänger Rechnung.

Absatz 6 regelt die Dokumentationspflicht und dient der Transparenz.

Zu § 40 Offenlegen personenbezogener Daten durch das Erteilen von Auskünften an Opfer

Die Vorschrift trägt dem hohen Stellenwert des Opferschutzgedankens gemäß Rechnung. Sie greift die in § 406d Absatz 2 Nummer 2 der Strafprozessordnung getroffene Regelung auf und billigt Opfern ein Recht auf Erteilen der Auskunft zu. Gerade Opfer von Gewalttaten oder Geschädigte, die in einer besonderen Beziehung zu den Gefangenen stehen, können den nachvollziehbaren Wunsch haben zu erfahren, ob und gegebenenfalls wann sie mit einer erneuten Begegnung mit dem Täter rechnen müssen, sei es im Rahmen von Lockerungen, vollzugsöffnenden Maßnahmen oder auf Grund des Entlassens des Gefangenen aus dem Vollzug. Desgleichen kann ein berechtigtes Bedürfnis der Opfer bestehen, die Entlassungsadresse des Gefangenen zu erfahren. Auch die Kenntnis der Vermögensverhältnisse des Gefangenen kann von erheblicher Bedeutung sein, etwa für das Realisieren geltend gemachter oder bereits zuerkannter Schadensersatzansprüche.

Absatz 1 Satz 1 verpflichtet die Justizvollzugsbehörden deshalb, Opfern Auskunft über die Inhaftierung des Gefangenen, deren Beendigung, das erstmalige oder erneute Gewähren von Lockerungen, vollzugsöffnenden Maßnahmen, opferbezogene Weisungen und das Unterbringen des Gefangenen im offenen Vollzug zu erteilen. Voraussetzung dafür ist, dass Opfer ein berechtigtes Interesse an der Auskunft darlegen und kein überwiegendes schutzwürdiges Interesse des Gefangenen am Ausschluss der Mitteilung vorliegt. Opferbelange können auch beim Entscheiden über erneute vollzugsöffnende Maßnahmen erheblich berührt sein. Der Auskunftsanspruch erstreckt sich auch darauf, ob und welche Weisungen den Gefangenen im Rahmen vollzugsöffnender Maßnahmen erteilt wurden. Nach Satz 2 ersetzt der Nachweis des Zulassens zur Nebenklage, entsprechend § 406d Absatz 2 Nummer 2 der Strafprozessordnung, in der Regel das Darlegen des berechtigten Interesses. Durch den Zusatz „in der Regel“ wird klargestellt, dass sich in Einzelfällen trotz Vorliegens der Voraussetzungen die Notwendigkeit eines ergänzenden Darlegens ergeben kann. Das Einschränken bedarf insbesondere in den Fällen des § 395 Absatz 1 Nummer 6 der Strafprozessordnung sorgfältiger Prüfung. Nach Satz 3 gilt diese Darlegungserleichterung nicht im Fall des Gewährens erneuter Lockerungen oder vollzugsöffnender Maßnahmen.

Absatz 2 sieht bei Flucht von Gefangenen, insbesondere bei dessen Entweichen, als Ausnahme zu Absatz 1, eine Mitteilungspflicht auch ohne Antrag der Opfer vor. Da die Auskünfte jedoch grundsätzlich nicht aufgedrängt werden sollen, ist die Verpflichtung an das Vorliegen einer Gefahr für Leib oder Leben der Opfer geknüpft. Dies entspricht den europarechtlichen Mindeststandards für die Rechte, die Unterstützung und den Schutz für Opfer von Straftaten Richtlinie 2012/29/EU vom 25. Oktober 2012, Amtsblatt der Europäischen Union vom 14. November 2012, Seiten 57 ff., sog. 2. Opferschutzrichtlinie).

Absatz 3 Satz 1 entspricht der Regelung in § 180 Absatz 5 Satz 2 StVollzG und ermöglicht es den Opfern und den aus der Straftat Anspruchsberechtigten auf schriftlichen Antrag Auskünfte über die Entlassungsadresse oder die Vermögensverhältnisse der Gefangenen zu erhalten. Voraussetzung hierfür ist jedoch, dass das Erteilen der Auskunft zum Feststellen oder Durchsetzen von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist.

Absatz 4 trägt den besonderen Interessen der Empfänger einer Mitteilung Rechnung. Besteht Anlass zu der Besorgnis, dass das Offenlegen von Lebensumständen der Antragsteller deren Leib oder Leben gefährdet, kann nach Satz 1 das Offenlegen gegenüber den Gefangenen unterbleiben. Die Mitteilung der Anschrift der Antragsteller an die Gefangenen bedarf nach Satz 2 des ausdrücklichen Einwilligens der betroffenen Mitteilungsempfänger. Die Vorschrift dient damit in besonderer Weise dem Opferschutz und trägt dem Umstand Rechnung, dass die Antragsteller ein überwiegendes Interesse daran haben können, einzelne personenbezogene Daten, insbesondere ihre Anschrift oder einzelne Lebensumstände, gegenüber den Gefangenen geheim zu halten, wenn ein Offenlegen dieser Daten sie in Leib oder Leben gefährden würde.

Absatz 5 ermächtigt die Justizvollzugsbehörden unter den dort genannten Voraussetzungen auch zum direkten Erteilen von Auskünften nach § 406d Strafprozessordnung. Absatz 6 trägt den Dokumentationspflichten der Justizvollzugsbehörden Rechnung.

Zu § 41 Offenlegen personenbezogener Daten durch das Überlassen von Akten und Dateisystemen

Die Vorschrift entspricht § 138 JVollzGB LSA und enthält in Absatz 1 eine Sonderregelung für das Überlassen von Akten mit enumerativer Aufzählung der hierfür in Frage kommenden öffentlichen Stellen. Ein solches Überlassen von Akten ist gleichzeitig das Offenlegen aller in der Akte enthaltenen personenbezogenen Daten. Dieser Umfang setzt zwingend eine gesetzliche Befugnis zum Offenlegen dieser personenbezogenen Daten voraus. Absatz 2 schreibt eine Interessen-abwägung vor, sofern eine untrennbare Verquickung von personenbezogenen Daten vorliegt. Bei personenbezogenen Daten besonderer Kategorien wird regelmäßig von vornherein ein überwiegendes berechtigtes Interesse der betroffenen Person an dem Geheimhalten ihrer personenbezogenen Daten unterstellt, sodass das Offenlegen personenbezogener Daten im Wege des Überlassens von Akten und Dateisystemen und damit das Überlassen von Akten oder Dateisystemen selbst unzulässig sind. Das Weiterverarbeiten oder Offenlegen der untrennbar verbundenen personenbezogenen Daten durch den Empfänger ist unzulässig**.**

Zu § 42 Offenlegen personenbezogener Daten durch das Einsehen von Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern

Die Vorschrift normiert ein Recht zum Einsehen der Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter durch Mitglieder einer Delegation des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment, im Weiteren CPT) während eines Anstaltsbesuchs. Damit wird einer Forderung des CPT aus dem Jahr 2016 entsprochen, Maßnahmen zu ergreifen, damit Besuchsdelegationen des Ausschusses künftig unbeschränkte Einsicht in die Personal- und Krankenakten von Gefangenen erhalten können. Aus Gründen der Klarstellung wurde normiert, dass das identische Recht zur Einsehen der Akten im Rahmen von Anstaltsbesuchen auch für Mitglieder einer durch das Übereinkommen der Vereinten Nationen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe legitimierten

Stelle gilt, auch wenn hierfür bereits eine Rechtsgrundlage in Artikel 14 Absatz 1 Buchstabe b und Artikel 20 Buchstabe b des Fakultativprotokolls zum Übereinkommen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe besteht. Das Einsehen der Akten wird gewährt, soweit dies zur Wahrnehmung der Aufgaben dieser Stellen erforderlich ist. Die Einschätzung der Erforderlichkeit wird in diesen Fällen von den Mitgliedern der genannten Stellen vorgenommen werden und von den Justizvollzugsbehörden im Regelfall zu akzeptieren sein. Das anlasslose Gewähren des Einsehens von Akten, die besonders sensible Daten der Gefangenen, insbesondere Gesundheitsdaten, enthalten, stellt einen schweren Eingriff in das Recht der Gefangenen auf informationelle Selbstbestimmung dar. Dieser ist hier aber aufgrund des hochrangigen Zwecks des Verhinderns beziehungsweise Aufdeckens von Folter und unmenschlicher Behandlung durch zu ihrem Schutz tätige internationale Organisationen zulässig, insbesondere verhältnismäßig. Anders als durch eine auf Forderung der Mitglieder der genannten Stellen umfassend zu gewährende Akteneinsicht lässt sich deren ungehindertes Wahrnehmen ihrer Aufgaben nicht sicherstellen. Forderte man, insbesondere für das Gewähren des Einsehens von Gesundheitsakten, das Vorliegen tatsächlicher Anhaltspunkte für Misshandlungen, wäre die Möglichkeit der genannten Stellen, die Rechtmäßigkeit der Behandlung der Gefangenen zu überprüfen, eingeschränkt. Tatsächliche Anhaltspunkte für Misshandlungen werden sich, rechtswidrige Zustände vorausgesetzt, weder aus den Gefangenpersonalakten noch durch eine Befragung von Gefangenen ergeben, die vor dem Besuch einer Delegation durch gezielte Desinformationen oder Einschüchtern beeinflusst werden könnten. Aus diesem Grund ist auch von einer Regelung abzusehen, die das Einehen in Gesundheitsakten von dem Einwilligen der Gefangenen abhängig macht. Auch das Einwilligungsverhalten der Gefangenen könnte durch die Justizvollzugsbehörden vor einem Besuch einer Delegation durch Desinformationen beeinflusst werden. Das internationale Monitoring der Behandlung der Gefangenen ist auf einen präventiven Schutz ausgerichtet. Das bedeutet, dass gerade das anlasslose Überprüfen eine Kernaufgabe der genannten Stellen ist. Die Tätigkeit dieser Stellen ist Teil der menschenrechtlichen Garantien in Europa und ist daher durch das Gewähren anlasslosen Einsehens in Akten in der Anstalt zu ermöglichen. In dieser speziellen Konstellation ist das normierte Einsehens in Akten mit dem Schutz der Grundrechte der Gefangenen und auch mit den Vorgaben des Artikel 10 der Richtlinie (EU) 2016/680 vereinbar, zumal die Mitglieder der genannten Stellen selbst strengen Verfahrensregeln unterliegen. Die Vorschrift erlaubt es auch Berufsgeheimnisträgern, den Mitgliedern der genannten Stellen Auskünfte und Erläuterungen zum Inhalt der Gesundheitsakten und Krankenblätter zu geben.

Zu § 43 Offenlegen personenbezogener Daten gegenüber wissenschaftlichen Einrichtungen

Die Vorschrift löst § 139 JVollzGB LSA ab und hebt den Verweis auf § 476 Strafprozessordnung auf. Inhaltlich entspricht sie § 476 Strafprozessordnung, geht allerdings darüber hinaus und erlaubt das Offenlegen personenbezogener Daten für wissenschaftliche Zwecke, nicht nur in der Form des Erteilens von Auskünften und dem Gewähren von Akteneinsicht, sondern erfasst zusätzlich auch in Dateisystemen gespeicherte personenbezogene Daten. Hierdurch wird das Verarbeiten personenbezogener Daten für wissenschaftliche Zwecke in ihrer Effizienz gesteigert. Gleichzeitig wird der in § 6 enthaltene Grundsatz konkretisiert und Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 im Fachrecht umgesetzt.

Zu § 44 Verantwortung und Verfahren beim Offenlegen personenbezogener Daten

Absatz 1 überträgt die Verantwortung für das Prüfen der Zulässigkeit des Offenlegens personenbezogener Daten grundsätzlich der offenlegenden Justizvollzugsbehörde und regelt das Verfahren, sofern das Offenlegen auf Ersuchen einer anderen Stelle erfolgt.

Absatz 2 dient dem Umsetzen von Artikel 4 Absatz 1 Buchstabe d und Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680. Absatz 3 dient dem Umsetzen von Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680. Absatz 4 dient dem Umsetzen von Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680.

Absatz 5 ist Ausfluss des Erforderlichkeitsgrundsatzes. Typischerweise ist das Offenlegen personenbezogener Daten, die einer konkreten Person zugeordnet werden können, gegenüber nicht öffentliche Stellen nicht erforderlich. Um betroffene Personen in diesen Fällen zu schützen, sind personenbezogene Daten deshalb grds. zu pseudonymisieren.

Das Pseudonymisieren personenbezogene Daten ist in § 3 Nummer 10 definiert. Nur sofern dies dem Erfüllen des Offenlegungszwecks zuwiderläuft, ist ausnahmsweise vom Pseudonymisieren personenbezogener Daten Abstand zu nehmen. Das ist etwa der Fall, wenn im Rahmen der Entlassungsvorbereitung eine Wohnung gesucht oder ein Arbeitsverhältnis angebahnt werden soll. Die Gefangenenbuchnummer ist im Justizvollzug ein praktikables Instrument, um den Interessen der Gefangenen am Pseudonymisieren ihrer personenbezogenen Daten gerecht zu werden.

Absatz 6 regelt die Verpflichtung der Empfänger personenbezogener Daten, diese nur zu den Zwecken weiterzuverarbeiten, zu denen sie die personenbezogenen Daten auch erhalten haben. Für andere Zwecke dürfen die offengelegten personenbezogenen Daten nur unter den Voraussetzungen von Satz 2 weiterverarbeitet werden. Satz 3 enthält die Verpflichtung der Justizvollzugsbehörden, die Empfänger personenbezogener Daten auf die Zweckbindung der offengelegten personenbezogenen Daten nach Satz 1 und 2 hinzuweisen. Die Regelung soll Missbrauch vorbeugen. Die Justizvollzugsbehörden haben als verantwortliche Stelle dafür Sorge zu tragen, dass die Empfänger personenbezogener Daten Kenntnis über ihre nach diesem Gesetz bestehenden Verpflichtungen erhalten.

Zu Unterabschnitt 4 - Offenlegen personenbezogener Daten durch Übermitteln an Drittstaaten und an internationale Organisationen

Dieser Unterabschnitt regelt das Offenlegen personenbezogener Daten durch Übermitteln gegenüber Drittstaaten und internationalen Organisationen. Mit der Überschrift des Unterabschnittes wird, insbesondere vor dem Hintergrund der Begriffsbestimmungen in § 3 Nummer 5, klargestellt, dass als Handlungsform des Offenlegens ausschließlich das Übermitteln personenbezogener Daten zulässig ist. Das Offenlegen personenbezogener Daten durch das Verbreiten oder eine andere Form des Bereitstellens ist nach diesem Unterabschnitt ausgeschlossen. § 42 stellt hier als Lex specialis eine gesetzliche Ausnahme dar.

Zu § 45 Allgemeine Voraussetzungen

Die Vorschrift setzt Artikel 35 der Richtlinie (EU) 2016/680 um und statuiert Voraussetzungen, die beim Offenlegen personenbezogener Daten gegenüber den verantwortlichen Stellen in Drittstaaten oder gegenüber internationalen Organisationen vorliegen müssen. Darüber hinaus sie zusätzliche Anforderungen an das Offenlegen personenbezogener Daten gegenüber den verantwortlichen Stellen in Drittstaaten oder gegenüber internationalen Organisationen, auch an die insbesondere nach den §§ 45 bis 48 erforderlichen Abwägungsentscheidungen, aufgrund der Rechtsprechung des Bundesverfassungsgerichts (so etwa in BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 u. 1 BvR 1140/06). Insbesondere fordert Absatz 2 das Unterbleiben des Offenlegens personenbezogener Daten, wenn im Einzelfall der Anlass zur Besorgnis besteht und diese Besorgnis auch nach dem Prüfen durch die Justizvollzugsbehörden weiterbesteht, dass ein, elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den offengelegten personenbezogenen Daten beim Empfänger nicht gesichert ist.

Zu § 46 Offenlegen personenbezogener Daten bei geeigneten Garantien

Die Vorschrift dient dem Umsetzen von Artikel 37 der Richtlinie (EU) 2016/680. In § 46 werden die § 45 ergänzenden Voraussetzungen für das Offenlegen personenbezogener Daten gegenüber den verantwortlichen Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 gefasst hat, formuliert. Bei solchen Konstellationen kommt den Justizvollzugsbehörden, insbesondere nach § 46 Absatz 1 Absatz 1 Nummer 2 die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Die auf der Grundlage dieses Gesetzes bestehenden Verpflichtungen der Justizvollzugsbehörden, nach einem solchen Beurteilen das Offenlegen personenbezogener Daten durch das Mitgeben von Verarbeitungsbedingungen, zu verbinden, sind dazu geeignet, das Beurteilen zu dokumentieren und ihr Ergebnis zu sichern. Im Zusammenhang mit dem auch hier anwendbaren § 46 Absatz 2 entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaates beim Prüfen des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Absatz 2 dient dem Umsetzen von Artikel 37 Absatz 3 der Richtlinie (EU) 2016/680 zum Dokumentieren des nach § 46 erfolgten Offenlegens personenbezogener Daten.

Absatz 3 dient dem Umsetzen von Artikel 37 Absatz 2 der Richtlinie (EU) 2016/680, der das Unterrichten des Landesbeauftragten für den Datenschutz über Kategorien des Offenlegens personenbezogener Daten vorsieht, die ohne Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen des Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach dem entsprechenden Beurteilen durch die offenlegende Justizvollzugsbehörde erfolgen.

Zu § 47 Offenlegen personenbezogener Daten ohne geeignete Garantien

Die Vorschrift dient dem Umsetzen von Artikel 38 der Richtlinie (EU) 2016/680 und beleuchtet Konstellationen, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in § 46 erwähnten Garantien in Form eines

rechtsverbindlichen Instruments oder nach Beurteilen durch die offenlegende Justizvollzugsbehörde bestehen.

Zu § 48 Sonstiges Offenlegen personenbezogener Daten gegenüber Drittstaaten

Die Vorschrift dient dem Umsetzen von Artikel 39 der Richtlinie (EU) 2016/680. Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Rahmen des Justizvollzuges tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa das Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit dem Offenlegen personenbezogener Daten verbunden sind. Für dieses Offenlegen personenbezogener Daten „im besonderen Einzelfall“ gelten die in § 48 Absatz 1 genannten strengen Voraussetzungen. In Absatz 4 ist eine verstärkte Zweckbindung der gemäß § 38 offengelegten Daten vorgesehen.

Zu Unterabschnitt 5 - Besondere Bedingungen

Zu § 49 Auftragsverarbeiter

Die Vorschrift dient dem Umsetzen von Artikel 22 der Richtlinie (EU) 2016/680 und stellt Anforderungen auf, wenn die Justizvollzugsbehörden Auftragsverarbeitungsverhältnisse eingehen wollen. Am bisherigen Regelungsansatz, wonach es für das Offenlegen personenbezogener Daten gegenüber einem Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, ändert sich durch das Umsetzen der Richtlinien nichts.

Absatz 1 greift die Regelung des § 11 Absatz 1 BDSG a. F. auf. In Anlehnung an die bisherige Regelung in § 8 Absatz 1 DSG LSA wird klargestellt, dass bei jedem Verarbeiten personenbezogener Daten durch einen Auftragsverarbeiter die Kontrolle durch den Landesbeauftragten für den Datenschutz sicherzustellen ist. Dies hat ggf. durch das vertragliche Festlegen dieser Bedingung zu erfolgen.

Absatz 2 beschreibt die an Auftragsverarbeiter zu stellende Anforderungen und setzt Artikel 22 Absatz 1 der Richtlinie (EU) 2016/680 um.

In Absatz 3 werden die Voraussetzungen für das Eingehen von Unterauftragsverarbeitungs-verhältnissen normiert und dadurch Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt. Durch die Unterrichtungspflicht in Satz 2 wird dem Verantwortlichen die Möglichkeit eingeräumt, gegen Änderungen in Bezug auf das Hinzuziehen oder das Ersetzen anderer Auftragsverarbeiter Einspruch zu erheben.

In Absatz 4 wird, durch das Übernehmen von Elementen aus Artikel 28 Absatz 4 der Verordnung (EU) 2016/679, das Überführen der Pflichten eines Auftragsverarbeiters auch auf dessen Unterauftragnehmer thematisiert.

In Absatz 5 werden die erforderlichen Inhalte einer jedem Verarbeiten personenbezogener Daten durch Auftragsverarbeiter zugrundeliegenden Vereinbarung niedergelegt. Diese Inhalte sind Artikel 22 Absatz 3 der Richtlinie (EU) 2016/680 und Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 entnommen. So werden in Satz 2 Nummer 1 Elemente aus Artikel 28 Absatz 3 Buchstabe a der VERORDNUNG (EU)

2016/679, in Nummer 5 Elemente aus Artikel 28 Absatz 3 Buchstabe h, in Nummer 7 Elemente aus Artikel 28 Absatz 3 Buchstabe c und in Nummer 8 Elemente aus Artikel 28 Absatz 3 Buchstabe f der Verordnung (EU) 2016/679 aufgenommen.

Absatz 6 trifft im Umsetzen von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680 Aussagen zur Form der Vereinbarung und Absatz 7 setzt Artikel 22 Absatz 5 der Richtlinie (EU) 2016/680 um.

Zu § 50 Funktionsübertragung

Die Vorschrift regelt die Voraussetzungen des Verarbeitens personenbezogener Daten durch öffentliche oder nicht öffentliche Stellen oder Personen, denen ganze Aufgaben des Vollzuges zur eigenständigen Erledigung innerhalb des räumlichen und organisatorischen Bereichs der Justizvollzugsbehörden übertragen wurden oder übertragen werden sollen. Die Befugnisnorm zum Übertragen von vollzuglichen Aufgaben selbst befindet sich in den Vollzugsgesetzen der Länder, in Sachsen-Anhalt beispielsweise in § 109 Absatz 1 JVollzGB LSA und § 98 Absatz 1 SVVollzG LSA.

Beim Übertragen von vollzuglichen Aufgaben an eine öffentliche oder nicht öffentliche Stelle (Auftragnehmer) zum selbstständigen Erledigen steht das Erfüllen der Sachaufgabe für die Justizvollzugsbehörden (Auftraggeber) im Vordergrund und nicht der Vorgang des Verarbeitens personenbezogener Daten selbst.

Geht mit dem Übertragen der Sachaufgabe zu deren Erfüllen (quasi als Annex) notwendigerweise auch das Verarbeiten personenbezogener Daten einher, handelt es sich in der datenschutzrechtlichen Terminologie um eine sog. Funktionsübertragung.

Diese wird allgemein bereits dann angenommen, wenn dem Auftragnehmer eigene Entscheidungsbefugnisse hinsichtlich der Art und der Auswahl der personenbezogenen Daten zustehen, dieser die ihm bei der Funktionsübertragung übertragene Aufgabe zumindest in Teilbereichen selbstständig erledigt und der Auftraggeber auf das Erledigen und damit auf das Verarbeiten der personenbezogenen Daten im Einzelfall nicht mehr oder nur noch teilweise Einfluss nehmen kann.

So wird also nur noch im Rahmen des vertraglich Vereinbarten eine Dienstleistung erbracht, die über das weisungsabhängige technische Verarbeiten personenbezogener Daten hinausgeht, der Auftragnehmer für die Zulässigkeit des Verarbeitens personenbezogener Daten zum Erfüllen der übertragenen Aufgaben verantwortlich ist und ihm hierzu auch Rechte zum Verwenden der personenbezogener Daten für eigene Zwecke überlassen sind und er ein eigenes Interesse an dem Verarbeiten personenbezogener Daten hat.

Das Verarbeiten personenbezogener Daten durch einen Auftragsverarbeiter hingegen zeichnet sich durch ein strikt weisungsgebundenes Verarbeiten personenbezogener Daten durch einen Auftragnehmer aus. Des Weiteren müssen die Vorgänge des Verarbeitens personenbezogener Daten selbst den Gegenstand des Auftragsverhältnisses bilden, d. h. den Vertragsgegenstand maßgeblich prägen (z. B. Verträge über das Vernichten und Entsorgen von Datenträgern). Die Vorgänge des Verarbeitens personenbezogener Daten des Auftragnehmers (Auftragsverarbeiters) werden dabei allein dem Auftraggeber (Justizvollzugsbehörden) als verantwortliche Stelle zugerechnet. Der Auftragsverarbeiter handelt hier quasi nur als „verlängerter Arm“

des Auftraggebers und gilt damit im datenschutzrechtlichen Sinne nicht als „Dritter“, weshalb es in diesem Verhältnis auch keiner datenschutzrechtlichen Befugnisse zum Offenlegen personenbezogener Daten bedarf.

Das zulässige Übertragen vollzuglicher Aufgaben zum eigenständigen Erledigen stellt demzufolge im datenschutzrechtlichen Sinn eine sog. Funktionsübertragung dar, die ihrerseits gesetzlicher Grundlagen zum Verarbeiten personenbezogener Daten bedarf, soweit zum Erledigen der übertragenen vollzuglichen Aufgaben zwingend auch personenbezogene Daten verarbeitet werden müssen.

Als Funktionsübertragung an interne private Stellen kann jede Form der funktionellen Privatisierung bzw. des Einsatzes von Verwaltungshelfern im Justizvollzug, insbesondere die weitgehend selbstständige Organisation der Gefangenenarbeit oder Versorgung der Gefangenen und deren medizinische Betreuung oder fachdienstliche Behandlung (Psychologen und Sozialarbeiter etc.), die Heranziehung privater Kaufleute zur weitgehend selbstständigen Abwicklung des Anstaltseinkaufes oder die Unterstützung durch private Sicherheitshilfsdienste in der Pforte innerhalb der Anstalten oder im Fuhrpark und Fahrdienst der Anstalten angesehen werden.

Für das Ausgestalten von Funktionsübertragungen stellt Absatz 2 Regeln über das Auswählen des Auftragnehmers (Satz 1), das Gewährleisten der datenschutzrechtlichen Standards (Satz 2), das schriftliche oder in einem elektronischen Format festzulegende Erteilen des Auftrages (Satz 3), zum Gegenstand und zum Umfang der Aufgabenübertragung, zur Erforderlichkeit des Verarbeitens personenbezogener Daten zum Erfüllen übertragener Aufgaben und das förmliche Verpflichten des hierfür einzusetzenden Personals nach § 1 des Verpflichtungsgesetzes (Satz 4) auf und wird hierdurch in dem erforderlichen Maße konkretisiert. Nach Satz 5 verpflichtet den Auftraggeber, das Einhalten der vom Auftragnehmer getroffenen datenschutzrechtlichen Maßnahmen regelmäßig zu überprüfen und dies zu dokumentieren.

Soweit zum Erfüllen der übertragenen Vollzugsaufgaben personenbezogene Daten verarbeitet werden, finden nach Absatz 3 auf das Verarbeiten personenbezogener Daten die Vorschriften dieses Gesetzes Anwendung. Bei der Funktionsübertragung an externe Stellen zum eigenständigen Erfüllen der übertragenen Vollzugsaufgaben außerhalb der Anstalten richtet sich das Verarbeiten personenbezogener Daten nach den für die externen Einrichtungen geltenden Vorschriften.

Zu § 51 Verarbeiten personenbezogener Daten auf Weisung des Verantwortlichen

Die Vorschrift setzt Artikel 23 der Richtlinie (EU) 2016/680 um.

Zu § 52 Gemeinsam Verantwortliche

Die Vorschrift setzt Artikel 21 der Richtlinie (EU) 2016/680 um. Zum Schutz der Rechte und Freiheiten der betroffenen Personen bedarf es einerseits des Festlegens der konkreten Verantwortungsbereiche und Zuständigkeiten der am Verarbeiten personenbezogener Daten einer betroffenen Person beteiligten Stellen in einer Vereinbarung.

Zu § 53 Elektronisches Führen von Akten

Die Vorschrift trägt der technischen Entwicklung Rechnung, erlaubt nunmehr ausdrücklich auch das Führen elektronischer Akten im Justizvollzug und bildet hierfür die gesetzliche Grundlage für diese Art des Führens von Akten. Soweit in den Vorschriften dieses Gesetzes auf Akten Bezug genommen wird, gelten diese Vorschriften für das elektronische Führen von Akten entsprechend.

Zu § 54 Zentrales Datei-, Buchhaltungs- und Abrechnungssystem

Der Justizvollzug betreibt seit mehreren Jahren ein zum Erfüllen seiner Aufgaben nach den Vollzugsgesetzen erforderliches Zentrales Datei-, Buchhaltungs- und Abrechnungssystem. In diesem System werden personenbezogene Daten betroffener Personen zu vollzuglichen Zwecken, zu Zwecken des Sicherstellens des Verfolgens und Ahndens von Straftaten und Ordnungswidrigkeiten und des Abwehrens von Gefahren sowie zu Zwecken des gegenwärtigen und zukünftigen Gewährleistens des ordnungsgemäßen Durchführens von Strafverfahren verarbeitet, deren Verarbeiten sich nach den Justizvollzugsgesetzen richtet und für das insoweit das für den Justizvollzug bereichsspezifische Datenschutzrecht gilt.

Die Vorschrift benennt in Absatz 1 beispielsweise die Möglichkeit des Standardisierens von Protokollierungstätigkeiten im Rahmen des Offenlegens personenbezogener Daten gegenüber anderen Stellen.

Absatz 2 konkretisiert in Satz 1 die Pflicht der Justizvollzugsbehörden zum Sicherstellen technisch Maßnahmen beim Verwenden von technischen Systemen beim Verarbeiten personenbezogener Daten und trägt damit den Anforderungen der Artikel 20 Absatz 1 und 29 Absatz 1 der Richtlinie (EU) 2016/680 Rechnung, wonach für die jeweiligen Verfahren technische und organisatorische Maßnahmen zum Schutz des Rechts auf informationelle Selbstbestimmung zu treffen sind.

Zum Umsetzen der Pflichten Satz 1 erlaubt Satz 2 den Justizvollzugsbehörden zum Vergeben von Zugriffsberechtigungen für die Nutzer dieses Systems, ein abgestuftes Rechte- und Rollenkonzept zu erstellen und zu verwenden. Dies entspricht der seit Jahren gängigen Praxis im Justizvollzug der Länder und hat sich, insbesondere mit Blick auf das Verarbeiten personenbezogener Daten betroffener Personen erfolgreich als hierfür geeignete Schutzmaßnahme etabliert. Satz 3 stellt klar, dass das Erstellen und das Fortschreiben des abgestuften Rechte- und Rollenkonzeptes unter dem Beteiligen des und dem Überwachen durch den behördlichen Datenschutzbeauftragten der jeweiligen Justizvollzugsbehörde zu erfolgen hat. Satz 4 enthält für diese Fälle die Pflicht der Justizvollzugsbehörden, den Landesbeauftragten für den Datenschutz zu unterrichten.

Zu § 55 Einrichten automatisierter Verfahren

§ 55 stellt die zentrale Vorschrift für das Einrichten automatisierter Verfahren zum Offenlegen oder Abrufen personenbezogener Daten dar.

Absatz 1 ermöglicht das Einrichten automatisierter Verfahren zum erforderlichen Austauschen und Abrufen personenbezogener Daten (bspw. auch aus Vorinhaftie-

rungen) zwischen den Justizvollzugsbehörden. Die Vorschrift trägt damit auch den Anforderungen der Artikel 20 Absatz 1 und 29 Absatz 1 der Richtlinie (EU) 2016/680 Rechnung.

Absatz 2 schafft für die Staatsanwaltschaften bei den Gerichten des Landes eine Rechtsgrundlage zum Abrufen personenbezogener Daten im automatisierten Verfahren, soweit diese Daten für die Zwecke der Strafrechtspflege erforderlich sind. Der Begriff der Strafrechtspflege ist weit zu verstehen. Er umfasst, neben dem Durchführen von Straf- und Bußgeldverfahren und Vollstrecken der Entscheidungen der Strafgerichte, auch die damit in innerem Zusammenhang stehenden Maßnahmen der Justizbehörden zum Ermöglichen des geordneten Durchführens der Strafverfolgung und Strafvollstreckungstätigkeiten, einschließlich der Tätigkeiten, die geeignet sein können, das Entschließen erst zu ermöglichen, ob überhaupt Strafverfolgungsmaßnahmen rechtfertigende Sachverhalte gegeben sind und ob ein staatlicher Strafverfolgungsanspruch verfolgt werden soll. Als anerkannter Beispiele gelten dafür u. a. das Führens des Bundeszentralregisters über Vorstrafen, des Erziehungsregisters jugendlicher Straftäter, das Verwalten von Akten und das Erstellen der Schöffenlisten.

Absatz 3 stellt klar, dass das automatisierte Offenlegen der in § 32 Absatz 2 des Bundeskriminalamt Gesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 2 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354) geändert worden ist, jeweils angeführten personenbezogenen Daten unberührt bleibt.

Absatz 4 erlaubt es dem Land, unter den Voraussetzungen von Absatz 1, beispielsweise einen Verbund mit anderen Ländern und dem Bund für automatisierte Verfahren oder zum Austausch personenbezogener Daten zu Vorinhaftierungen mit anderen Ländern und dem Bund einzugehen. Die Vorschriften über die Zulässigkeit für den Einzelabruf personenbezogener Daten bleibt hiervon unberührt. Innerhalb der automatisierten Verfahren oder des Verbundsystems muss das Verarbeiten personenbezogener Daten selbst daher auch den jeweils einschlägigen Zulässigkeitsanforderungen für das Verarbeiten dieser personenbezogenen Daten in den jeweiligen Kategorien entsprechen.

Zu § 56 Verantwortung und Verordnungsermächtigung

Absatz 1 bestimmt im Grundsatz die Verantwortung des für Justizvollzug zuständigen Ministeriums in den Fällen des Einrichtens von automatisierten Verfahren, Verbundverfahren und Verbunddateisystemen und ermächtigt dieses gleichzeitig zum Delegieren dieser Verantwortung auf eine für die jeweilige Fachverfahren bestimmte Stelle durch Verordnung.

Absatz 2 stellt klar, dass beim Offenlegen oder Abrufen personenbezogener Daten im automatisierten Verfahren oder im automatisierten Verbundverfahren, die Empfänger die Verantwortung für die Rechtmäßigkeit des Abrufes tragen.

Absatz 3 bestimmt alle an einem gemeinsamen Datenverbund beteiligten Stellen zu gemeinsam Verantwortlichen und ermöglicht es somit der betroffenen Person, ihre Rechte, die vom Verarbeiten personenbezogener Daten beeinträchtigt sein könnten, effektiv durchsetzen zu können.

Absatz 4 stellt klar, dass jede an einem Verbund zum Verarbeiten personenbezogener Daten beteiligte Stelle für die in ihrem Zuständigkeitsbereich vorgenommenen Vorgänge des Verarbeitens personenbezogener Daten die technischen und organisatorischen Maßnahmen zu treffen hat, die erforderlich sind, und gewährleisten muss, dass die Vorgänge des Verarbeitens personenbezogener Daten nach Maßgabe von § 16 protokolliert werden.

Absatz 5 enthält die Ermächtigung des für Justizvollzug zuständigen Ministeriums, durch Verordnung die Einzelheiten der elektronischen Aktenführung und des Einrichtens automatisierter Offenlegungs- und Abrufverfahren zu bestimmen sowie der IT-Leitstelle für den Justizvollzug die Pflichten zum Gewährleisten der Sicherheit personenbezogener Daten und die entsprechende Weisungsbefugnis gegenüber den Anstalten zu übertragen. Zudem muss die Verordnung Maßnahmen zur Datensicherung und zur Kontrolle vorsehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen und die Empfänger, die Kategorien der personenbezogenen Daten und die Zwecke des Offenlegens und des Abrufens festlegen. Der Landesbeauftragte für den Datenschutz ist zu unterrichten. Dies entspricht den Vorgaben der Artikel 20 Absatz 1 und 29 Absatz 1 der Richtlinie (EU) 2016/680 und setzt gleichzeitig die verfassungsgerichtliche Rechtsprechung zum flankierenden Grundrechtsschutz durch Kontrolle und Transparenz behördlichen Handelns um (BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, Juris Rn. 134 f.).

Zu Unterabschnitt 6 - Schutz von Geheimnisträgern

Zu § 57 Geheimnisträger

Die Vorschrift entspricht § 153 JVollzGB LSA und setzt Artikel 10 der Richtlinie (EU) 2016/680 um.

In Absatz 1 sind im und für den Justizvollzug ständig oder vorübergehend tätigen Personen aufgeführt, die einer gesetzlichen Geheimhaltungspflicht unterliegen bzw. 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 Verschwiegenheits-verpflichtung. Für diese Personen wie auch für die in Absatz 1 Satz 1 Nummer 4 genannten Seelsorger schreibt Absatz 1 Satz 1 die grundsätzliche Verschwiegenheit untereinander sowie gegenüber den Justizvollzugsbehörden vor. Diese Schweigepflicht erfasst nach Absatz 1 Satz 2 auch ihre Gehilfen und die Personen, die zur Berufsausübung bei ihnen tätig sind, jedoch nicht im Verhältnis zu den Berufsträgerinnen und Berufsträgern selbst, und Dolmetscher.

Um das effektive Behandeln und Betreuen der Gefangenen im Rahmen des verfassungsrechtlich gebotenen Auftrages zur Resozialisierung zu gewährleisten, macht Absatz 2 Satz 1 im Verhältnis der Berufsgeheimnisträger untereinander und abweichend von Absatz 1 eine Ausnahme und verpflichtet Berufsgeheimnisträger beim Vorliegen der genannten Voraussetzungen zum umfassenden gegenseitigen Informieren und Erteilen von Auskünften.

Die Auskunftspflichten und die Informationspflichten gelten auch berufsgruppenübergreifend. Ärzte können sich also gegenüber Psychologen nicht auf ihre ärztliche Schweigepflicht berufen und andersherum. Seelsorger sind keine Berufsgeheimnisträger im Sinne dieser Vorschrift. Das ungestörte Ausüben ihrer Tätigkeit erfährt be-

reits besonderen verfassungsrechtlichen Schutz und somit bestehen bei ihnen keine Offenbarungspflichten. Nach Satz 2 ist Aufgabe der Justizvollzugsbehörden, Berufsgeheimnisträger außerhalb des Justizvollzuges über die Offenbarungspflichten und -befugnisse nach diesem Gesetz in Kenntnis zu setzen, da nicht davon ausgegangen werden kann, dass diese, ohne eine solche Information, Kenntnis über diese besonderen Verpflichtungen haben.

Insgesamt ermöglicht die Vorschrift den Behandlern und Betreuern, ihre Interaktion mit den Gefangenen entsprechend zu gestalten und vermeidet dadurch spätere Komplikationen, wenn z. B. die Justizvollzugsbehörden Auskunft zu bestimmten Behandlungsergebnissen verlangen, um die Vollzugs- und Eingliederungspläne der Gefangenen fortzuschreiben und die richtigen Maßnahmen zur Resozialisierung der Gefangenen festzulegen.

Zu § 58 Pflicht der Berufsgeheimnisträger zum Offenbaren personenbezogener Daten

Die Vorschrift entspricht § 154 JVollzGB LSA, dient dem Umsetzen von Artikel 10 der Richtlinie (EU) 2016/680 und stellt eine Rechtfertigungsnorm für die Berufsgeheimnisträger innerhalb und außerhalb des Justizvollzuges dar.

Die Berufsgeheimnisträger sind unter den Voraussetzungen von Absatz 1 verpflichtet, die ihnen bekannt gewordenen personenbezogenen Daten gegenüber dem Anstaltsleiter zu offenbaren.

Über Absatz 1 hinaus regelt Absatz 2 die besonderen Voraussetzungen, unter denen die Berufsgeheimnisträger verpflichtet sind, personenbezogene Daten gegenüber dem Anstaltsleiter zu offenbaren, damit dieser selbst, die ihm obliegenden Verpflichtungen - auch gegenüber dem Gefangenen - erfüllen kann. Die Vorschrift schließt damit eine bisher vorhandene Regelungslücke, die in der Praxis bisher beispielsweise dazu geführt hat, dass Gefangene, die zur medizinischen Behandlung und Betreuung in eine medizinische Einrichtung außerhalb des Justizvollzuges verbracht wurden und bei denen hierzu vereinzelt auch das Vollstrecken der Strafe unterbrochen werden musste, die Gefangenen die medizinische Einrichtung zu weiteren Behandlung in einer anderen Einrichtung oder aus anderen Gründen verlassen hatten und weder die Justizvollzugsbehörden noch die Strafvollstreckungsbehörden hierüber von der medizinischen Einrichtung informiert wurden. Infolgedessen, konnten zunächst keine Maßnahmen zum (Fortführen) der Strafvollstreckung getroffen werden. Zudem konnte hier weder durch die Justizvollzugsbehörden noch durch die Strafvollstreckungsbehörden sichergestellt werden, dass die Gefangenen ohne jegliches Kontrollieren und Überwachen keine weiteren Straftaten während der Abwesenheit von den Anstalten begehen werden. Diesen, den Schutz der Allgemeinheit gefährdenden Zuständen wird mit der Neuregelung wirksam begegnet.

Nach Absatz 3 haben Sozialarbeiter und Sozialpädagogen, die als Bedienstete im Justizvollzug tätig sind, über Absatz 1 hinaus weitergehende Offenbarungspflichten. Sie sind als Bedienstete Teil der Anstalten und haben keine besondere Vertrauensstellung, wie sie üblicherweise außerhalb des Justizvollzuges besteht. Deshalb müssen sie ihre Kenntnisse dem Anstaltsleiter gegenüber bereits dann offenbaren, wenn dies für die Erfüllung der in § 1 genannten Zwecke erforderlich ist.

Zu § 59 Befugnis der Berufsgeheimnisträger zum Offenbaren personenbezogener Daten

Die Vorschrift entspricht § 155 JVollzGB LSA und setzt Artikel 10 der Richtlinie (EU) 2016/680 um. Regelmäßig können Berufsgeheimnisträger aufgrund eigener Sachkunde am besten beurteilen, inwieweit die ihnen bekannt gewordenen personenbezogenen Daten zum Erfüllen der in § 1 genannten Zwecke, auch unter Berücksichtigung des Gefangeneninteresses am Geheimhalten, erforderlich sind. Deshalb sie entscheiden, ob sie Informationen gegenüber dem Anstaltsleiter offenbaren. Die Vorschrift stellt eine Rechtfertigungsnorm für Berufsgeheimnisträger dar. Es obliegt den Justizvollzugsbehörden, die Berufsgeheimnisträger, die außerhalb des Justizvollzuges tätig sind, über die hier eingeräumten Befugnisse zu informieren.

Zu § 60 Pflicht zum Unterrichten

Die Vorschrift entspricht § 156 JVollzGB LSA und dient dem Umsetzen von Artikel 10 und Artikel 12 Absatz 2 der Richtlinie (EU) 2016/680.

Damit die Gefangenen selbstbestimmt über das Preisgeben von Informationen entscheiden können, müssen sie über die Offenbarungspflichten und -befugnisse der Berufsgeheimnisträger informiert sein. Um Missverständnisse zu vermeiden und zum Nachweis von ausreichenden Informationen muss das Unterrichten der Gefangenen durch die Berufsgeheimnisträger nach Absatz 1 Satz 1 in der Regel vor dem Erheben personenbezogener Daten schriftlich erfolgen.

Als verantwortliche Stellen müssen die Justizvollzugsbehörden beim Einschalten von Berufsgeheimnisträgern von außerhalb der Anstalten nach Satz 2 selbst dafür zu sorgen, dass die Gefangenen vor dem Erheben personenbezogener Daten durch die Berufsgeheimnisträger über deren Pflichten und Befugnisse zum Offenbaren personenbezogener Daten informiert sind.

Während in Absatz 1 das grundsätzliche und abstrakte Vorabinformieren der Gefangenen geregelt ist, schreibt Absatz 2 Satz 1 das Benachrichtigen der Gefangenen nach dem konkreter Offenbaren personenbezogener Daten vor, damit die Gefangenen über das tatsächliche Weiterleiten ihrer personenbezogenen Daten im Einzelfall Kenntnis erhalten.

Zu § 61 Zweckbindung nach dem Offenbaren personenbezogener Daten

Die Vorschrift entspricht § 157 JVollzGB LSA. Wegen der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung beim Offenbaren von personenbezogenen Daten aus einem besonderen Vertrauensverhältnis schreibt Satz 1 die strenge Zweckbindung der offenbarten personenbezogenen Daten vor. Liegen diese Voraussetzungen vor, kann der Anstaltsleiter nach Satz 2 allgemein festlegen, gegenüber welchen anderen Bediensteten das Offenbaren dieser personenbezogenen Daten erfolgen darf. Dies entspricht u. a. § 107 Absatz 1 JVollzGB LSA, wonach Aufgaben der Anstaltsleitung auch auf andere Bedienstete übertragen werden dürfen.

Zu § 62 Zugriff auf personenbezogene Daten in Notfällen

Die Bestimmung entspricht § 158 JVollzGB LSA und setzt Artikel 8 der Richtlinie (EU) 2016/680 um. Satz 1 ermöglicht den Zugriff auf personenbezogene Daten in Notfällen und stellt damit klar, dass Regelungen zum Schutz personenbezogener Daten das Retten eines Menschen in Notfällen niemals behindern dürfen. Das Kenntnisnehmen dieser personenbezogenen Daten ist jedoch auf die im Justizvollzug tätigen Personen beschränkt, die die personenbezogenen Daten der betroffenen Person nur gegenüber den für die Notfallrettung eingesetzten, im Regelfall anstaltsfremden, Personen vorzunehmen haben. Durch das Verbot des Weiterverarbeitens dieser personenbezogenen Daten zu anderen Zwecken in Satz 2 und durch die Dokumentationspflicht in Satz 3 soll Missbrauchsgefahren vorgebeugt werden.

Zu Unterabschnitt 7 - Löschen und Vernichten, Einschränken des Verarbeitens, Berichtigen personenbezogener Daten

Zu § 63 Löschen und Vernichten personenbezogener Daten

Absatz 1 Satz 1 entspricht § 162 Absatz 1 JVollzGB LSA und normiert den Grundsatz des verpflichtenden Löschens und Vernichtens personenbezogener Daten, soweit nicht einer der dort aufgezählten Ausnahmefälle gegeben ist. Der Ausnahmefall des vollzuglichen Zwecks kann beispielsweise erfüllt sein, wenn Gefangene unter Bewährung oder unter Führungsaufsicht entlassen werden. Absatz 1 dient damit auch dem Umsetzen von Artikel 4 Absatz Buchstabe 1 e) der Richtlinie (EU) 2016/680. Satz 2 verpflichtet die Justizvollzugsbehörden jährlich zu überprüfen, ob personenbezogene Daten gelöscht und vernichtet werden müssen. Satz 3 regelt den Beginn der Jahresfrist. Die dort genannten sonstigen Fälle können z. B. personenbezogene Daten von anstaltsfremden Personen oder Besuchern. Die Sätze 2 und 3 dienen damit auch dem Umsetzen von Artikel 5 der Richtlinie (EU) 2016/680 (vgl. auch Erwägungsgrund 26 am Ende).

Absatz 2 entspricht grds. § 162 Absatz 2 JVollzGB LSA. In Satz 1 werden länderübergreifend für den Vollzug der Freiheitsstrafe, der Jugendstrafe und des Jugendarrestes individuelle Fristen zum Löschen und Vernichten personenbezogener Daten normiert. Die Regelung trägt sowohl Artikel 5 als auch Artikel 6 der Richtlinie (EU) 2016/680 Rechnung. Satz 2 enthält für Fälle, wo eine besondere Vorschrift, beispielsweise die Justizaufbewahrungsverordnung eines Landes, eine längere Aufbewahrungsfrist für die Gefangenenpersonalakten vorsieht, eine Ausnahme. In diesen Fällen liegt ein Fall des § 64 Absatz 1 Nummer 3 vor.

Absatz 3 trägt dem Unterscheiden nach Haftarten ebenfalls Rechnung, wie dies in Artikel 6 der Richtlinie (EU) 2016/680 vorgegeben ist, und folgt aus der gesetzlichen Unschuldsvermutung. Erfasst werden selbstverständlich nicht nur die personenbezogenen Daten dieser besonderen Gefangenenklientel, sondern auch die ihrer Angehörigen und Besucher. Des Weiterverarbeitens dieser personenbezogenen Daten bedarf es nach dem Entlassen der Gefangenen grds. nicht mehr. Gleichzeitig wird Artikel 5 der Richtlinie (EU) 2016/680 Rechnung getragen.

Absatz 4 entspricht § 147 Absatz 3 JVollzGB LSA und dient ebenfalls dem Umsetzen von Artikel 5 der Richtlinie (EU) 2016/680.

Absatz 5 enthält eine Höchstspeicherfrist für Aufzeichnungen nach §§ 26 und 27, die im Hinblick auf die Eingriffsintensität des Erhebens dieser personenbezogenen Daten kurz ist und somit auch Artikel 5 der Richtlinie (EU) 2016/680 umsetzt. Die Vorschrift entspricht inhaltlich grds. §§ 145 Absatz 1 Satz 2 und Absatz 2 Satz 1 JVollzGB LSA.

Die bisherige Frist von (nur) 48 Stunden hat sich in der Praxis nicht bewährt gewährt, sondern als eindeutig zu kurz erwiesen. Dies gilt insbesondere in den Fällen zum Erkennen und Qualifizieren der Zwecke, die ein Weiterverarbeiten dieser personenbezogenen Daten rechtfertigen würden. Hier war in einer Vielzahl der Fälle bereits ein längerer Zeitraum erforderlich, um das entsprechende Material zusammenzutragen und ohne, dass schon ein Bewerten dieses Materials hätte rechtzeitig erfolgen können. Das Anheben dieser Frist ist zum Erfüllen der in § 1 genannten Zwecke unerlässlich und trägt sowohl den Belangen betroffener Personen als auch der Praxis ausreichend Rechnung, da es sich hier nur um eine Höchstspeicherfrist handelt.

Zu § 64 Einschränken des Verarbeitens personenbezogener Daten

Absatz 1 Satz 1 trägt Artikel 16 Absatz 3 der Richtlinie (EU) 2016/680 Rechnung, wonach anstelle des Löschens und Vernichtens personenbezogener Daten aus bestimmten Gründen das Einschränken ihres Verarbeitens möglich ist.

Nummer 1 trägt den hochrangigen Interessen der Gefahrenverhütung, Gefahrenabwehr und Strafverfolgung Rechnung, die durch die Richtlinie (EU) 2016/680 als Verarbeitungszwecke anerkannt sind. Nummer 2 trägt sowohl den Interessen der Verantwortlichen als auch der betroffenen Personen an der sachlichen Richtigkeit personenbezogener Daten Rechnung.

Nummer 3 sieht bei abweichenden gesetzlichen Aufbewahrungsfristen eine entsprechende Ausnahme vom Löschen und Vernichten personenbezogener Daten vor.

Nach Nummer 4 darf das Löschen und Vernichten personenbezogener Daten nicht das Durchsetzen von Rechten der betroffenen Person beeinträchtigen oder vereiteln (vgl. Erwägungsgrund Nummer 47 der Richtlinie (EU) 2016/680).

Nummer 5 trägt u. a. den technischen Bedingungen Rechnung, die einem Löschen und Vernichten personenbezogener Daten entgegenstehen können.

Nummer 6 stellt sicher, dass die Interessen der Verantwortlichen und der betroffenen Personen nach dem Entlassen der Gefangenen geltend gemacht und durchgesetzt werden können. Haben Gefangene z. B. im Vollzug gearbeitet, kann auch noch mehre Jahre nach dem Entlassen der Nachweis über die Beschäftigung gegenüber anderen öffentlichen Stellen erforderlich werden. Ergeben sich aus der Gefangenenpersonalakte Anhaltspunkte für eine spätere Beweisbedürftigkeit einer Tatsache, wird anstelle des Löschens und Vernichtens der personenbezogenen Daten nur das Einschränken ihres Verarbeitens möglich sein.

Nummer 7 dient dem Sicherstellen des Durchführens im öffentlichen Interesse liegender Forschungsvorhaben.

Um den betroffenen Personen das Ausüben ihrer Rechte und eine wirksame Kontrollmöglichkeit des Verarbeitens ihrer personenbezogenen Daten zur Verfügung zu stellen, sieht Nummer 8 einen weiteren Einschränkungstatbestand vor.

Nummer 9 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 dient.

Aufgrund des besonderen Ausnahmecharakters des Einschränkens des Verarbeitens personenbezogener Daten, ist das Weiterverarbeiten dieser personenbezogenen Daten nur unter den in Absatz 2 genannten Voraussetzungen möglich und zulässig. Ist das Verarbeiten dieser personenbezogenen Daten zu Zwecken, zu dem ihr Löschen und Vernichten unterblieben ist, nicht mehr erforderlich, sind diese personenbezogenen Daten unverzüglich zu löschen und zu vernichten. Die Regelung orientiert sich an dem Verhältnismäßigkeits-gebot der Richtlinie (EU) 2016/680 und § 32 Absatz 2 Satz 3 Bundeskriminalamtsgesetz vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 2 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354) geändert worden ist (BKAG).

Absatz 3 sieht, neben dem Einwilligen der betroffenen Person, den wichtigen Anwendungsfall für das Aufheben des Einschränkens des Verarbeitens personenbezogener Daten im Falle einer neuen Inhaftierung vor. In diesem Fall ist es unbedingt erforderlich, personenbezogene Daten zum vormaligen Vollzugsverhalten oder die durchgeführten Behandlungsmaßnahmen erneut abrufen zu können. Die Justizvollzugsbehörden können so ohne Informationsverlust wieder an das bisherige Behandeln und Betreuen der Gefangenen anknüpfen. Das Aufheben des Einschränkens des Verarbeitens personenbezogener Daten ist für die Gefangenen im Übrigen häufig weniger belastend als das vollständige Neuerheben ihrer personenbezogenen Daten.

Wird das Einschränken des Verarbeitens personenbezogener Daten wieder vollständig aufgehoben, richtet sich die Frage des Löschens und Vernichtens dieser personenbezogenen Daten erneut nach § 63.

Absatz 4 enthält eine zum Sichern des Akteneinsichtsrechtes der betroffenen Person abschließende Aufzählung der Gründe, die zum Anbringen eines Vermerkes des Einschränkens personenbezogener Daten berechtigen. Ein solcher Vermerk dient zwar auch den Interessen der betroffenen Personen, indem ein Anschein dafürspricht, dass andere Aktenbestandteile nicht der Akteneinsicht entgegenstehen.

Das Informationsinteresse der betroffenen Person muss aber zurücktreten, wenn der Schutz der genannten Rechtsgüter, eine gesetzliche Geheimhaltungspflicht oder medizinische Gründen allein zum Wohl der betroffenen Person hier den Vorrang beanspruchen. Die weitere Wertigkeit des Vermerkes im Rahmen des Rechts auf informationelle Selbstbestimmung wird durch den eng begrenzten Kreis der zum Anfertigen eines solchen Vermerkes berechtigten Funktionsträger zum Ausdruck gebracht.

Absatz 5 Satz 1 stellt klar, dass auch in den Fällen, in denen das Verarbeiten personenbezogener Daten eingeschränkt ist, die Höchstgrenzen für das Aufbewahren personenbezogener Daten nicht überschritten werden dürfen. Wie Gesundheitsakten und Krankenblätter stellen auch die in Gefangenenpersonalakten und Therapieakten

enthaltenen personenbezogenen Daten äußerst sensible Datensätze dar. In Anlehnung an § 10 Absatz 3 der Berufsordnung der Ärztekammer Sachsen-Anhalt (beschlossen durch die Kammerversammlung am 8.11.1997; genehmigt mit Maßgabe durch das Ministerium für Arbeit, Gesundheit und Soziales des Landes Sachsen-Anhalt am 26.3.1998; zuletzt geändert durch Beschluss der Kammerversammlung am 26.4.2014, genehmigt durch das Ministerium für Arbeit und Soziales am 7.5.2014, bestimmt Satz 1 deshalb für sie eine einheitliche maximale Speicherfrist von zehn Jahren.

Absatz 5 Satz 2 sieht gleichwohl eine Ausnahme von den Höchstgrenzen für das Aufbewahren vor, wenn ein Fall des Absatzes 1 vorliegt, also noch Anhaltspunkte gegeben sind, dass die personenbezogenen Daten zu Zwecken des Absatzes 1 weiterhin erforderlich sind. Satz 3 legt den Fristbeginn fest, wobei die Fristberechnung an das Jahr der aktenmäßigen Weglegung anknüpft. Als dieses gilt entsprechend den Bestimmungen über die Aufbewahrungsfrist für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden bei Gefangenenpersonalakten das Jahr, in dem die letzte Verfügung zur Sache ergangen ist, bei den Gesundheitsakten das Jahr, in dem das letzte personen- und sachbezogene Eintragen erfolgt ist, und bei Gefangenenbüchern das Jahr, in dem der Vollzug bezüglich aller darin aufgeführten Gefangenen beendet ist.

Absatz 6 setzt Artikel 5 Satz 2 der Richtlinie (EU) 2016/680 um, wonach das auch Einschränken des Verarbeitens personenbezogener Daten durch entsprechende Vorkehrungen sichergestellt werden muss.

Zu § 65 Berichtigen personenbezogener Daten

Die Regelung in Absatz 1 Satz 1 enthält ein Umsetzen 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 regelt einen weiteren Fall des Einschränkens des Verarbeitens personenbezogener Daten. Artikel 16 Absatz 3 Buchstabe a der Richtlinie (EU) 2016/680 sieht im (berechtigten) Berichtigen von unrichtigen Daten einen Unterfall des Löschens und Vernichtens. In Anlehnung an § 58 Absatz 1 Satz 3 und 4 des Bundesdatenschutzgesetzes in der Fassung seiner Bekanntmachung vom 30. Juni 2017 soll der Fall des Löschens und Vernichtens personenbezogener Daten wegen des Berichtigens unrichtiger personenbezogener Daten im Vierten Buch Justizvollzugsgesetzbuch Sachsen-Anhalt systematisch als Fall des Berichtigens erfasst werden (vgl. auch Begründung zum Gesetzentwurf der Bundesregierung vom 24. Februar 2017, BT-Drucksache 18/11325, Seite 114). Das Aufheben des Einschränkens des Verarbeitens personenbezogener Daten nach Satz 4 führt daher entweder zum Berichtigen der personenbezogenen Daten oder zu deren uneingeschränkten Verarbeiten.

Nach Absatz 2, der Artikel 16 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 umsetzt, sind unvollständige personenbezogene Daten der betroffenen Person zu vervollstän-

digen oder zu ergänzen, was auch durch eine ergänzende Erklärung erfolgen kann. Dies sollte zur Wahrung der Aktenklarheit und Aktenwahrheit auch für das sonstige Berichtigen personenbezogener Daten gelten.

Zu § 66 Verfahren

Absatz 1 Satz 1 dient dem Umsetzen von Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680. Satz 2 bis 4 dienen dem Umsetzen von Artikel 7 Absatz 3 und Artikel 16 Absatz 6 der Richtlinie (EU) 2016/680.

Der Verpflichtung des Empfängers, das Berichtigen personenbezogener Daten im eigenen Datenbestand vorzunehmen, folgt aus deren eigener Verantwortung, unrichtige personenbezogene Daten unverzüglich zu berichtigen.

Absatz 2 dient dem Umsetzen von Artikel 16 Absatz 4 Satz 1, Absatz 3 dem Umsetzen von Artikel 16 Absatz 4 Satz 2 und Absatz 7 dem Umsetzen von Artikel 16 Absatz 4 Satz 3 der Richtlinie (EU) 2016/680.

Absatz 4 dient dem Schutz, der in Absatz 3 enthaltenen Zwecke.

Absatz 5 entspricht § 162 Absatz 9 JVollzGB LSA.

Absatz 6 dient der Transparenz des Verwaltungshandelns und dem Schutz der Rechte der betroffenen Person. Satz 3 übernimmt dabei den Gedanken aus § 20 Absatz 1 Satz 2 Bundesdatenschutzgesetz 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.

Zu Abschnitt 5 - Rechte der betroffenen Person

Zu § 67 Rechte der betroffenen Person

Die Vorschrift dient dem Umsetzen von Teilen von Artikel 16 der Richtlinie (EU) 2016/680, soweit dieser Betroffenenrechte statuiert. Nach allgemeinen Grundsätzen des Europäischen Rechts (vgl. EuGH, Urteil der Dritten Kammer vom 14. Januar 2010, C 343/08, Rn. 41) müssen alle vom Anwendungsbereich der Richtlinie (EU) 2016/680 betroffenen Personen „klar und genau wissen, welche Rechte und Pflichten sie unter allen Umständen haben“. § 67 benennt daher, unter Verweis auf die §§ 63 bis 65 und die §§ 68 bis 71, klar und eindeutig die subjektiv-öffentlichen Rechte der Gefangenen und anderer betroffener Personen.

Zu § 68 Allgemeine Informationen

Die Vorschrift dient dem Umsetzen von Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680. Sie regelt die Informationspflichten der Justizvollzugsbehörden gegenüber betroffenen Personen, unabhängig vom Geltendmachen von Betroffenenrechten.

Ihren Informationspflichten sollen die Justizvollzugsbehörden in allgemeiner Form nachkommen können. Durch die explizit in Erwägungsgrund 42 der Richtlinie (EU)

2016/680 enthaltene Möglichkeit der Information über die Internetseite des Verantwortlichen wird der Sinn und Zweck der Regelung klargestellt: Betroffene Personen sollen sich, unabhängig vom Verarbeiten personenbezogener Daten im konkreten Fall, in leicht zugänglicher Form einen Überblick über die Zwecke des bei den Justizvollzugsbehörden durchgeführten Verarbeitens personenbezogener Daten verschaffen können und eine Übersicht über die ihnen zu Gebote stehenden Betroffenenrechte erhalten. Bei Gefangenen erfüllen die Justizvollzugsbehörden ihre Verpflichtung bereits durch das schriftliche Erteilen allgemeiner Informationen bei deren Aufnahme im Justizvollzug.

Zu § 69 Benachrichtigen der betroffenen Person

Die Vorschrift betrifft die Fälle, in denen das aktive Benachrichtigen betroffener Personen vorgesehen ist. Das Festlegen, dieser in Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 bezeichneten „besonderen Fälle“, ist nicht zu verallgemeinern. Leitend für Entscheidungen, ob das Benachrichtigen unabhängig vom Geltendmachen eines Betroffenenrechts angezeigt ist, dürfte z. B. sein, ob das Verarbeiten personenbezogener Daten mit oder ohne Wissen der betroffenen Person, ggf. in Verbindung mit einer erhöhten Eingriffstiefe, stattfindet. In letztgenannten Fällen gibt das aktive, ggf. nachträgliche Benachrichtigen der betroffenen Person die einzige Möglichkeit, von dem Verarbeiten der sie betreffenden personenbezogenen Daten Kenntnis zu erlangen und ggf. dessen Rechtmäßigkeit mithilfe des Geltendmachens ihrer Betroffenenrechten zu prüfen.

Absatz 1 stellt klar, welche Informationen der betroffenen Person von den Justizvollzugsbehörden in diesen Fällen aktiv übermittelt werden müssen und dient dabei dem Umsetzen von Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680.

Absatz 2 ermöglicht es, im Umsetzen von Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680, zu den dort genannten Zwecken vom Bereitstellen der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder sie aufzuschieben.

Die Vorschrift geht zum Schutz der betroffenen Person über das durch die Richtlinie (EU) 2016/680 Gebotene hinaus, indem tatbestandlich jeweils eine Gefährdung, gegenüber einer in der Richtlinie (EU) 2016/680 angesprochenen Beeinträchtigung, der genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass das Erteilen einer Auskunft nicht zur Gefährdung des ordnungsgemäßen Erfüllens, insbesondere der Aufgaben der Justizvollzugsbehörden führen darf.

Absatz 3 statuiert ein Zustimmungserfordernis der dort genannten Stellen, wenn sich das Benachrichtigen auf das Offenlegen personenbezogener Daten gegenüber diesen Stellen (nach Absatz 1 Satz 1 Nummer 4) bezieht. Insofern besteht ein, der Situation des aktiven Geltendmachens von Betroffenenrechten vergleichbarer Sachverhalt, weshalb das Übernehmen geboten ist. Die Nutzung der Möglichkeit, vom Bereitstellen der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder aufzuschieben, muss Verhältnismäßigkeitsgrundsätzen genügen, mithin in ein angemessenes Verhältnis zur Bedeutung der Betroffeneninformation für das spätere Geltendmachen von Betroffenenrechten gebracht werden. So haben die Justizvollzugsbehörden im Einzelfall zu prüfen, ob das Bereitstellen etwa nur teil- oder zeitweise eingeschränkt werden kann.

Die Absätze 5 bis 9 dienen dem Umsetzen von Artikel 31 der Richtlinie (EU) 2016/680.

In Absatz 10 wird der in § 76 Absatz 7 enthaltenen Gedanke aufgegriffen, wonach auch beim Benachrichtigen der betroffenen Person die Motivation zum Benachrichtigen über eine Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch das Melden verfügbar werdenden Informationen zum Verarbeiten personenbezogener Daten zum Einleiten eines Strafverfahrens führen können.

Zu § 70 Auskunft an die betroffene Person

Die Vorschrift regelt im Umsetzen 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 das bisherige Recht sah in § 159 JVollzGB LSA Auskunftsrechte vor, die unter bestimmten Voraussetzungen entfallen konnten.

Absatz 1 enthält die objektiv-rechtliche Verpflichtung der Justizvollzugsbehörden zum Erteilen einer Auskunft über die bei den Justizvollzugsbehörden verarbeiteten personenbezogenen Daten der betroffenen Person. Über § 67 besteht das subjektiv-öffentliche Recht der betroffenen Person auf das Erteilen der Auskunft. Gegenüber dem bisherigen Recht erweitert Satz 2 den Umfang der Auskunft und konkretisiert die Verpflichtung aus Satz 1. Wie Erwägungsgrund Nummer 43 der Richtlinie (EU) 2016/680 verdeutlicht, ermöglicht der in den Nummern 1 und 4 genannte Begriff „Kategorie“ den Justizvollzugsbehörden eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten und den Empfängern derartiger personenbezogener Daten. Die Angaben zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Pflicht zur Angabe der verfügbaren Informationen zur Quelle der personenbezogenen Daten bedeutet nicht, dass die Identität von Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Die Justizvollzugsbehörden müssen sich bei der Angabe zu den personenbezogenen Daten, die Gegenstand des Verarbeitens sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über den Umfang und die Art ihrer verarbeiteten Daten zu erzeugen und es ihr so ermöglichen, aufgrund dieser Informationen zu ermessen, ob das Verarbeiten ihrer personenbezogenen Daten rechtmäßig ist und, wenn Zweifel hieran bestehen, ggf. das Geltendmachen weiterer Betroffenenrechte auf diese Informationen stützen zu können.

Absatz 2 orientiert sich an § 19 Absatz 2 und § 33 Absatz 2 Satz 1 des Bundesdatenschutzgesetzes i. d. F. 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 haben die Justizvollzugsbehörden sicherzustellen, dass durch geeignete technische und organisatorische Maßnahmen das Weiterverarbeiten der personenbezogenen Daten zu anderen Zwecken ausgeschlossen ist. Beim Ermitteln des Aufwandes haben die Justizvollzugsbehörden die bestehenden technischen Möglichkeiten, in ihrem Verarbeiten eingeschränkte und

archivierte personenbezogene Daten der betroffenen Personen im Rahmen des Erteilens der Auskunft verfügbar zu machen, zu berücksichtigen. Werden personenbezogene Daten ausschließlich aufgrund von Aufbewahrungsvorschriften gespeichert, ist deren Verarbeiten einzuschränken.

Das Erteilen einer Auskunft unterbleibt in den Fällen von Absatz 3, wenn die betroffenen Personen keine hinreichend konkreten Angaben machen, mit denen sich die verarbeiteten personenbezogenen Daten ermitteln lassen. Macht etwa ein Besucher keine Angaben dazu, welchen Gefangenen er besucht hat, würde die Verpflichtung zum Erteilen einer Auskunft einen unverhältnismäßigen Aufwand der Justizvollzugsbehörden verursachen.

Absatz 4 übernimmt den Katalog aus § 69 Absatz 2, wodurch auch vom Erteilen einer Auskunft abgesehen werden kann. Je nach Umfang der beeinträchtigten Interessen kann von der Auskunft vollständig abgesehen oder diese teilweise eingeschränkt werden. Die Einschränkungen entsprechen Artikel 15 Absatz 1 und Erwägungsgrund Nummer 44 der Richtlinie (EU) 2016/680.

Absatz 5 entspricht § 159 Absatz 4 und Absatz 6 dem § 159 Absatz 6 JVollzGB LSA.

Absatz 7 Sätze 1 und 2 dienen dem Umsetzen 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 das Nichterteilen der Auskunft zu begründen, um dem Gefangenen oder anderen betroffenen Personen das Überprüfen des Nichterteilens der Auskunft zu ermöglichen.

Ist vom Erteilen einer Auskunft gegenüber den betroffenen Personen abzusehen, sieht Absatz 8 Satz 1 im Umsetzen von Artikel 17 der Richtlinie (EU) 2016/680, als neues Verfahren zum effektiven Schutz der Rechte der betroffenen Personen, das Überprüfen der Verarbeitungs-tätigkeiten durch den Landesbeauftragten für den Datenschutz vor. Nach Absatz 8 Satz 1 tritt der Landesbeauftragte für den Datenschutz in die Rechte der betroffenen Personen ein. Die Justizvollzugsbehörden weisen die betroffenen Personen darauf hin, dass sie ihr Auskunftsrecht durch den Landesbeauftragten für den Datenschutz ausüben lassen können, und auf die Möglichkeit zur Inanspruchnahme gerichtlichen Rechtsschutzes. Machen die betroffenen Personen von ihrem Recht Gebrauch, ist dem Landesbeauftragten für den Datenschutz die entsprechende Auskunft zu erteilen. Die Sätze 4 bis 7 regeln das Verfahren des Weitergebens der Ergebnisse der Prüfung an die betroffenen Personen.

Absatz 9 entspricht § 159 Absatz 10 JVollzGB LSA. Die Vorschrift stellt nochmals ausdrücklich klar, dass die Regelungen dieses Gesetzes abschließend sind und so eine unmittelbare gesetzliche Sperrwirkung u. a. gegenüber dem Informationsfreiheitsgesetz vom 5. September 2005 (BGBl. I S. 2722), das durch Artikel 2 Absatz 6 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist oder dem Informationszugangsgesetz Sachsen-Anhalt (IZG LSA) vom 19. Juni 2008, zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Februar 2018 (GVBl. LSA S. 10, 12) entfalten (vgl. auch OLG Naumburg, Beschluss vom 26. Juni 2012, 2 Ws 79/12). Diese gesetzliche Sperrwirkung ist insbesondere aus Gründen der Sicherheit der Anstalten und zum Schutz der Allgemeinheit unabdingbar, um jederzeit beispielsweise den Inhalt von Sicherungsvorkehrungen und -einrichtungen, Alarmplänen oder

Vorgehensweisen und Verhaltensanweisungen der Anstalten bei Vorkommnissen im Justizvollzug (Meuterei, Befreiungen, Geiselnahmen, Evakuierungen u.a.) wirksam geheim halten zu können.

Zu § 71 Akteneinsicht der betroffenen Person

Die Vorschrift entspricht im Wesentlichen § 160 JVollzGB LSA.

Absatz 1 gewährt über Artikel 14 der Richtlinie (EU) 2016/680 hinausgehend ein Akteneinsichts-recht der betroffenen Personen. Ist betroffenen Personen Auskunft nach § 70 zu gewähren, erhalten sie auf Antrag Akteneinsicht, soweit eine Auskunft für das Wahrnehmen ihrer rechtlichen Interessen nicht ausreicht, das Einsehen der Akte hierfür erforderlich ist und Rechte Dritter und Geheimhaltungsinteressen berücksichtigt, die das Versagen der Akteneinsicht rechtfertigen könnten. Im Vollzug der Untersuchungshaft und der Freiheitsentziehungen nach § 1 Nummer 7 und 8 ist die Akteneinsicht bspw. ausgeschlossen, wenn die Staatsanwaltschaft mitgeteilt hat, dass eine Auskunft an die Gefangenen die Aufgabe des Vollzugs der Untersuchungshaft gefährden würde.

Absatz 2 stellt klar, dass personenbezogenen Daten, die in ihrem Verarbeiten eingeschränkt wurden, nicht der Akteneinsicht unterliegen. Die Vorschrift schränkt insoweit das Akteneinsichtsrecht der Gefangenen ein. Davon unberührt bleibt das allgemeine Auskunftsrecht nach § 70.

Absatz 3 Satz 1 und 2 bestimmen, welche Personen bei einer Akteneinsichtnahme hinzugezogen werden können und wer hiervon ausgeschlossen ist. Dadurch soll individuell unterschiedlichen intellektuellen Fähigkeiten oder auch Sprachschwierigkeiten betroffener Personen Rechnung getragen werden.

Andernfalls könnten das Einsichtsrecht und das Recht auf Wahrnehmen rechtlicher Interessen faktisch leerlaufen. Das Verbot von Satz 2 besteht auch dann, wenn ein Gefangener die Voraussetzungen von Satz 1 erfüllt.

Absatz 4 bestimmt das Recht des genannten Personenkreises, sich Notizen zu machen.

Absatz 5 Satz 1 regelt, unter welchen Voraussetzungen das Recht besteht, Ablichtungen einzelner Dokumente oder aus automatisierten Dateien Ausdrucke eines Teilbestands der personenbezogenen Daten zu verlangen. Soweit die betroffenen Personen - insbesondere zum Durchsetzen ihrer Rechte - auf Ausdrucke angewiesen sind, sind diese nach Satz 2 zu fertigen. Die Kostenregelungen sind in § 72 als allgemeine Verfahrensvorschrift enthalten.

Zu § 72 Verfahren zu den Rechten der betroffenen Person

In § 72 setzt verschiedene Elemente aus Artikel 12 der Richtlinie (EU) 2016/680 um.

Absatz 1 entspricht zunächst § 160 Absatz 7 JVollzGB LSA und benennt die Arten von Akten, die im Justizvollzug regelmäßig verwendet werden. Hierzu zählen auch elektronische Akten, soweit diese nach §§ 53 bis 56 zugelassen und von Justizvollzugsbehörden geführt werden.

Absatz 2 und 3 setzen die Vorgaben aus Artikel 12 Absatz 1 bis 3 der Richtlinie (EU) 2016/680 zu den Mitteilungen und den Modalitäten der Mitteilungen gegenüber der betroffenen Person um.

Absatz 4 Satz 2 und 3 machen von der Möglichkeit in Artikel 12 Absatz 4 der Richtlinie (EU) 2016/680 Gebrauch, bei einer offensichtlich unbegründeten oder exzessiven Antragstellung vom Bescheiden des Antragstellers oder einer näheren Begründung abzusehen. Als Beispielsfall wird das häufige sachgrundlose Wiederholen von Anträgen als möglicher Ablehnungsgrund für das Erteilen von Informationen genannt.

Absatz 5 Satz 2 bis 4 regeln die Verpflichtung zum Ermöglichen von Ablichtungen und Ausdrucken, die Vorschusspflicht und die Folgen bei deren Nichterfüllen. Dies steht in Einklang mit Artikel 12 Absatz 4 der Richtlinie (EU) 2016/680, wonach für das Erteilen von Informationen angemessene Gebühren erhoben werden können, bei denen die Verwaltungskosten berücksichtigt werden.

Absatz 6 dient dem Umsetzen von Art. 12 Absatz 5 der Richtlinie (EU) 2016/680.

Zu Abschnitt 6 - Datenschutzbeauftragter

Der Abschnitt 6 enthält die bereichsspezifischen Vorschriften für den Justizvollzug des Landes zum Benennen, zur Stellung und zu den Aufgaben des behördlichen Datenschutzbeauftragten der jeweiligen Justizvollzugsbehörde.

Zu § 73 Datenschutzbeauftragter

Absatz 1 Satz 1 regelt im Umsetzen von Artikel 32 Absatz 1 Satz 1 der Richtlinie (EU) 2016/680 das verpflichtende Benennen des behördlichen Datenschutzbeauftragten bei jeder Justizvollzugsbehörde. In Umsetzung des Artikels 32 Absatz 2 der Richtlinie (EU) 2016/680 regelt Satz 2 die fachlich notwendigen Voraussetzungen zum Ausüben des Amtes des behördlichen Datenschutzbeauftragten der jeweiligen Justizvollzugsbehörde. Satz 3 dient dem Umsetzen von Artikel 32 Absatz 4 der Richtlinie (EU) 2016/680.

Absatz 2 enthält die Verpflichtung der Justizvollzugsbehörden, ihrem behördlichen Datenschutzbeauftragten das Ausüben seines Amtes nicht nur zu ermöglichen, sondern ihn dabei auch durch das Bereitstellen der erforderlichen Mittel zum Erfüllen seiner Aufgaben zu unterstützen und seine fachliche Qualifikation zu fördern und dient damit dem Umsetzen von Artikel 33 Absatz 1 und 2 der Richtlinie (EU) 2016/680.

Absatz 3 enthält die Verpflichtung der Justizvollzugsbehörden, die Unabhängigkeit ihres behördlichen Datenschutzbeauftragten sicherzustellen. Dieser ist in dem Ausüben seines Amtes auch fachlich vollkommen unabhängig und nicht an Weisungen von den in den Justizvollzugsbehörden Tätigen oder deren Leiter gebunden. Hier besteht seitens des behördlichen Datenschutzbeauftragten lediglich die Verpflichtung, dem Leiter der Justizvollzugsbehörden zu berichten.

Absatz 4 enthält das Verbot des Abberufens und Benachteiligens des behördlichen Datenschutzbeauftragten sowie die Voraussetzungen unter denen das Abberufen

oder Kündigen möglich ist. Absatz 4 entspricht der Regelung des § 4f Absatz 3 Satz 4 bis 6 BDSG a. F. Bei dem besonderen Abberufungs- und Kündigungsschutz der behördlichen Datenschutzbeauftragten der Justizvollzugsbehörden handelt es sich um eine arbeitsrechtliche Regelung, die ergänzend zu den Vorgaben der Verordnung (EU) 2016/679 beibehalten werden kann.

Absatz 5 regelt die Befugnis der betroffenen Person, sich in allen Fragen des Verarbeitens ihrer personenbezogenen Daten durch die Justizvollzugsbehörde an deren behördlichen Datenschutzbeauftragten zu wenden und in zu Rate zu ziehen. Darüber hinaus enthält Absatz 5 die grds. Verpflichtung zur Verschwiegenheit des behördlichen Datenschutzbeauftragten zur Identität und zu den Umständen einer Anfrage der betroffenen Person. Die Verletzung von Privatgeheimnissen durch den behördlichen Datenschutzbeauftragten der jeweiligen Justizvollzugsbehörden ist gemäß § 203 Absatz 2a des Strafgesetzbuches zudem strafbewehrt.

Absatz 6 regelt die Voraussetzungen eines Zeugnisverweigerungsrechts des behördlichen Datenschutzbeauftragten. Das Zeugnisverweigerungsrecht in Absatz 6 sichert die Verschwiegenheitspflicht ab und entspricht § 4f Absatz 4a BDSG a. F. Die Regelungskompetenz für den Bereich der Verordnung (EU) 2016/679 folgt aus Artikel 38 Absatz 5 der Verordnung (EU) 2016/679. Die Regelung geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus und erfolgt zum Zweck einer kohärenten Rechtsstellung des behördlichen Datenschutzbeauftragten der jeweiligen Justizvollzugsbehörden.

Absatz 7 dient dem Umsetzen von Artikel 34 der Richtlinie (EU) 2016/680. Um die Aufgaben des behördlichen Datenschutzbeauftragten der jeweiligen Justizvollzugsbehörde für alle Verarbeitungszwecke einheitlich auszugestalten, entspricht die Norm unter lediglich redaktioneller Anpassung Artikel 39 der Verordnung (EU) 2016/679.

Absatz 8 stellt klar, dass der behördliche Datenschutzbeauftragte der jeweiligen Justizvollzugsbehörden weitere Aufgaben und Pflichten wahrnehmen kann, sofern diese nicht zu einem Interessenkonflikt führen. Die Regelung entspricht Artikel 38 Absatz 6 der Verordnung (EU) 2016/679, deren Regelungsgehalt auf den Anwendungsbereich der Richtlinie (EU) 2016/680 und der Datenverarbeitung außerhalb des Anwendungsbereichs des Rechts der Europäischen Union (z. B. zu nachrichtendienstlichen Zwecken) erstreckt wird.

Absatz 9 entspricht Artikel 39 Absatz 2 der Verordnung (EU) 2016/679. Die Regelung hat keine Entsprechung in Artikel 34 der Richtlinie (EU) 2016/680, wird aber auch außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 als Grundsatz festgeschrieben.

Zu Abschnitt 7 - Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und zwischen den Aufsichtsbehörden

Zu § 74 Grundsatz der Zusammenarbeit

Die Vorschrift dient dem Umsetzen von Artikel 26 der Richtlinie (EU) 2016/680. Die hier angesprochene Pflicht der Justizvollzugsbehörden zur Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz fasst die sich ohnehin aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperationsbeziehungen

zwischen den Justizvollzugsbehörden und dem Landesbeauftragten für den Datenschutz zusammen. Satz 2 übernimmt dabei die Festlegung aus § 23 Absatz 1 Satz 2 DSG LSA.

Zu § 75 Anhören des Landesbeauftragten für den Datenschutz

Die Vorschrift dient dem Umsetzen von Artikel 28 der Richtlinie (EU) 2016/680. Das Vorkonsultieren - hier als Anhören bezeichnet - des Landesbeauftragten für den Datenschutz dient dem datenschutzrechtlichen Absichern in Bezug auf das beabsichtigte Verarbeiten personenbezogener Daten in neu anzulegenden oder wesentlich geänderten Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutzfolgenabschätzung aus der Verordnung (EU) 2016/679. Prozedural wird diese Verbindung dadurch hergestellt, dass nach Absatz 1 Nummer 1 das Anhören durchzuführen ist, wenn im Ergebnis einer Datenschutzfolgenabschätzung eine erhöhte Gefährdung angenommen wird und die Justizvollzugsbehörden hierauf nicht mit Maßnahmen zur Gefährdungsminimierung reagiert.

Der Umfang der dem Landesbeauftragten für den Datenschutz vorzulegenden Unterlagen wird in Absatz 2 durch Zusammenführung der Vorgaben aus Artikel 28 Absatz 4 der Richtlinie (EU) 2016/680 und Artikel 36 Absatz 3 der Verordnung (EU) 2016/679 angeglichen.

Absatz 3 enthält die Befugnis des Landesbeauftragten für den Datenschutz, den Justizvollzugsbehörden unter den dort genannten Voraussetzungen und Bedingungen schriftliche Empfehlungen zum Abwehren möglicher Verstöße gegen gesetzliche Vorgaben zu unterbreiten.

Artikel 28 der Richtlinie (EU) 2016/680 knüpft an das Einleiten des Konsultierens an, setzt aber nicht voraus, dass dies bereits zwingend abgeschlossen sein muss, bevor personenbezogene Daten entsprechend verarbeitet werden.

Zwar wird man im Regelfall den Abschluss des Konsultierens im Interesse der betroffenen Personen abwarten. Im Ausnahmefall können jedoch Abweichungen geboten sein. Die in Absatz 4 vorgesehene Eilfallregelung trägt solchen vollzuglichen und operativen Erfordernissen in Abweichung von Absatz 3 Satz 1 Rechnung. Das Nutzen der Eilfallregelung entbindet die Justizvollzugsbehörden gleichwohl nicht davon, die Empfehlungen des Landesbeauftragten für den Datenschutz nach pflichtgemäßem Ermessen zu prüfen und das Verarbeiten personenbezogener Daten gegebenenfalls daraufhin anzupassen. Weiterhin bedeutet die Eilfallregelung kein Einschränken der dem Landesbeauftragten für den Datenschutz zur Verfügung stehenden Befugnisse.

Zu § 76 Meldungen an den Landesbeauftragten für den Datenschutz

Die Vorschrift setzt Artikel 30 der Richtlinie (EU) 2016/680 um und legt Umfang und Modalitäten des Meldens des „Verletzens des Schutzes personenbezogener Daten“ an den Landesbeauftragten für den Datenschutz fest. Ansatzpunkt des Meldens sind beispielsweise Vorfälle wie etwa das Abfließen personenbezogener Daten.

Das in Absatz 5 geforderte Dokumentieren muss in seiner Qualität und Quantität so beschaffen sein, dass es dem Landesbeauftragten für den Datenschutz das Überprüfen des Einhaltens der gesetzlichen Vorgaben ermöglicht.

Nach Absatz 7 soll die Motivation zum Melden nicht dadurch verringert werden, dass die durch das Melden verfügbar werdenden Informationen zum Verarbeiten personenbezogener Daten zum Einleiten eines Strafverfahrens führen können.

Absatz 8 stellt klar, dass die Meldepflicht an den Landesbeauftragten für den Datenschutz andere Meldepflichten, etwa solche an das Bundesamt für Sicherheit in der Informationstechnik als Meldestelle des Bundes für IT-Sicherheitsvorfälle (vgl. § 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik), nicht ausschließt bzw. diesen nicht vorgeht.

Zu § 77 Gegenseitige Amtshilfe

Die Vorschrift setzt Artikel 50 der Richtlinie (EU) 2016/680 um.

Zu Abschnitt 8 - Rechtsbehelfe

Zu § 78 Beschwerde

Die Vorschrift dient dem Umsetzen von Artikel 52 Absatz 2 der Richtlinie (EU) 2016/680 um und stellt für den Bereich des Verarbeitens personenbezogener Daten durch die Justizvollzugsbehörden, Auftragsverarbeiter oder eine beauftragte Stelle, der vollzugliche Aufgaben zum Erledigen übertragen wurden, zu den in § 1 genannten Zwecken klar, dass sich die betroffene Person mit Beschwerden über das bei den genannten Verantwortlichen durchgeführte Verarbeiten personenbezogener Daten an den Landesbeauftragten für den Datenschutz wenden können.

Zu § 79 Gerichtlicher Rechtsschutz gegen Entscheidungen des Landesbeauftragten für den Datenschutz

Die Vorschrift dient dem Umsetzen von Artikel 53 der Richtlinie (EU) 2016/680.

Zu Abschnitt 9 - Haftung und Sanktionen

Abschnitt 9 dient dem Umsetzen der Artikel 56 und 57 der Richtlinie (EU) 2016/680.

Zu § 80 Recht auf Schadenersatz

Die Vorschrift dient dem Umsetzen von Artikel 56 der Richtlinie (EU) 2016/680.

Zu § 81 Strafvorschriften

Die Vorschrift dient dem Umsetzen von Artikel 57 der Richtlinie (EU) 2016/680.

Zu Abschnitt 10 - Schlussvorschriften

Zu § 82 Übergangsvorschriften zum Anpassen automatisierter Verarbeitungssysteme

Auf der Basis von Artikels 63 Absatz 2 der Richtlinie (EU) 2016/680 mit Erwägungsgrund Nummer 96 berücksichtigt Absatz 2 die sich aus der Datenschutzreform ergebenden weitreichenden Änderungen für die IT-Verfahren im Justizvollzug.

Die Neuregelung zur Protokollierung wird im praktischen Umsetzen zu erheblichem Umstellungs- und Anpassungsaufwand führen. Zum Abfedern dieser erheblichen Auswirkungen und zum Etablieren des gesicherten Auslegens der neuen Vorschriften nimmt § 82 die Umsetzungsfrist nach Artikel 63 Absatz 2 der Richtlinie (EU) 2016/680 bis zum 6. Mai 2023 in Anspruch und schafft auf diese Weise eine angemessene Übergangsregelung.

Zu § 83 Anwenden weiterer Vorschriften

In § 83 wird klargestellt, dass für das Verarbeiten personenbezogener Daten durch die Justizvollzugsbehörden zu anderen Zwecken als denen nach diesem Gesetz die Verordnung (EU) 2016/679 und die hierzu erlassenen Vorschriften des Landes gelten.

Zu § 84 Einschränken von Grundrechten

Mit dem JVollzGB IV LSA wird in das durch die Landesverfassung in Artikel 6 Absatz 1 Satz 1 geschützte Recht auf den Schutz personenbezogener Daten eingegriffen. Diese datenschutzrechtlich relevanten Grundrechtseinschränkungen sind durch das Beachten des Zitiergebots für den Gesetzgeber kenntlich zu machen.

Zu § 85 Sprachliche Gleichstellung

Da in diesem Gesetz bei dem Bezeichnen von Personen generell die männliche Form benutzt wird, wird zum Wahren einer geschlechtergerechten Sprache eine sprachliche Gleichstellungsklausel eingefügt.

Zu Artikel 2 - Änderung des Justizvollzugsgesetzbuches Sachsen-Anhalt

Zu Nummer 1

Mit dem Einführen von Artikel 1 des Gesetzentwurfes - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt - bedürfen die Justizvollzugsgesetze des Landes einer entsprechenden Anpassung, um formell in die neue Systematik von vier Büchern des Justizvollzugsgesetzbuches Sachsen-Anhalt überführt zu werden. Alle Bücher - Erstes, Zweites, Drittes und Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt (JVollzGB I, II, III und IV LSA) stellen weiterhin materiell eigenständige Regelungswerke dar. Es handelt sich um eine Folgeänderung zu Artikel 1.

Zu Nummer 2

Mit dem Einführen von Artikel 1 des Gesetzentwurfes - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt wird der Datenschutz im Justizvollzug von Sachsen-Anhalt zentral und vollständig neu in einem eigenen Gesetz geregelt. Regelungen in den bestehenden Justizvollzugsgesetzen des Landes zum Datenschutz im Justizvollzug sind aus diesem Grund aufzuheben.

Zu Nummer 3

Es handelt sich um eine Folgeänderung aufgrund des Änderns der Strafprozessordnung.

Zu Nummer 4

Buchstabe a

Es handelt sich um eine Folgeänderung aufgrund des Anfügens von Buchstabe c.

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Anfügens von Buchstabe c.

Buchstabe c

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 25 Absatz 5 von Artikel 1.

Zu Nummer 5

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 22 Absatz 3 von Artikel 1.

Zu Nummer 6

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 31 von Artikel 1.

Zu Nummer 7

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 31 von Artikel 1.

Zu Nummer 8

Buchstabe a

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 50 Absatz 2 von Artikel 1.

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund von Buchstabe a.

Zu Nummer 9

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1.

Nummer 10

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1.

Nummer 11

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1.

Zu Artikel 3 - Änderung des Sicherungsverwahrungsvollzugsgesetzes Sachsen-Anhalt

Zu Nummer 1

Mit der Einführung von Artikel 1 des Gesetzentwurfes - Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt – bedürfen die Justizvollzugsgesetze des Landes einer entsprechenden Anpassung, um formell in die neue Systematik von vier Büchern des Justizvollzugsgesetzbuches Sachsen-Anhalt überführt zu werden. Alle Bücher - Erstes, Zweites, Drittes und Viertes Buch Justizvollzugsgesetzbuch Sachsen-Anhalt (JVollzGB I, II, III und IV LSA) stellen weiterhin materiell eigenständige Regelungswerke dar. Es handelt sich um eine Folgeänderung zu Artikel 1.

Zu Nummer 2

Buchstabe a

Es handelt sich um eine Folgeänderung. Mit Artikel 2 des Gesetzes zur Weiterentwicklung des Justizvollzugs in Sachsen-Anhalt vom 18. Dezember 2015 (GVBl. LSA S. 666) wurden bereits Teil 2 und 3 Sicherungsverwahrungsvollzugs-gesetzes Sachsen-Anhalt aufgehoben und sind weggefallen. Diese materiellen Regelungen waren der Grund der Gliederung dieses Gesetzes in vier Teile. Nach Wegfall von Teil 2 und 3 bedarf es auch der Teile 1 und 4 nicht mehr. Die Gliederung des Gesetzes ergibt sich allein aus den neuen Abschnitten 1 bis 20.

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Einführens des §§ 22 Absatz 1 und 2, 27 und 28 sowie 30 Absatz 1 und 3 und 31 von Artikel 1.

Buchstabe c

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1.

Buchstabe d

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1.

Buchstabe e

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1 und Buchstabe a).

Buchstabe f

Es handelt sich um eine Folgeänderung.

Zu Nummer 3

Es handelt sich um eine Folgeänderung (vgl. zu Nummer 2 Buchstabe a).

Zu Nummer 4

Buchstabe a

Es handelt sich um eine Folgeänderung aufgrund des Anfügens von Buchstabe c.

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Anfügens von Buchstabe c.

Buchstabe c

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 25 Absatz 5 von Artikel 1.

Zu Nummer 5

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 25 von Artikel 1.

Zu Nummer 6

Buchstabe a

Es handelt sich um eine Folgeänderung aufgrund des Anfügens von Buchstabe b.

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 31 von Artikel 1.

Zu Nummer 7

Buchstabe a

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 31 von Artikel 1.

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Anfügens von Buchstabe a.

Zu Nummer 8

Es handelt sich um eine Folgeänderung (vgl. zu Nummer 2 Buchstabe b.)

Zu Nummer 9

Buchstabe a

Es handelt sich um eine Folgeänderung (vgl. Buchstabe b.)

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 38 von Artikel 1.

Zu Nummer 10

Buchstabe a

Es handelt sich um eine Folgeänderung (vgl. Buchstabe b.)

Buchstabe b

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 50 Absatz 2 von Artikel 1.

Zu Nummer 11

Es handelt sich um eine Folgeänderung aufgrund des Einführens des § 43 von Artikel 1.

Zu Nummer 12

Es handelt sich um eine Folgeänderung aufgrund des Einführens von Artikel 1.

Zu Nummer 13

Es handelt sich um eine Folgeänderung (vgl. zu Nummer 2 Buchstabe a).

Zu Nummer 14

Es handelt sich um eine Folgeänderung.

Zu Nummer 15

Buchstabe a

Es handelt sich um eine Folgeänderung. Die Verordnung über die Vergütungsstufen des Arbeitsentgelts nach dem Sicherungsverwahrungsvollzugsgesetz Sachsen-Anhalt (Sicherungsverwahrungsvergütungsverordnung - SVVergVO) vom 2. August 2013 (GVBl. LSA S. 411) ist am 9. August 2013 in Kraft getreten.

Buchstabe b

Es handelt sich um eine Folgeänderung (vgl. Buchstabe a und c).

Buchstabe c

Es handelt sich um eine Folgeänderung (vgl. zu Nummer 2 Buchstabe a).

Zu Artikel 4 - Inkrafttreten

Zu Absatz 1

In Absatz 1 wird das Inkrafttreten dieses Gesetzes geregelt.

Zu Absatz 2

In Absatz 2 wird die in § 82 von Artikel 1 enthaltene Übergangsregelung abgesichert.