Landtag von Sachsen-Anhalt

Drucksache 7/3207
31.07.2018

Gesetzentwurf

Landesregierung

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes

Sehr verehrte Frau Landtagspräsidentin,

als Anlage übersende ich gemäß Artikel 77 Abs. 2 der Verfassung des Landes Sachsen-Anhalt den von der Landesregierung am 24. Juli 2018 beschlossenen

> Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes

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

Federführend ist das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt.

Mit freundlichen Grüßen

Dr. Reiner Haseloff
Ministerpräsident

(Ausgegeben am 02.08.2018)

Vorblatt

A. Zielsetzung

Der vorliegende Gesetzentwurf soll nach dem Inkrafttreten der Richtlinie (EU) 2016/680 vom 27. April 2016 die dort enthaltenen Vorgaben zur Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten umsetzen.

B. Lösung

Zu diesem Zweck werden die Regelungsinhalte aus Teil 3 (§§ 45 ff.) des neuen Bundesdatenschutzgesetzes (BDSG), das am 25. Mai 2018 in Kraft getreten ist, in das Landesrecht übernommen. Diese größtenteils wörtliche Übernahme der Regelungen bietet den Vorteil, dass damit eine einheitliche Behandlung von Datenschutzfragen auf der Ebene der Strafverfolgungsbehörden (insbesondere der Staatsanwaltschaften und der ihr zuarbeitenden Polizeibehörden), welche die Strafprozessordnung (StPO) anzuwenden haben, und der Ebene der Polizeibehörden, die auch im Bereich der nur landesrechtlich geregelten Gefahrenabwehr zur Verhütung von Straftaten tätig werden, gewährleistet werden kann. Diese Verschränkung der beiden Strafverfolgungsbehörden wird insbesondere in § 483 der StPO deutlich. In § 483 Abs. 3 StPO ist geregelt, dass die Datenverarbeitung der Polizei als Strafverfolgungsbehörde sich nach dem Landesdatenschutzrecht richtet, wenn die Datenspeicherung in einer sogenannten Mischdatei erfolgt. In § 484 Abs. 4 StPO ist geregelt, dass die Datenverarbeitung der Polizei zum Zweck der Strafverfolgungsvorsorge sich nach dem Landesrecht richtet. Insofern bedarf eine Umsetzung der Richtlinie (EU) 2016/680 zwingend auch einer Anpassung des Datenschutzrechts im Bereich der Landespolizei. Mit dem vorliegenden Gesetzentwurf soll auf der Ebene der Bundespolizeibehörden und der Landespolizeibehörden ein einheitliches Querschnittsdatenschutzrecht umgesetzt werden.

Daneben sollen die bereichsspezifischen Regelungen zum Datenschutz im Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) sowie die Datenschutzregelungen im Maßregelvollzugsgesetz an die Vorgaben der Richtlinie (EU) 2016/680 angepasst werden. Außerdem sollen redaktionelle Anpassungen im Ausführungsgesetz zum Therapieunterbringungsgesetz in Sachsen-Anhalt erfolgen. Ergänzend werden unabdingbare datenschutzrechtliche Anpassungen im SOG LSA mit Blick auf die Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz (BKAG) vorgenommen.

Schließlich wird in Artikel 2 des Gesetzentwurfs eine Übergangsregelung für den Datenschutz im Verfassungsschutz geschaffen.

C. Alternativen

Mit redaktionellen Anpassungen und der Beschränkung des Geltungsbereichs auf den Datenschutz im Bereich Polizei und Justiz könnte das Datenschutzgesetz des Landes Sachsen-Anhalt fortentwickelt werden. Dieser Rechtszustand wäre jedoch unbefriedigend, weil damit datenschutzrechtliche Fragestellungen auf der Ebene der Bundesbehörden nach den § 45 ff. BDSG zu beantworten wären, während die Lan-

despolizeibehörden weiter auf der Grundlage des novellierten Datenschutzgesetzes Sachsen-Anhalt (DSG LSA) arbeiten müssten. Vor diesem Hintergrund scheidet eine Fortschreibung des bisherigen Datenschutzrechts schon aus Gründen der Wahrung der Rechtseinheitlichkeit aus.

Ein zweiter Ansatz könnte die umfassende Anwendung der Datenschutz-Grundverordnung auch für Zwecke des Datenschutzes im Bereich von Polizei und Justiz sein. Diesen Ansatz verfolgt beispielsweise das Land Brandenburg. Auch über diesen Ansatz würde kein homogenes Datenschutzrecht entstehen können, weil insbesondere im Bereich der sogenannten Betroffenenrechte aus Gründen der polizeilichen Arbeit erhebliche Einschränkungen zu normieren wären. Im Übrigen würde auch dieser Ansatz zu einer Rechtszersplitterung auf den Ebenen der Bundes- und der Landespolizeibehörden führen.

D. Kosten

Der Gesetzentwurf löst außerhalb der Polizei keine unmittelbaren Kosten für den Landeshaushalt aus. Die Aufsichtsaufgabe liegt beim Landesbeauftragten für den Datenschutz als unabhängige Kontrollbehörde. Der Landesbeauftragte für den Datenschutz hat durch die Beschlüsse zum Haushaltsplan 2017/2018 einen eigenen Einzelplan erhalten, der im geringen Umfang Personalverstärkungen ausweist.

Für den Bereich der Polizei erfordert die Umsetzung der Vorgaben der EU-Datenschutzrechtsreform demgegenüber zwingend eine Erneuerung der Fachanwendung für die Einsatz- und Ermittlungsbearbeitung. Das vorhandene System kann nicht wirtschaftlich angepasst werden. Das aktuelle Verfahren Integriertes Vorgangsbearbeitungssystem der Polizei des Landes Sachsen-Anhalt (IVOPol LSA) wird bereits seit 1997 in der Polizei betrieben. Das Verfahren basiert auf Entwicklungsumgebungen (z. B. XVT-Plattform), die in den 1990er Jahren gängige Standards darstellten, mittlerweile aber überholt sind. Die Umsetzung der Vorgaben der EU-Datenschutz-Rechtsreform würden so umfassende Anpassungen erforderlich machen, dass sie mit einer Neuentwicklung des Verfahrens gleichzusetzen sind.

Der Gesamtaufwand für die Beschaffung eines neuen Verfahrens sowie die Herstellung der Betriebsbereitschaft wird mit ca. acht Millionen Euro über einem Zeitraum von fünf Jahren geschätzt. Dies beinhaltet den Anteil für die Beteiligung an einer Entwicklungskooperation (650.000 Euro pro Jahr), den Betrieb eines Test-/Entwicklungssystems bei Dataport (2,5 Millionen Euro für fünf Jahre), die Schnittstellen-Anpassungsprogrammierung und die Einführung des Verfahrens (1,9 Millionen Euro für fünf Jahre) sowie einmalige Kosten in Höhe von 150.000 Euro für die Herstellung der Betriebsbereitschaft bei Dataport.

In der Anmeldung für den Haushalt 2019 wurden zusätzlich die Kosten für den Betrieb des Verfahrens (bei Dataport) eingeplant. Für die Jahre 2022/2023 wurden jeweils zwei Millionen Euro für den erforderlichen Parallelbetrieb mit IVOPol LSA kalkuliert.

Einsparpotenzial durch die Einstellung des Verfahrens IVOPol LSA im Einzelplan 19 entsteht nicht.

E. Anhörung

Gelegenheit zur Stellungnahme hatten der Landesbeauftragte für den Datenschutz, der Präsident des Oberlandesgerichts Sachsen-Anhalt, die Generalstaatsanwaltschaft Sachsen-Anhalt, der Städte- und Gemeindebund Sachsen-Anhalt, der Landkreistag Sachsen-Anhalt, die Rechtsanwaltskammer Sachsen-Anhalt, der Deutsche Gewerkschaftsbund Bezirk Niedersachsen-Bremen-Sachsen-Anhalt, die Gewerkschaft der Polizei Landesbezirk Sachsen-Anhalt, der Deutsche Beamtenbund und Tarifunion Sachsen-Anhalt, die Deutsche Polizeigewerkschaft Landesverband Sachsen-Anhalt und der Bund Deutscher Kriminalbeamter Landesverband Sachsen-Anhalt.

Zum Gesetzentwurf sind vier Stellungnahmen eingegangen. Der Landesbeauftragte für den Datenschutz nahm vor allem zu den vorgesehenen Änderungen im SOG LSA besonders ausführlich und detailliert Stellung. Der Präsident des Oberlandesgerichts, die Generalstaatsanwaltschaft, der Städte- und Gemeindebund, die Rechtsanwaltskammer und die Gewerkschaft der Polizei haben von einer Stellungnahme abgesehen bzw. keine Bedenken vorgetragen. Der Deutsche Beamtenbund und der Deutsche Gewerkschaftsbund haben sich über die Fachgewerkschaften hinaus nicht geäußert.

Grundsätzliche Bedenken gegen den Gesetzentwurf der Landesregierung wurden nicht erhoben. Die Anregungen zu Einzelfragen des Gesetzentwurfs wurden sorgfältig geprüft und zum Teil in den Normtext oder die Begründung eingearbeitet. Daneben wurden vereinzelt weitere redaktionelle Änderungen vorgenommen. Das Vorblatt wurde entsprechend angepasst. Die wichtigsten Anregungen und deren Bewertung werden im Folgenden dargestellt.

Allgemein

Der Landesbeauftragte für den Datenschutz regt an, die bisherigen Regelungen zur Vorabkontrolle aus § 14 DSG LSA bei der Umsetzung der Richtlinie (EU) 2016/680 insoweit zu übernehmen, dass eine Vorabkontrolle entsprechend § 14 Abs. 2 DSG LSA auch in Zukunft eine Rechtsgrundlage findet. Dazu ist anzumerken, dass die Regelungen zur Vorabkontrolle nach § 14 DSG LSA nach wie vor gelten, da das DSG LSA durch den Gesetzentwurf nicht aufgehoben wird. Des Weiteren hat der Landesbeauftragte für den Datenschutz nach § 25 Abs. 1 Satz 2 des Gesetzentwurfs die Möglichkeit, eine Liste der Verarbeitungsvorgänge zu erstellen, die der Pflicht zu seiner Anhörung nach Satz 1 unterliegen. Um hier größtmögliche Rechtssicherheit zu gewährleisten, wurde der Gesetzeswortlaut von „neu angelegten“ auf „wesentlich geänderte“ Dateisysteme erweitert. So werden im Bereich der Umsetzung der Richtlinie (EU) 2016/680 auch in Zukunft umfassende, gestaltbare Anhörungsrechte gewährleistet. Weiter gehende allgemeine Regelungen zur Vorabkontrolle wären demgegenüber auch in Zukunft in demjenigen Gesetz zu regeln, das das DSG LSA ablösen wird.

Der Bund Deutscher Kriminalbeamter begrüßt unter Hinweis auf die größtenteils wörtliche Übernahme der Regelungen der §§ 45 ff. BDSG, dass mit dem Gesetzgebungsverfahren eine einheitliche Behandlung von Datenschutzfragen auf der Ebene

der Strafverfolgungsbehörden (Staatsanwaltschaften und Polizei) gewährleistet werden kann.

Zu Artikel 1

Der Landkreistag Sachsen-Anhalt bittet vor dem Hintergrund des in § 1 Abs. 1 Nr. 1 Buchst. b) vorgesehenen Auffangtatbestandes für die Verfolgung und Ahndung von Ordnungswidrigkeiten, den durch die Regelungen insgesamt entstehenden Mehraufwand zu ermitteln und gemäß Artikel 87 Abs. 3 der Verfassung des Landes Sachsen-Anhalt eine Kostenausgleichsregelung in das Gesetz aufzunehmen. Eine Kostenausgleichsregelung ist jedoch bereits deswegen nicht erforderlich, weil den Kommunen durch das Gesetz keine neuen Aufgaben übertragen werden, da die Regelungen zum Verfahren bei der Bearbeitung von Ordnungswidrigkeiten im Ordnungswidrigkeitengesetz (OWiG) und der StPO wie bisher auf Regelungen des BDSG verweisen. Auch an der Abgrenzung der Anwendungsbereiche des Bundes- und des Landesdatenschutzrechts ändert sich nichts, da diese aus der Gesetzgebungsbefugnis resultieren. Der Gesetzentwurf sieht für die Fälle, in denen bisher Regelungen des DSG LSA zur Anwendung gekommen sind, in § 1 Abs. 1 Nr. 1 Buchst. b) einen Auffangtatbestand vor, damit in diesen Fällen die Regelungen des Gesetzentwurfs an die Stelle entsprechender Regelungen des bisherigen DSG LSA treten können. Unabhängig davon entstehen den Kommunen bereits deswegen keine zusätzlichen Kosten und damit kein Mehraufwand, weil ihnen neben den Bußgeldern für das Verwaltungsverfahren Gebühren und Auslagen zustehen (§ 107 OWiG).

Dem Landesbeauftragten für den Datenschutz erscheint die Regelung zur Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken in § 6 des Gesetzentwurfs zu weitgehend. Sie lasse eine Abwägung mit den Interessen der Betroffenen vermissen. Die Bedenken werden nicht geteilt. Die Regelung ist wortidentisch mit § 50 BDSG. Die Begründung zum BDSG wurde ebenfalls wortidentisch übernommen.

Der Landesbeauftragte für den Datenschutz hält die Regelungen zur Einwilligung in § 7 des Gesetzentwurfs nur für eingeschränkt anwendbar und regt eine Ergänzung der Begründung an. Die Regelung ist wortidentisch mit § 51 BDSG. Der Anregung wurde ungeachtet dessen gefolgt und die Begründung ergänzt.

Der Landesbeauftragte für den Datenschutz begrüßt die Regelung zum Datengeheimnis in § 9 des Gesetzentwurfs ausdrücklich und regt an, diese um eine klarstellende Regelung mit Blick auf das Beamtenstatusgesetz zu ergänzen. Dieser Anregung wird nicht gefolgt. Die Regelung ist wortidentisch mit § 53 BDSG.

Der Landesbeauftragte für den Datenschutz sieht die Regelung zum Auskunftsrecht in § 13 Abs. 2 des Gesetzentwurfs nicht mit der Richtlinie (EU) 2016/680 in Einklang. Diese Bedenken werden nicht geteilt. Die Regelung ist wortidentisch mit § 57 Abs. 2 BDSG.

Der Landesbeauftragte für den Datenschutz regt an, die Anrufungsrechte in § 16 des Gesetzentwurfs um eine Whistleblower-Regelung entsprechend § 19 Nr. 2 in Verbindung mit § 2 DSG LSA zu ergänzen. Dies ist derzeit nicht erforderlich, da das DSG LSA bis auf Weiteres anwendbar bleibt. Im Übrigen wäre eine Whistleblower-Regelung in dem Gesetz zu treffen, dass das DSG LSA ablösen wird.

Der Landesbeauftragte für den Datenschutz regt an, in den Regelungen zur Datenschutz-Folgenabschätzung in § 23 Abs. 1 des Gesetzentwurfs entsprechend Artikel 27 Abs. 1 der Richtlinie (EU) 2016/680 auf ein „hohes Risiko“ statt auf eine „erhebliche Gefahr“ abzustellen. Der Anregung wurde gefolgt.

Der Landesbeauftragte für den Datenschutz weist zur Regelung zur Zusammenarbeit in § 24 des Gesetzentwurfs darauf hin, dass Auftragsverarbeiter davon nicht erfasst seien. Dies widerspreche der Richtlinie (EU) 2016/680. Der Hinweis des Landesbeauftragten führte zu einer Änderung des Gesetzentwurfs. Die Regelung umfasst nun auch den Auftragsverarbeiter.

Der Landesbeauftragte für den Datenschutz regt an, in der Anhörungsregelung in § 25 Abs. 1 Nr. 1 und 2 des Gesetzentwurfs den Begriff der „erheblichen Gefahr“ durch den Begriff „hohes Risiko“ zu ersetzen. Der Anregung wurde gefolgt.

Der Landesbeauftragte für den Datenschutz merkt zu Artikel 1 insgesamt an, dass sich Anhörungsrechte zukünftig nicht auf den Erlass von Rechts- und Verwaltungsvorschriften erstreckten. Diese Rechtsauffassung wird nicht geteilt. Wie bei der Vorabkontrolle nach § 14 Abs. 2 DSG LSA gilt auch die Anhörungspflicht aus § 14 Abs. 1 Satz 3 DSG LSA fort, da das DSG LSA durch den Gesetzentwurf nicht aufgehoben wird. Wie bei der Vorabkontrolle wären auf Grund des allgemeinen Charakters allgemeine Anhörungspflichten auch in Zukunft in demjenigen Gesetz zu regeln, dass das DSG LSA ablösen wird.

Zu Artikel 2

Der Landesbeauftragte für den Datenschutz regt zu der in Artikel 2 vorgesehenen Änderung des Gesetzes über den Verfassungsschutz unter Hinweis auf die Organisationsänderungen seiner Behörde klarstellende Ergänzungen an. Der Anregung wurde gefolgt.

Zu Artikel 3

Der Landesbeauftragte für den Datenschutz äußert Bedenken zur Systematik und zum Geltungsbereich datenschutzrechtlicher Regelungen im neu geregelten § 4 SOG LSA. Diesen Bedenken wird gefolgt. Auf die beabsichtigte Änderung des § 4 SOG LSA wird verzichtet. Die bisher in der geplanten Änderung des § 4 SOG LSA enthaltenen Inhalte werden jetzt im § 13a SOG LSA zusammengeführt. Damit wird das Verhältnis des SOG LSA zum unmittelbar geltenden Recht der Europäischen Union sowie dem Datenschutzquerschnittsrecht des Landes Sachsen-Anhalt für den Rechtsanwender an zentraler Stelle im SOG LSA klargestellt.

Der Landesbeauftragte für den Datenschutz erhebt Bedenken gegen die in § 3 SOG LSA geplante Einführung des Begriffs „Weiterverarbeiten“. Auf Grund dieser Bedenken wurde Artikel 3 des Gesetzentwurfs überarbeitet. Nunmehr wurde auf ausschließlich im SOG LSA anzuwendende datenschutzrechtliche Begriffe verzichtet. Soweit die jeweils zuständigen Behörden personenbezogene Daten im Anwendungsbereich der Verordnung (EU) 2016/679 verarbeiten, legt das SOG LSA jetzt allein die datenschutzrechtlichen Begriffe des unmittelbar geltenden Rechts der Europäischen Union zugrunde. Soweit der Anwendungsbereich der Richtlinie (EU)

2016/680 betroffen ist, liegen die datenschutzrechtlichen Begriffe des DSUG LSA (Artikel 1 des Gesetzentwurfs) zugrunde. Im SOG LSA wird der Begriff „Weiterverarbeiten“ nur dann verwendet, wenn der Regelungsinhalt des jeweiligen Paragraphen oder Teils eines Paragraphen eine Zweckänderung beinhaltet bzw. zulässt. Soweit Befugnisnormen, die bisher z. B. beschränkt waren auf „speichern, verändern oder nutzen“ (§ 22 Abs. 1 SOG LSA) nunmehr durch den neuen Verarbeitungsbegriff, der z. B. auch die Erhebung bzw. Übermittlung enthält, ersetzt wurden, ist damit jedoch keine Erweiterung der Befugnisse verbunden. Denn das SOG LSA enthält weiterhin speziellere und damit vorgehende Regelungen zur Datenerhebung (§ 15) und Datenübermittlung (§§ 26 ff.).

Der Landesbeauftragte für den Datenschutz hält die geplante Regelung in § 23 Abs. 5 SOG LSA, die § 18 Abs. 5 BKAG entspricht und die Verarbeitung personenbezogener Daten von Beschuldigten einschränkt, insbesondere unter Hinweis auf die Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Neustrukturierung des BKAG vom 10. März 2017, für überarbeitungsbedürftig. Dieser Auffassung wird nicht gefolgt. Die vom Landesbeauftragten für den Datenschutz für erforderlich gehaltene Überarbeitung würde zu einer nicht unerheblichen Abweichung des Landespolizeirechts vom BKAG führen und damit dem Ziel der Harmonisierung datenschutzrechtlicher Regelungen für die Polizei widersprechen. Die Landespolizei müsste aufgrund der bundesrechtlichen Verpflichtung zum kriminalpolizeilichen Informationsaustausch des BKAG personenbezogene Daten im Informationsverbund der Polizeien des Bundes und der Länder speichern, wäre aber bei den betroffenen Fallkonstellationen nicht befugt, eine Datenspeicherung im Polizeilichen Informationssystem des Landes zu tätigen. Daher hat der Gesetzentwurf keine dahingehende Änderung erfahren.

Der Landesbeauftragte für den Datenschutz begrüßt die in § 23d SOG LSA vorgesehene Neuregelung zur Speicherung von DNA-Identifizierungsmustern zur Erkennung von Trugspuren mit dem Hinweis darauf, dass eine ausdrückliche gesetzliche Regelung zur Verarbeitung von DNA-Identifizierungsmustern zur Erkennung von Trugspuren geschaffen werden soll. Aufgrund seiner Anmerkungen ist im Gesetzentwurf klargestellt worden, dass DNA-Identifizierungsmuster der Mitarbeiter der Polizei nur auf der Grundlage einer Einwilligung der betroffenen Person verarbeitet werden dürfen. Da sich die Anforderungen an die Einwilligung aus § 7 DSUG LSA (vgl. Artikel 1 des Gesetzentwurfs) ergeben, ist die Rechtswirksamkeit der Einwilligung ausdrücklich von der freiwilligen Entscheidung der betroffenen Person abhängig. Die dahingehenden Bedenken des Landesbeauftragten für den Datenschutz sind somit unbegründet.

Der Landesbeauftragte für den Datenschutz erhebt Bedenken gegen die geplante Neuregelung zu Datenübermittlungen zum Zweck von Zuverlässigkeitsüberprüfungen in § 29 SOG LSA. Hierzu führt er an, dass im Rahmen der Zuverlässigkeitsüberprüfung insbesondere auch unspezifische Information zu eingestellten Ermittlungsverfahren oder zum Stand von laufenden Ermittlungsverfahren, die keinen hinreichenden Ansatz für Zweifel an der Zuverlässigkeit begründen können, übermittelt werden könnten. Im Übrigen sei die Regelung mit Bundesrecht unvereinbar. Demgegenüber begrüßt die Deutsche Polizeigewerkschaft, dass der Gesetzentwurf eine Befugnis zur Durchführung von Datenübermittlungen zum Zweck der Durchführung einer Sicherheitsüberprüfung für Einstellungen in den Polizeivollzugsdienst vorsieht. Die Deutsche Polizeigewerkschaft schlägt unter Hinweis darauf, dass dies einen

nicht unerheblichen Beitrag zur vorbeugenden Bekämpfung der Organisierten Kriminalität leisten könne, vor, dass Zuverlässigkeitsüberprüfung auch bei Einstellungen bei anderen Behörden, die Sicherheitsaufgaben wahrnehmen, zulässig sein sollten (z. B. Meldeämter, Fahrerlaubnisbehörden). Den Bedenken des Landesbeauftragten für den Datenschutz wird durch eine Ergänzung des § 29 Abs. 1 SOG LSA Rechnung getragen. In den Datenabgleich dürfen nach dieser Ergänzung nur solche personenbezogenen Daten einbezogen werden, die von der Polizei auf der Grundlage des § 23 Abs. 1 SOG LSA im polizeilichen Informationssystem weiterverarbeitet werden. Bei den nach § 23 Abs. 1 SOG LSA betroffenen Personenkategorien liegen regelmäßig spezifische personenbezogene Daten aus strafrechtlichen Ermittlungsverfahren vor, die Zweifel an der Zuverlässigkeit begründen können. Entgegen der Auffassung des Landesbeauftragten für den Datenschutz ist die geplante Regelung auch mit dem Bundesrecht vereinbar. Hierzu wird auch auf die Begründung zu dieser Befugnis verwiesen. Danach darf aufgrund von § 26 Abs. 4 SOG LSA die Übermittlung personenbezogener Daten nicht zu einer Erweiterung des Kreises der Stellen nach § 41 des Bundeszentralregistergesetzes führen, die von Eintragungen, die in ein Führungszeugnis nicht aufgenommen werden, Kenntnis erhalten, und muss das Verwertungsverbot im Bundeszentralregister getilgter oder zu tilgender Eintragungen nach §§ 51 und 52 des Bundeszentralregistergesetzes berücksichtigen. Ungeachtet dessen kommt die von der Deutschen Polizeigewerkschaft vorgeschlagene Erweiterung des Anwendungsbereichs derzeit nicht in Betracht.

Der Landesbeauftragte für den Datenschutz hält eine zeitliche Befristung der Übergangsvorschrift für die Verarbeitung personenbezogener Daten durch die Polizei in § 109a SOG LSA für erforderlich. Eine solche Befristung ist jedoch nicht möglich, da die Dauer der Erforderlichkeit der Übergangsregelung nicht sicher prognostiziert werden kann. So sind die für die Umsetzung des Gesetzes erforderlichen Haushaltsmittel (über einen Zeitraum von fünf Jahren) zwar geplant, wurden aber noch nicht durch ein Haushaltsgesetz verbindlich zur Verfügung gestellt. Der Gesetzentwurf hat daher keine dahingehende Änderung erfahren.

Die Deutsche Polizeigewerkschaft hat neben den Anmerkungen zur in § 29 SOG LSA vorgesehenen Neuregelung bezweifelt, dass die veranschlagten Kosten für die Erneuerung der Fachanwendung für die Einsatz- und Ermittlungsbearbeitung der Polizei auskömmlich seien, da die bestehende Fachanwendung über Schnittstellen mit anderen polizeilichen Systemen verbunden sei. Die Landesregierung hält diese Befürchtung für unbegründet. Die Kostenermittlung berücksichtigt alle durch das Gesetzgebungsverfahren relevanten Umstände (einschließlich Anpassung der Schnittstellen).

Zu Artikel 4

Der Landesbeauftragte für den Datenschutz hält die vorgesehene Änderung in § 36 des Maßregelvollzugsgesetzes für zu weitgehend und regt vor dem Hintergrund der laufenden Gesetzgebungsvorhaben zum Datenschutz eine Anpassung der Begründung zu § 38 an. Den Hinweisen wurde mit Blick auf die Begründung, nicht jedoch auf die gesetzliche Regelung gefolgt.

Zu Artikel 6

Der Landesbeauftragte für den Datenschutz sieht Artikel 2 des Gesetzentwurfs vom Zitiergebot nicht betroffen und regt eine Streichung des Verweises auf Artikel 2 an. Dieser Anregung wurde gefolgt.

F. Zuständigkeit

Federführend ist das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt.

Entwurf

Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 und zur Anpassung von bereichsspezifischen Datenschutzvorschriften an die Richtlinie (EU) 2016/680 sowie zur Regelung der Datenschutzaufsicht im Bereich des Verfassungsschutzes.

Artikel 1
Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt - DSUG LSA)

Inhaltsübersicht

Kapitel 1
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

§ 1 Anwendungsbereich
§ 2 Begriffsbestimmungen
§ 3 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Kapitel 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 4 Verarbeitung besonderer Kategorien personenbezogener Daten
§ 5 Verarbeitung zu anderen Zwecken und gemeinsame Dateisysteme
§ 6 Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken
§ 7 Einwilligung
§ 8 Verarbeitung auf Weisung des Verantwortlichen
§ 9 Datengeheimnis
§ 10 Automatisierte Einzelentscheidung

Kapitel 3
Rechte der betroffenen Person

§ 11 Allgemeine Informationen zu Datenverarbeitungen
§ 12 Benachrichtigung betroffener Personen
§ 13 Auskunftsrecht
§ 14 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung
§ 15 Verfahren für die Ausübung der Rechte der betroffenen Person
§ 16 Anrufung des Landesbeauftragten für den Datenschutz
§ 17 Verfahren bei Beschwerden, die in die Zuständigkeit einer anderen Aufsichtsbehörde eines EU-Mitgliedstaats fallen

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 18 Auftragsverarbeitung
§ 19 Gemeinsam Verantwortliche

§ 20 Anforderungen an die Sicherheit der Datenverarbeitung
§ 21 Meldung von Verletzungen des Schutzes personenbezogener Daten an den Landesbeauftragten für den Datenschutz
§ 22 Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten
§ 23 Durchführung einer Datenschutz-Folgenabschätzung
§ 24 Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz
§ 25 Anhörung des Landesbeauftragten für den Datenschutz
§ 26 Verzeichnis von Verarbeitungstätigkeiten
§ 27 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
§ 28 Unterscheidung zwischen verschiedenen Kategorien betroffener Personen
§ 29 Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen
§ 30 Verfahren bei Übermittlungen
§ 31 Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung
§ 32 Protokollierung
§ 33 Vertrauliche Meldung von Verstößen

Kapitel 5
Datenübermittlung an Drittstaaten und an internationale Organisationen

§ 34 Allgemeine Voraussetzungen
§ 35 Datenübermittlung bei geeigneten Garantien
§ 36 Datenübermittlung ohne geeignete Garantien
§ 37 Sonstige Datenübermittlung an Empfänger in Drittstaaten

Kapitel 6
Zusammenarbeit der Aufsichtsbehörden

§ 38 Gegenseitige Amtshilfe

Kapitel 7
Haftung und Sanktionen

§ 39 Schadensersatz und Entschädigung
§ 40 Strafvorschriften

Kapitel 8
Schlussbestimmungen

§ 41 Sprachliche Gleichstellung
§ 42 Einschränkung von Grundrechten

Kapitel 1
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

§ 1
Anwendungsbereich

(1) Die Vorschriften dieses Gesetzes gelten für die Verarbeitung personenbezogener Daten in Dateisystemen und Akten durch diejenigen öffentlichen Stellen, die zuständig sind

1. für die

   a) Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder
   b) Verfolgung oder Ahndung von Ordnungswidrigkeiten, die nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes fallen,

2. für den Vollzug der durch strafrichterliche Entscheidung angeordneten freiheitsentziehenden Maßregeln nach den §§ 63 und 64 des Strafgesetzbuchs,

soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Öffentliche Stellen im Sinne dieses Gesetzes sind Behörden und anderer öffentlich-rechtlich organisierter Einrichtungen des Landes, der Kommunen und sonstiger der Aufsicht des Landes unterstehender juristische Personen des öffentlichen Rechts sowie deren Vereinigungen, ungeachtet ihrer Rechtsform. Nimmt eine nicht-öffentliche Stelle Aufgaben aus Satz 1 wahr, ist sie insoweit öffentliche Stelle.

(2) Für die Verarbeitung personenbezogener Daten bei der straftatbezogenen Gefahrenabwehr der Polizeibehörden gelten die Vorschriften dieses Gesetzes.

§ 2
Begriffsbestimmungen

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Ab-

fragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Anonymisierung“ die Verarbeitung 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;

6. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;

7. „Verschlüsselung“ eine technische Maßnahme, die Daten unter Anwendung 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;

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

9. „Akte“ jede amtlichen, dienstlichen oder Geschäftszwecken dienende Unterlage, einschließlich Bild und Tonträger, jedoch ohne Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen; soweit die Unterlagen die in Nummer 8 festgelegten Kriterien erfüllen, können Akten auch Dateisysteme sein;

10. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

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

12. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

13. „Dritter“ eine natürliche oder juristische Person, Behörde oder Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiter befugt sind, die personenbezogenen Daten zu verarbeiten;

14. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;

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

16. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;

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

18. „besondere Kategorien personenbezogener Daten“

    a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

    b) genetische Daten,

    c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

d) Gesundheitsdaten und

e) Daten zum Sexualleben oder zur sexuellen Orientierung;

19. „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) eingerichtete unabhängige staatliche Stelle;

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

21. „zuständige Behörde“ jede öffentliche Stelle nach § 1 Abs. 1 Satz 3 und 4;

22. „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 3
Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

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

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

3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,

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

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

6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Kapitel 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 4
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

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

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,

2. die Festlegung von besonderen Aussonderungsprüffristen,

3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,

5. die von anderen Daten getrennte Verarbeitung,

6. die Pseudonymisierung personenbezogener Daten,

7. die Anonymisierung personenbezogener Daten,

8. die Verschlüsselung personenbezogener Daten oder

9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 5
Verarbeitung zu anderen Zwecken und gemeinsame Dateisysteme

(1) Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 1 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 1 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(2) Die Einrichtung eines automatisierten Abrufverfahrens oder eines gemeinsamen automatisierten Dateisystems, in oder aus der mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten, ist zulässig, soweit dies unter Berücksichtigung der Rechte und Freiheiten 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.

§ 6
Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

Personenbezogene Daten dürfen im Rahmen der in § 1 genannten Zwecke in archivarischer, wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

§ 7
Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

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

§ 8
Verarbeitung auf Weisung des Verantwortlichen

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

§ 9
Datengeheimnis

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

§ 10
Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

Kapitel 3
Rechte der betroffenen Person

§ 11
Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,

2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,

3. den Namen und die Kontaktdaten des Verantwortlichen und des Landesbeauftragten für den Datenschutz,

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

5. die Erreichbarkeit des Landesbeauftragten für den Datenschutz.

§ 12
Benachrichtigung betroffener Personen

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

1. die in § 11 genannten Angaben,

2. die Rechtsgrundlage der Verarbeitung,

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

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie

5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls

1. die Erfüllung der in § 1 genannten Aufgaben,

2. die öffentliche Sicherheit oder

3. Rechtsgüter Dritter

gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Absatz 2 gilt § 13 Abs. 7 entsprechend.

§ 13
Auskunftsrecht

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

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

2. die verfügbaren Informationen über die Herkunft der Daten,

3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,

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

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

6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,

7. das Recht nach § 16, 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 werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

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

(4) Der Verantwortliche kann unter den Voraussetzungen des § 12 Abs. 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 12 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über den Landesbeauftragten für den Datenschutz ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 16 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 die zuständige oberste Landesbehörde 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 des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. Der Landesbeauftragte für den Datenschutz hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 14
Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,

2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 1 dienen, weiter aufbewahrt werden müssen oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.

(4) Können personenbezogene Daten in Akten nicht einzeln gelöscht werden, ist eine Löschung nach den Absätzen 1 bis 3 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Soweit eine Löschung nach Satz 1 unterbleibt, sind die personenbezogenen Daten daraufhin zu kennzeichnen, dass ihre weitere Verarbeitung unterbleibt; Absatz 3 Satz 2 findet entsprechende Anwendung.

(5) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(6) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt werden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(7) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 12 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(8) § 13 Abs. 7 und 8 findet entsprechende Anwendung.

§ 15
Verfahren für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 13 Abs. 6 und des § 14 Abs. 7 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) Die Erteilung von Informationen nach § 11, die Benachrichtigungen nach den §§ 12 und 22 und die Bearbeitung von Anträgen nach den §§ 13 und 14 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 13 und 14 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des An-

trags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrages belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 13 oder 14 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 16
Anrufung des Landesbeauftragten für den Datenschutz

(1) Jedermann kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an den Landesbeauftragten für den Datenschutz wenden, wenn er der Auffassung ist, bei der Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen zu den in § 1 genannten Zwecken in seinen Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Der Landesbeauftragte für den Datenschutz hat die Beschwerde führende Person über den Stand und das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs zu unterrichten.

(2) Niemand darf wegen einer Beschwerde nach Absatz 1 benachteiligt oder gemaßregelt werden.

§ 17
Verfahren bei Beschwerden, die in die Zuständigkeit einer anderen Aufsichtsbehörde eines EU-Mitgliedstaates fallen

Der Landesbeauftragte für den Datenschutz hat eine bei ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiterzuleiten. Er hat in diesem Fall die Beschwerde führende Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 18
Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen und zu gewährleisten, dass dies durch den Landesbeauftragten für den Datenschutz kontrolliert werden kann. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den ge-

setzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;

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

3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;

5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 32 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;

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

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

8. alle gemäß § 20 erforderlichen Maßnahmen ergreift und

9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 20 bis 23 und § 25 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen.

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

(8) An die Stelle des Verantwortlichen können auch die Fachaufsichtsbehörden oder die von ihnen bestimmten Stellen über Genehmigungen nach Absatz 3 entscheiden und die erforderlichen Festlegungen nach Absatz 5 treffen. Entscheidungen der Fachaufsichtsbehörden oder der von ihnen bestimmten Stellen gelten als Entscheidungen des Verantwortlichen.

§ 19
Gemeinsam Verantwortliche

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

§ 20
Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Sie haben die Verarbeitung personenbezogener Daten an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere bei der Verarbeitung von besonderen Kategorien personenbezogener Daten ist von den Möglichkeiten der Anonymisierung, Pseudonymisierung oder Verschlüsselung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Der Verantwortliche hat die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnologie zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und

2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

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

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),

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

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),

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

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

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

12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit). Ein Zweck nach den Nummern 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 21
Meldung von Verletzungen des Schutzes personenbezogener Daten an den Landesbeauftragten für den Datenschutz

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, dem Landesbeauftragten für den Datenschutz zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat. Erfolgt die Meldung an den Landesbeauftragten für den Datenschutz nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

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

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,

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

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

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

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) Eine Meldung nach Artikel 33 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) oder eine Benachrichtigung 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 Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

(8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 22
Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 21 Abs. 3 Nrn. 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Von der Benachrichtigung nach Absatz 1 kann abgesehen werden, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;

2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr im Sinne des Absatzes 1 mehr besteht, oder

3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann der Landesbeauftragte für den Datenschutz förmlich feststellen, dass seiner Auffassung nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine erhebliche Gefahr im Sinne des Absatzes 1 zur Folge hat.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 12 Abs. 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Absatzes 1 überwiegen.

(6) § 21 Abs. 7 findet entsprechende Anwendung.

§ 23
Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Risikopotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat den Landesbeauftragten für den Datenschutz an der Durchführung der Datenschutz-Folgenabschätzung zu beteiligen.

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

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,

3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und

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

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

§ 24
Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz

Verantwortliche und Auftragsverarbeiter haben mit dem Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zusammenzuarbeiten. Die öffentlichen Stellen des Landes sind verpflichtet, dem Landesbeauftragten für den Datenschutz und seinen Beauftragten

1. jederzeit Zugang zu den Grundstücken und Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung seiner Aufgaben notwendig sind, zu gewähren und

2. alle Informationen, die für die Erfüllung seiner Aufgaben erforderlich sind, bereitzustellen.

§ 25
Anhörung des Landesbeauftragten für den Datenschutz

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden oder wesentlich geänderten Dateisystemen den Landesbeauftragten für den Datenschutz anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 23 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder

2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hat.

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

(2) Dem Landesbeauftragten für den Datenschutz sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 23 durchgeführte Datenschutz-Folgenabschätzung,

2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,

3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,

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

5. Name und Kontaktdaten des Landesbeauftragten für den Datenschutz.

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

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

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

§ 26
Verzeichnis von Verarbeitungstätigkeiten

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten des Landesbeauftragten für den Datenschutz,

2. die Zwecke der Verarbeitung,

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

4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

5. gegebenenfalls die Verwendung von Profiling,

6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,

7. Angaben über die Rechtsgrundlage der Verarbeitung,

8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und

9. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 20.

Soweit die Verarbeitungstätigkeit sich auf die Führung eines durch Rechtsvorschrift eingerichteten öffentlichen Registers beschränkt und die Rechtsvorschrift die Angaben nach Satz 2 Nrn. 1 bis 9 bereits enthält, gilt die Rechtsvorschrift als Verzeichnis.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Landesbeauftragten für den Datenschutz,

2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und

3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 20.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch und bei automatisierten Verfahren je Dateisystem zu führen. § 18 Abs. 8 gilt entsprechend.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse dem Landesbeauftragten für den Datenschutz zur Verfügung zu stellen.

§ 27
Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen An-

forderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

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

§ 28
Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende 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, und

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

§ 29
Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche

Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 30
Verfahren bei Übermittlungen

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(3) Die übermittelnde Stelle darf 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 Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 31
Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen,

1. wenn ihre Verarbeitung unzulässig ist,
2. sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder
3. ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(3) § 14 Abs. 3 bis 6 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

(5) Vor der Löschung nach Absatz 2 Nrn. 2 und 3 ist die Übermittlung personenbezogener Daten an das zuständige öffentliche Archiv zulässig, wenn das Archiv zuvor deren Archivwürdigigkeit festgestellt hat.

§ 32
Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

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

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

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch den Datenschutzbeauftragten, den Landesbeauftragten für den Datenschutz und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle dem Landesbeauftragten für den Datenschutz auf Anforderung zur Verfügung zu stellen.

§ 33
Vertrauliche Meldung von Verstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

Kapitel 5
Datenübermittlungen an Drittstaaten und an internationale Organisationen

§ 34
Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in § 1 genannten Zwecke zuständig ist und

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

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

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine gegenwärtige und erhebliche 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 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

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

§ 35
Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 34 Abs. 1 Nr. 2 kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 34 auch dann zulässig, wenn

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

2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche hat Übermittlungen nach Absatz 1 Nr. 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist dem Landesbeauftragten für den Datenschutz auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat den Landesbeauftragten für den Datenschutz zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nr. 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 36
Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 34 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 § 35 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 34 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,

2. zur Wahrung berechtigter Interessen der betroffenen Person,

3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,

4. im Einzelfall für die in § 1 genannten Zwecke oder

5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 1 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 35 Abs. 2 entsprechend.

§ 37
Sonstige Datenübermittlung an Empfänger in Drittstaaten

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 34 Abs. 1 Nr. 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

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

2. die Übermittlung an die in § 34 Abs. 1 Nr. 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und

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

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 34 Abs. 1 Nr. 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 35 Abs. 2 und 3 entsprechend.

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

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

Kapitel 6
Zusammenarbeit der Aufsichtsbehörden

§ 38
Gegenseitige Amtshilfe

(1) Der Landesbeauftragte für den Datenschutz hat den Datenschutzaufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. 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 hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang 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. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) Der Landesbeauftragte für den Datenschutz hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang

der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Er hat im Fall des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

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

(6) Der Landesbeauftragte für den Datenschutz hat Amtshilfeersuchen kostenfrei zu erledigen, soweit er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen des Landesbeauftragten für den Datenschutz hat alle erforderlichen Informationen zu enthalten; hierzu 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.

Kapitel 7
Haftung und Sanktionen

§ 39
Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

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

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

(4) Hat bei der Entstehung 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.

§ 40
Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 1 findet § 42 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) entsprechende Anwendung.

Kapitel 8
Schlussbestimmungen

§ 41
Sprachliche Gleichstellung

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

§ 42
Einschränkung 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.

Artikel 2
Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt

§ 30 Satz 1 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt in der Fassung der Bekanntmachung vom 6. April 2006 (GVBl. LSA S. 236), zuletzt geändert durch Artikel 2 des Gesetzes vom 3. Juli 2015 (GVBl. LSA S. 314, 317), erhält folgende Fassung:

> „Bei der Erfüllung der Aufgaben nach § 4 durch die Verfassungsschutzbehörde findet das Datenschutzgesetz Sachsen-Anhalt in der am 13. Januar 2016 geltenden Fassung (GVBl. LSA S. 24) mit Ausnahme der §§ 9 bis 13, 15, 16, 21 Abs. 3 und 4, 22 Abs. 4a und 26 Abs. 1 Anwendung.“

Artikel 3
Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt

Das Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt in der Fassung der Bekanntmachung vom 20. Mai 2014 (GVBl. LSA S. 182, 380), zuletzt geändert durch § 1 des Gesetzes vom 12. Juli 2017 (GVBl. LSA S. 130), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 13a erhält folgende Fassung:

      „§ 13a Geltung von anderen Vorschriften zum Schutz personenbezogener Daten“.

   b) Nach der Angabe zu § 13a werden folgende Angaben eingefügt:

      „§ 13b Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

§ 13c Informationssystem der Polizei
§ 13d Kennzeichnung personenbezogener Daten
§ 13e Regelung von Zugriffsberechtigungen für das Informationssystem der Polizei
§ 13f Verordnungsermächtigungen zur Sicherstellung erforderlicher organisatorischer und technischer Vorkehrungen im Informationssystem der Polizei“.

c) Die Angaben zu den §§ 22 bis 23b erhalten folgende Fassung:

„§ 22 Grundsätze des Verarbeitens personenbezogener Daten
§ 23 Verarbeiten von personenbezogenen Daten aus strafrechtlichen Ermittlungsverfahren; Daten zu Verurteilten, Beschuldigten, Tatverdächtigen, sonstigen Anlasspersonen und anderen Personen
§ 23a Weiterverarbeiten von personenbezogenen Daten, die von Strafverfolgungsbehörden der Mitgliedstaaten der europäischen Union an die Polizei übermittelt worden sind
§ 23b Aufzeichnung von Telefon- und Funkgesprächen“.

d) Nach der Angabe zu § 23b werden folgende Angaben eingefügt:

„§ 23c Ermittlung des Aufenthaltsorts gefährdeter Personen
§ 23d Speicherung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren“.

e) Die Angabe zu § 24 erhält folgende Fassung:

„§ 24 Benachrichtigung beim Speichern von personenbezogenen Daten von Kindern“.

f) Die Angabe zu § 25 erhält folgende Fassung:

„§ 25 Weiterverarbeiten für die wissenschaftliche Forschung“.

g) Nach der Angabe zu § 25 wird folgende Angabe eingefügt:

„§ 25a Weiterverarbeiten von Daten zur Aus- und Fortbildung sowie zu statistischen Zwecken“.

h) Die Angabe zu § 29 erhält folgende Fassung:

„§ 29 Datenübermittlungen zum Zweck von Zuverlässigkeitsüberprüfungen“.

i) Die Angabe zu § 32 erhält folgende Fassung:

„§ 32 Anbietungspflicht“.

j) Nach der Angabe zu § 32 werden folgende Angaben eingefügt:

„§ 32a Aussonderungsprüffristen und Löschfristen

§ 32b Berichtigung personenbezogener Daten sowie Einschränkung der Verarbeitung in Akten sowie Vernichtung von Akten
§ 32c Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten“.

k) Nach der Angabe zu § 109 wird folgende Angabe eingefügt:

„§ 109a Übergangsvorschrift für die Verarbeitung personenbezogener Daten durch die Polizei“.

2. In § 6 Abs. 3 werden nach dem Wort „Rasse,“ die Wörter „seiner Ethnie,“ und nach dem Wort „Anschauungen“ die Wörter „, seiner Gewerkschaftszugehörigkeit“ eingefügt.

3. In § 12 Abs. 4 Satz 4 wird die Angabe „§§ 25 und 32 Abs. 7 bis 9“ durch die Angabe „§§ 25, 25a und 32 Abs. 9“ ersetzt.[1]

4. § 13a erhält folgende Fassung:

„§ 13a
Geltung von anderen Vorschriften zum Schutz personenbezogener Daten

(1) Bei der Verarbeitung personenbezogener Daten gelten, soweit dieses Gesetz oder die nachstehenden Regelungen nicht anderes bestimmen, die Vorschriften des Datenschutzgesetzes Sachsen-Anhalt.

(2) Die Vorschriften dieses Gesetzes sind bei der Verarbeitung personenbezogener Daten im Anwendungsbereich 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) in der jeweils geltenden Fassung, zu beachten, soweit dieses Gesetz spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen oder die Pflichten oder Rechte nach Art. 23 Abs. 1 Datenschutz-Grundverordnung beschränken.

(3) Bei der Verarbeitung personenbezogener Daten durch

1. die Polizei zum Zweck

a) der Verhütung, Erforschung, Verfolgung oder Ahndung von Straftaten einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit oder
b) der Erforschung, Verfolgung, Ahndung oder Vollstreckung von Ordnungswidrigkeiten

oder

2. die Sicherheitsbehörden zum Zweck der Verfolgung, Ahndung oder Vollstreckung von Ordnungswidrigkeiten

[1] Erläuternde Anmerkung (nicht Bestandteil des Entwurfs). Diese Änderung betrifft eine Regelung im SOG LSA in der am dem 1. Juli 2018 geltenden Fassung

gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt.“

5. Nach § 13a werden folgende §§ 13b bis 13f eingefügt:

„§ 13b
Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

(1) Die Polizei kann personenbezogene Daten, die sie selbst erhoben hat, weiterverarbeiten

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

Beim Weiterverarbeiten von personenbezogenen Daten, die aus Maßnahmen nach § 17 Abs. 4 oder § 17b Abs. 1 erlangt wurden, muss im Einzelfall eine Gefahr im Sinne des § 17 Abs. 4 vorliegen.

(2) Die Polizei kann zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn

1. mindestens

   a) vergleichbar schwerwiegende Straftaten verhütet, aufgedeckt oder verfolgt oder
   b) vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und

2. sich im Einzelfall

   a) konkrete Ermittlungsansätze zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder
   b) tatsächliche Anhaltspunkte zur Abwehr von Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.

§ 22 Abs. 5 und die §§ 25 und 25a bleiben unberührt.

(3) Für das Weiterverarbeiten von personenbezogenen Daten, die durch Maßnahmen nach § 17 Abs. 4 oder § 17b Abs. 1 erlangt wurden, gilt Absatz 2 Satz 1 Nr. 2 Buchst. b mit der Maßgabe entsprechend, dass im Einzelfall eine Gefahr im Sinne des § 17 Abs. 4 vorliegen muss. Personenbezogene Daten, die durch Herstellung von Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

(4) Abweichend von Absatz 2 kann die Polizei die vorhandenen Grunddaten (§ 23 Abs. 2 Nr. 1 Buchst. a) weiterverarbeiten, um diese Person zu identifizieren.
(5) Beim Weiterverarbeiten von personenbezogenen Daten stellt die verantwortliche Polizeibehörde durch organisatorische und technische Vorkehrungen sicher, dass die Absätze 1 bis 4 beachtet werden.

§ 13c
Informationssystem der Polizei

Die Polizei betreibt zur Strafverfolgung, vorbeugenden Bekämpfung von und Vorsorge für die Verfolgung von Straftaten und zur Gefahrenabwehr ein Informationssystem. Es erfüllt insbesondere folgende Grundfunktionen:

1. Unterstützung bei polizeilichen Ermittlungen,
2. Unterstützung bei Ausschreibungen von sowie Fahndungen nach Personen und Sachen,
3. Unterstützung bei der polizeilichen Informationsverdichtung durch Abklärung von Hinweisen und Spurenansätzen,
4. Durchführung von Abgleichen von personenbezogenen Daten,
5. Unterstützung bei der Erstellung von strategischen Analysen und Statistiken.

§ 13d
Kennzeichnung personenbezogener Daten

(1) Bei der Speicherung im Informationssystem der Polizei sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie nach dem § 23 bei Personen, zu denen Grunddaten angelegt wurden,
3. Angabe der
   a) Rechtsgüter, deren Schutz die Erhebung dient oder
   b) Straftaten, deren Verfolgung oder Verhütung die Erhebung dient,
4. Angabe der Stelle, die sie erhoben hat.

Die Kennzeichnung nach Satz 1 Nr. 1 kann auch durch Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden.

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

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

§ 13e
Regelung von Zugriffsberechtigungen für das Informationssystem der Polizei

(1) Die Polizei hat bei der Erteilung von Zugriffsberechtigungen der Nutzer des Informationssystems der Polizei sicherzustellen, dass

1. auf Grundlage der nach § 13d Abs. 1 vorzunehmenden Kennzeichnungen die Vorgaben des § 13b bei der Nutzung des Informationssystems beachtet werden und

2. der Zugriff nur auf diejenigen personenbezogenen Daten und Erkenntnisse möglich ist, deren Kenntnis für die Erfüllung der jeweiligen dienstlichen Pflichten erforderlich ist.

(2) Die Polizei hat darüber hinaus sicherzustellen, dass Änderungen, Berichtigungen und Löschungen von personenbezogenen Daten im Informationssystem nur durch eine hierzu befugte Person erfolgen können.

(3) Die Polizei trifft hierzu alle erforderlichen organisatorischen und technischen Vorkehrungen und Maßnahmen, die dem Stand der Technik entsprechen. Die Vergabe von Zugriffsberechtigungen auf die im Informationssystem gespeicherten Daten erfolgt auf der Grundlage eines abgestuften Rechte- und Rollenkonzeptes, das die Umsetzung der Maßgaben der Absätze 1 und 2 technisch und organisatorisch sicherstellt. Die Erstellung und Fortschreibung des abgestuften Rechte- und Rollenkonzeptes erfolgt im Benehmen mit dem Landesbeauftragten für den Datenschutz.

(4) Das Informationssystem der Polizei ist so zu gestalten, dass eine weitgehende Standardisierung der nach § 32 Abs. 1 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt zu protokollierenden Abfragegründe im Rahmen der Aufgaben der Polizei erfolgt.

§ 13f
Verordnungsermächtigungen zur Sicherstellung erforderlicher organisatorischer und technischer Vorkehrungen im Informationssystem der Polizei

Das für öffentliche Sicherheit und Ordnung zuständige Ministerium wird ermächtigt, durch Verordnung einer Polizeibehörde Pflichten zur Sicherstellung organisatorischer und technischer Vorkehrungen nach § 13b Abs. 5 oder § 13e Abs. 3 oder 4 zu übertragen, wenn dies zur sachgerechten Erfüllung der Pflichten erforderlich ist. Es kann dabei auch die Weisungsbefugnis gegenüber anderen Polizeibehörden regeln.“

6. § 15 wird wie folgt geändert:

   a) In Absatz 4 Satz 3 werden die Wörter „oder Nutzung“ gestrichen.
   b) Absatz 7 wird wie folgt geändert:

      aa) Die Sätze 3 und 4 werden aufgehoben.
      bb) Die Sätze 5 und 6 werden die Sätze 3 und 4.

7. § 16 wird wie folgt geändert:

a) Absatz 5 erhält folgende Fassung:

„(5) Die Aufzeichnungen sind nach Ablauf des Zeitraumes, der für die Feststellung ausreicht, ob die Aufzeichnungen im Sinne des Satzes 3 benötigt werden, zu löschen. Im Übrigen sind Bild- und Tonaufzeichnungen, in einem Dateisystem gespeicherte personenbezogene Daten spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten. Dies gilt nicht, wenn die Daten zur Verfolgung von Straftaten benötigt werden oder tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. In

den in Satz 3 genannten Fällen müssen personenbezogene Daten unbeteiligter Personen gelöscht oder unkenntlich gemacht werden, soweit dies ohne unverhältnismäßig hohen Aufwand möglich ist. § 15 Abs. 7 Satz 3 Halbsatz 2 gilt entsprechend. Die §§ 25 und 25a bleiben unberührt.“

b) In Absatz 5a Satz 3 wird die Angabe „§ 32 Abs. 7 bis 9“ durch die Angabe „§ 32 Abs. 9“ ersetzt.

8. § 17 wird wie folgt geändert:

a) In Absatz 2 Satz 5 wird die Angabe „§ 15 Abs. 7 Satz 5 Halbsatz 2“ durch die Angabe „§ 15 Abs. 7 Satz 3“ ersetzt.
b) Absatz 4e wird aufgehoben.
c) Absatz 7 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ ersetzt.
bb) In Satz 2 im Satzteil vor Nummer 1 und Nummer 3 werden jeweils das Wort „Unterrichtung“ durch das Wort „Benachrichtigung“ ersetzt.

9. In § 17b Abs. 5 Satz 3 wird die Angabe „§ 17 Abs. 4b bis 4e und 5a“ durch die Angabe „§ 13b Abs. 3 und § 17 Abs. 4b bis 4d und 5a“ ersetzt.

10. In § 18 Abs. 6 Satz 2 wird das Wort „Unterrichtung“ durch das Wort „Benachrichtigung“ ersetzt.

11. In § 19 Abs. 1 werden die Wörter „einer als Teil des polizeilichen Fahndungsbestandes geführten Datei“ durch die Wörter „einem als Teil des polizeilichen Fahndungsbestandes geführten Dateisystem“ ersetzt.

12. In § 20a Abs. 1 Satz 5 werden die Wörter „einer Datei“ durch die Wörter „einem Dateisystem“ ersetzt.

13. § 22 wird wie folgt geändert:

a) In Absatz 1 werden die Wörter „Dateien speichern, verändern oder nutzen“ durch die Wörter „Dateisystemen verarbeiten“ ersetzt.
b) Absatz 2 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „speichern, verändern oder nutzen“ durch das Wort „verarbeiten“ ersetzt.
bb) In Satz 2 werden die Wörter „Speichern, Verändern oder Nutzen“ durch das Wort „Verarbeiten“ ersetzt.

c) Absatz 3 erhält folgende Fassung:

„(3) Die Protokollierung nach § 32 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt erfolgt zu Verarbeitungsvorgängen im Informationssystem der Polizei ergänzend zu den dort genannten Anforderungen in einer Weise, dass die Protokolle

1. den Datenschutzbeauftragten und dem Landesbeauftragten für den Datenschutz in elektronisch auswertbarer Form für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung zur Verfügung stehen und
2. eine Überprüfung ermöglichen, dass Zugriffe auf personenbezogene Daten im Informationssystem der Polizei innerhalb der Zugriffsberechtigungen nach § 13d erfolgen.

Es ist insbesondere der Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Dienststelle zu protokollieren.“

d) Absatz 4 wird aufgehoben.
e) Absatz 5 erhält folgende Fassung:

„(5) Die Sicherheitsbehörden und die Polizei können zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns personenbezogene Daten verarbeiten; die Absätze 1 bis 3 sowie die §§ 23 und 23a finden insoweit keine Anwendung.“

f) In Absatz 6 wird das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.

14. § 23 erhält folgende Fassung:

„§ 23
Weiterverarbeiten von personenbezogenen Daten aus strafrechtlichen Ermittlungsverfahren; Daten zu Verurteilten, Beschuldigten, Tatverdächtigen, sonstigen Anlasspersonen und anderen Personen

(1) Die Polizei kann personenbezogene Daten, die sie im Rahmen von strafrechtlichen Ermittlungsverfahren gewonnen hat, zur Abwehr einer Gefahr, vorbeugenden Bekämpfung von Straftaten oder Vorsorge für die Verfolgung von Straftaten weiterverarbeiten von

1. Verurteilten,
2. Beschuldigten,
3. Personen, die einer Straftat verdächtig sind, sofern das Weiterverarbeiten der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und
4. Personen, bei denen Anlass zum Weiterverarbeiten der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).

(2) Die Polizei kann weiterverarbeiten:

1. von Personen nach Absatz 1 Nrn. 1 bis 4

   a) die Grunddaten wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Anschrift und
   b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale,

c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,
d) die Tatzeiten und Tatorte,
e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten;

2. von Personen nach Absatz 1 Nrn. 1 und 2 weitere personenbezogene Daten, soweit das Weiterverarbeiten der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind;

3. von Personen nach Absatz 1 Nrn. 3 und 4 weitere personenbezogene Daten.

(3) Die Polizei kann personenbezogene Daten weiterverarbeiten, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach Absatz 1 erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck weiterverarbeitet werden und sind im Informationssystem der Polizei gesondert zu speichern. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt.

(4) Die Polizei kann personenbezogene Daten weiterverarbeiten, soweit dies erforderlich ist zum Zweck des Nachweises von Personen, die wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen. Die Löschung von Daten, die allein zu diesem Zweck weiterverarbeitet werden, erfolgt nach zwei Jahren.

(5) Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist das Weiterverarbeiten unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

(6) Soweit es zur Abwehr einer erheblichen Gefahr, vorbeugenden Bekämpfung von Straftaten oder Vorsorge für die Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich ist, kann die Polizei zur Erfüllung ihrer Aufgaben nach § 2 personenbezogene Daten von Personen weiterverarbeiten, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen,
2. sie als Opfer einer künftigen Straftat in Betracht kommen,
3. sie mit in Absatz 1 Nrn. 1 bis 3 bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken, oder
4. es sich um Hinweisgeber und sonstige Auskunftspersonen handelt.

Das Weiterverarbeiten nach Satz 1 ist zu beschränken auf die in Absatz 2 Nr. 1 Buchst. a bis c bezeichneten Daten sowie auf die Angabe, in welcher Eigenschaft der Person und in Bezug auf welchen Sachverhalt die Speicherung der Daten erfolgt. Personenbezogene Daten über Personen nach Satz 1 Nrn. 1, 2 und 4 dürfen nur mit Einwilligung der betroffenen Person gespeichert werden. Die Einwilligung ist nicht erforderlich, wenn das Bekanntwerden der Speicherungsabsicht den mit der Speicherung verfolgten Zweck gefährden würde.

(7) Die Polizei kann personenbezogene Daten weiterverarbeiten von Vermissten, unbekannten Personen und unbekannten Toten

1. zu Zwecken der Identifizierung,
2. zur Abwehr einer erheblichen Gefahr für die genannten Personen.

Entsprechendes gilt, soweit es sonst zur Erfüllung ihrer Aufgaben erforderlich ist, weil tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um Täter, Opfer oder Zeugen im Zusammenhang mit einer Straftat handelt.

(8) Die Polizei kann personenbezogene Daten weiterverarbeiten, um festzustellen, ob die betreffenden Personen die Voraussetzungen nach Absatz 6 oder Absatz 7 erfüllen. Die Daten dürfen ausschließlich zu diesem Zweck weiterverarbeitet werden und sind im Informationssystem der Polizei gesondert zu speichern. Die Daten sind nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 6 oder Absatz 7 erfüllt.“

15. Nach § 23 wird folgender neuer § 23a eingefügt:

„§ 23a
Verarbeiten von personenbezogenen Daten, die von Strafverfolgungsbehörden der Mitgliedstaaten der europäischen Union an die Polizei übermittelt worden sind

Daten, die von Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union an die Polizei übermittelt worden sind, dürfen nur für die Zwecke, für die sie übermittelt wurden, oder zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit verarbeitet werden. Für einen anderen Zweck oder als Beweismittel in einem gerichtlichen Verfahren dürfen sie nur verarbeitet werden, wenn der übermittelnde Staat zugestimmt hat. Von dem übermittelnden Staat für die Verarbeitung der Daten gestellte Bedingungen sind zu beachten. Die Polizei erteilt dem übermittelnden Staat auf dessen Ersuchen zu Zwecken der Datenschutzkontrolle Auskunft darüber, wie die übermittelten Daten verarbeitet wurden.“

16. Der bisherige § 23a wird § 23b und wie folgt geändert:

a) In Satz 3 wird das Wort „sperren“ durch die Wörter „in der Verarbeitung einzuschränken“ ersetzt.
b) Satz 4 erhält folgende Fassung:
„Die §§ 25, 25a und 32 Abs. 9 bleiben unberührt.“

17. Der bisherige § 23b wird § 23c und in Absatz 3 Satz 4 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ ersetzt.

18. Nach § 23c wird folgender § 23d eingefügt:

„§ 23d
Speicherung von DNA-Identifizierungsmustern
zur Erkennung von DNA-Trugspuren

(1) Die Polizei kann auf Grundlage einer Einwilligung von ihren Mitarbeitern, die Umgang mit Spurenmaterial haben oder die Bereiche in ihren Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird,

1. mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen entnehmen,
2. diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen und
3. die festgestellten DNA-Identifizierungsmuster mit den an Spurenmaterial festgestellten DNA-Identifizierungsmustern automatisiert abgleichen, um zur Erkennung von DNA-Trugspuren festzustellen, ob an Spurenmaterial festgestellte DNA-Identifizierungsmuster von diesen Personen stammen.

Die entnommenen Körperzellen dürfen nur für die in Satz 1 genannte molekulargenetische Untersuchung verwendet werden; sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Bei der Untersuchung dürfen andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, nicht getroffen werden; hierauf gerichtete Untersuchungen sind unzulässig.

(2) Untersuchungen und Abgleiche nach Absatz 1 bei Personen, die nicht Mitarbeiter der Polizei sind, dürfen nur mit deren Einwilligung erfolgen.

(3) Die nach den Absätzen 1 und 2 erhobenen Daten sind zu pseudonymisieren und darüber hinaus im Informationssystem der Polizei gesondert zu speichern. Eine Verwendung dieser Daten zu anderen als den in den Absätzen 1 und 2 genannten Zwecken ist unzulässig. Die DNA-Identifizierungsmuster sind zu löschen, wenn sie für die genannten Zwecke nicht mehr erforderlich sind. Die Löschung hat spätestens drei Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem in Absatz 1 Satz 1 genannten Bereich zu erfolgen. Betroffene Personen sind schriftlich über den Zweck und die Speicherung sowie die Löschung der erhobenen Daten zu informieren.“

19. § 24 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 24
Benachrichtigung beim Speichern von personenbezogenen Daten von Kindern.“

b) Absatz 1 wird aufgehoben.
c) Die Absatzbezeichnung „(2)“ wird gestrichen.

d) In Satz 1 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ ersetzt.
e) In Satz 2 wird das Wort „Unterrichtung“ jeweils durch das Wort „Benachrichtigung“ ersetzt.

20. § 25 erhält folgende Fassung:

„§ 25
Weiterverarbeiten für die wissenschaftliche Forschung

(1) Die Polizei kann im Rahmen ihrer Aufgaben bei ihr vorhandene personenbezogene Daten, wenn dies für bestimmte wissenschaftliche Forschungsarbeiten erforderlich ist, weiterverarbeiten, soweit eine Weiterverarbeitung anonymisierter Daten zu diesem Zweck nicht möglich ist und das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse der betroffenen Person erheblich überwiegt. Das Weiterverarbeiten von personenbezogenen Daten, die aus in § 13b Abs. 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen.

(2) Die Polizei kann personenbezogene Daten an Hochschulen, andere Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentliche Stellen übermitteln, soweit

1. dies für die Durchführung bestimmter wissenschaftlicher Forschungsarbeiten erforderlich ist,
2. ein Weiterverarbeiten anonymisierter Daten zu diesem Zweck nicht möglich ist und
3. das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Übermittlung erheblich überwiegt.

Eine Übermittlung von personenbezogenen Daten im Sinne des Absatzes 1 Satz 2 ist ausgeschlossen.

(3) Die Übermittlung der Daten erfolgt durch Erteilung von Auskünften, wenn hierdurch der Zweck der Forschungsarbeit erreicht werden kann und die Erteilung keinen unverhältnismäßigen Aufwand erfordert. Andernfalls kann auch Akteneinsicht gewährt werden. Einsicht in elektronische Akten wird durch Bereitstellen des Inhalts der Akte zum Abruf gewährt. Ein Aktenausdruck oder ein Datenträger mit dem Inhalt der elektronischen Akten wird auf besonders zu begründenden Antrag nur übermittelt, wenn die antragstellende Person hieran ein berechtigtes Interesse hat. Einsicht in Akten, die in Papierform vorliegen, wird durch Bereitstellen des Inhalts der Akte zur Einsichtnahme in Diensträumen gewährt. Auf besonderen Antrag wird die Einsicht in Akten, die in Papierform vorliegen, durch Übersendung von Kopien, durch Übergabe zur Mitnahme oder durch Übersendung der Akten gewährt.

(4) Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Abs. 2, 3 und 4 Nr. 2 des Verpflichtungsgesetzes findet auf die Verpflichtung zur Geheimhaltung entsprechende Anwendung.

(5) Die personenbezogenen Daten dürfen nur für die Forschungsarbeit weiterverarbeitet werden, für die sie übermittelt worden sind. Das Weiterverarbeiten für andere Forschungsarbeiten oder die Weitergabe richtet sich nach den Absätzen 2 bis 4 und bedarf der Zustimmung der Stelle, die die Daten übermittelt hat.

(6) Durch organisatorische und technische Maßnahmen hat die wissenschaftliche Forschung betreibende Stelle zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

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

(8) Wer nach den Absätzen 2 bis 4 personenbezogene Daten erhalten hat, darf diese nur veröffentlichen, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist und das Landeskriminalamt zugestimmt hat.“

21. Nach § 25 wird folgender § 25a eingefügt:

„§ 25a
Weiterverarbeiten von Daten
zur Aus- und Fortbildung sowie zu statistischen Zwecken

Die Polizei kann bei ihr vorhandene personenbezogene Daten zur polizeilichen Aus- und Fortbildung oder zu statistischen Zwecken weiterverarbeiten, soweit das Weiterverarbeiten anonymisierter Daten zu diesem Zweck nicht möglich ist. Entsprechendes gilt für die Übermittlung an das Bundeskriminalamt zu kriminalstatistischen Zwecken. Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. § 25 Abs. 1 Satz 2 und Abs. 2 Satz 2 gilt entsprechend.“

22. § 26 wird wie folgt geändert:

a) In Absatz 1 Satz 2 Halbsatz 2 wird das Wort „Abrufverfahren“ durch die Wörter „Verfahren auf Abruf“ ersetzt.
b) In Absatz 4 wird die Angabe „§ 41“ durch die Angabe „§§ 41 und 61“ und die Angabe „§§ 51 und 52“ durch die Angabe „§§ 51, 52 und 63“ ersetzt.

23. § 27 wird wie folgt geändert:

a) In Absatz 2 Satz 2 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ ersetzt.
b) Nach Absatz 3 wird folgender Absatz 3a eingefügt:

„(3a) Die Polizei kann personenbezogene Daten einschließlich nicht gefahren- oder tatbezogener persönlicher Merkmale von Personen, die nach diesem Gesetz oder anderen Rechtsvorschriften von ihr festgehalten werden, an Stellen,

die aufgrund völkerrechtlicher Übereinkommen zur Überprüfung der Einhaltung der Rechte festgehaltener Personen zuständig sind, übermitteln.“

24. § 27a wird wie folgt geändert:

a) Absatz 5 wird aufgehoben.
b) Die bisherigen Absätze 6 bis 8 werden die Absätze 5 bis 7.
c) In Absatz 7 wird die Angabe „Absätze 1 bis 7“ durch die Angabe „Absätze 1 bis 6“ ersetzt.

25. § 28 wird wie folgt geändert:

a) Nach Absatz 2 wird folgender neuer Absatz 3 eingefügt:

„(3) Die Polizei kann personenbezogene Daten, die der Kontaktaufnahme zu einer Person dienen, zum Zweck der persönlichen Beratung dieser Person an nichtöffentliche Stellen übermitteln, wenn die betroffene Person oder ein Sorgeberechtigter in Kenntnis des Zwecks der Datenübermittlung eingewilligt hat oder tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies im Interesse der Person liegt und sie in Kenntnis des Zwecks einwilligen würde.“

b) Der bisherige Absatz 3 wird Absatz 4.

26. § 29 erhält folgende Fassung:

„§ 29
Datenübermittlungen zum Zweck von Zuverlässigkeitsüberprüfungen

(1) Die Polizei kann auf der Grundlage der Einwilligung einer betroffenen Person ihre nach § 23 Abs. 1 im Informationssystem der Polizei des Landes Sachsen-Anhalt gespeicherten oder im polizeilichen Informationsverbund zwischen Bund und Ländern zum Abruf durch die Polizei bereitstehenden personenbezogenen Daten zum Zweck der Durchführung einer Zuverlässigkeitsüberprüfung weiterverarbeiten. Die Polizei kann hierfür die Identität der betroffenen Person feststellen und von ihr vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern.

(2) Eine Zuverlässigkeitsüberprüfung kann insbesondere zu folgenden Zwecken durchgeführt werden:

1. privilegierter Zutritt zu einer besonders gefährdeten Veranstaltung in öffentlicher oder nichtöffentlicher Trägerschaft,
2. privilegierter Zutritt zu einem Amtsgebäude oder einem anderen gefährdeten Objekt, sofern dies aufgrund der Gefährdungslage erforderlich ist,
3. Erbringung selbständiger Dienstleistungen zur Unterstützung von Vollzugsaufgaben,
4. Einstellung in den Polizeivollzugsdienst.

Die Vorschriften des Bundes oder Landes zur Durchführung von Sicherheitsüberprüfungen bleiben unberührt.

(3) Das Ergebnis einer Zuverlässigkeitsüberprüfung kann einer öffentlichen oder nichtöffentlichen Stelle übermittelt werden. Ist der Empfänger eine nichtöffentliche Stelle, beschränkt sich die Datenübermittlung auf die Einschätzung, ob tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die betroffene Person unzuverlässig ist. Die Polizei hat den Empfänger der personenbezogenen Daten der betroffenen Person schriftlich zu verpflichten, die Zweckbestimmung einzuhalten und eine Löschung der personenbezogenen Daten spätestens nach Wegfall des Zwecks vorzunehmen. Beabsichtigt der nicht öffentliche Empfänger der überprüften Person trotz Sicherheitsbedenken den privilegierten Zugang zu einer besonders gefährdeten Veranstaltung zu gewähren, teilt er dies der Polizei unverzüglich mit.“

27. In § 30 Abs. 1 Satz 1 und Abs. 2 wird jeweils das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.

28. In § 31 Abs. 5 Satz 1 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ und das Wort „Datennutzung“ durch das Wort „Datenverwendung“ ersetzt.

29. § 32 erhält folgende Fassung:

„§ 32
Anbietungspflicht

Vor der Löschung oder Vernichtung von Dateisystemen oder Akten, die personenbezogene Daten enthalten, bei denen nach einer zu einer bestimmte Frist vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist, sind diese nach Maßgabe des Archivgesetzes Sachsen-Anhalt dem zuständigen öffentlichen Archiv anzubieten und zu übergeben. Solange eine fristgerechte Entscheidung über die Archivwürdigkeit aussteht, dürfen die angebotenen Akten und Dateisysteme nur nach Maßgabe des Archivgesetzes Sachsen-Anhalt oder zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person genutzt werden.“

30. Nach § 32 werden folgende §§ 32a bis 32c eingefügt:

„§ 32a
Aussonderungsprüffristen und Löschfristen

(1) Die Polizei prüft nach § 31 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt bei der Einzelfallbearbeitung und nach festgesetzten Fristen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Die Aussonderungsprüffristen nach § 31 Abs. 4 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt dürfen bei im Informationssystem der Polizei verarbeiteten personenbezogenen Daten bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist. Die Beachtung der Aussonderungsprüffristen ist durch geeignete technische Maßnahmen zu gewährleisten.

(2) In den Fällen des § 23 Abs. 6 dürfen die Aussonderungsprüffristen bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre nicht überschreiten. Personenbezogene Daten der in § 23 Abs. 6 Satz 1 Nrn. 1 bis 4 bezeichneten Personen können

ohne Zustimmung der betroffenen Person nur für die Dauer eines Jahres gespeichert werden. Die Speicherung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des § 23 Abs. 6 weiterhin vorliegen. Die maßgeblichen Gründe für die Aufrechterhaltung der Speicherung nach Satz 3 sind aktenkundig zu machen. Die Speicherung nach Satz 2 darf jedoch insgesamt drei Jahre und bei der Verhütung und Verfolgung von Straftaten nach § 129a, auch in Verbindung mit § 129b Abs. 1 des Strafgesetzbuchs sowie nach den §§ 6 bis 13 des Völkerstrafgesetzbuchs fünf Jahre nicht überschreiten.

(3) Die Fristen beginnen mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Die Speicherung kann über die in Absatz 1 Satz 2 genannten Fristen hinaus auch allein für Zwecke der Vorgangsverwaltung aufrechterhalten werden, sofern dies erforderlich ist; in diesem Falle können die Daten nur noch für diesen Zweck oder zur Behebung einer bestehenden Beweisnot verwendet werden.

§ 32b
Berichtigung personenbezogener Daten sowie Einschränkung der Verarbeitung in Akten sowie Vernichtung von Akten

(1) Stellt die Polizei die Unrichtigkeit personenbezogener Daten in Akten fest, ist die in § 31 Abs. 1 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt genannte Berichtigungspflicht dadurch zu erfüllen, dass dies in der Akte vermerkt oder auf sonstige Weise festgehalten wird. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten entsprechend zu kennzeichnen, um eine Verarbeitungseinschränkung nach § 14 Abs. 1 Satz 2 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt zu ermöglichen.

(2) Die Polizei hat die Verarbeitung personenbezogener Daten in Akten einzuschränken, wenn

1. die Verarbeitung unzulässig ist oder
2. aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Kenntnis der Daten zur Erfüllung der der Polizei obliegenden Aufgaben nicht mehr erforderlich ist oder eine Löschungsverpflichtung nach § 32a Abs. 3 besteht.

Die Akte ist zu vernichten, wenn sie insgesamt zur Erfüllung der Aufgaben der Polizei nicht mehr erforderlich ist. Die Vernichtung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass andernfalls schutzwürdige Interessen der betroffenen Person beeinträchtigt würden oder
2. die personenbezogenen Daten für Zwecke eines gerichtlichen Verfahrens weiter aufbewahrt werden müssen.

In diesen Fällen ist die Verarbeitung der Daten einzuschränken und sind die Unterlagen mit einem entsprechenden Einschränkungsvermerk zu versehen.

(3) In ihrer Verarbeitung eingeschränkte Daten dürfen nur für den Zweck verarbeitet werden, für den die Vernichtung der Akte unterblieben ist; sie dürfen auch verarbeitet werden, wenn dies zur Behebung einer bestehenden Beweisnot unerlässlich ist oder die betroffene Person einwilligt.
(4) § 31 Abs. 4 und 5 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt gilt entsprechend.

§ 32c
Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten

(1) Über die in den §§ 13 und 14 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt enthaltenen Rechte der betroffenen Person hinaus gilt für die Verarbeitung im polizeilichen Informationssystem die Besonderheit, dass bei Daten, die dort verarbeitet werden, das Landeskriminalamt die Auskunft nach § 13 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt im Einvernehmen mit der Stelle, die die datenschutzrechtliche Verantwortung trägt, erteilt. Bei der Berichtigung, Löschung und Verarbeitungseinschränkung personenbezogener Daten findet Satz 1 entsprechende Anwendung bei Daten, die im polizeilichen Informationssystem verarbeitet werden.

(2) Sind die Daten der betroffenen Person im polizeilichen Informationssystem gespeichert und ist die betroffene Person nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann sie sich zur Geltendmachung ihrer Rechte an das Landeskriminalamt wenden. Dieses ist verpflichtet, das Vorbringen der betroffenen Person an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Die betroffene Person ist über die Weiterleitung und jene Stelle zu unterrichten. Das Landeskriminalamt kann statt der betroffenen Person den Landesbeauftragten für den Datenschutz unterrichten. Das weitere Verfahren richtet sich nach § 57 Abs. 7 Satz 3 und 6 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt.

(3) Bei der Datenverarbeitung im polizeilichen Informationssystem gilt das Landeskriminalamt gegenüber einer betroffenen Person als allein Verantwortlicher im Sinne von § 39 Abs. 1 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt. § 39 Abs. 3 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt ist nicht anzuwenden.“

31. Nach § 109 wird folgender § 109a eingefügt:

„§ 109a
Übergangsvorschrift für die Verarbeitung personenbezogener Daten durch die Polizei

Abweichend von § 13d Abs. 2 ist das Verarbeiten personenbezogener Daten mit Hilfe automatisierter Verfahren auch zulässig nach den Bestimmungen des für die Daten am [Einsetzen Inkrafttreten dieses Gesetzes] jeweils geltenden Verfahrensverzeichnisses nach § 14 Abs. 3 des Datenschutzgesetzes Sachsen-Anhalt in der Fassung der Bekanntmachung vom 13. Februar 20016 (GVBl. LSA S. 24, 25), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Februar 2018 (GVBl. LSA S. 10) .“

Artikel 4
Änderung des Maßregelvollzugsgesetzes Sachsen-Anhalt

Das Maßregelvollzugsgesetz Sachsen-Anhalt vom 21. Oktober 2010 (GVBl. S. 510) wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) In der Überschrift des Abschnitts 5 werden die Wörter „Dokumentation, Datenerhebung und“ gestrichen.

b) Die Angaben zu den §§ 33 und 34 erhalten folgende Fassung:

„§ 33 Optisch-elektronische Beobachtung und Verarbeitung von Bildaufzeichnungen

§ 34 Datenverwendung“.

c) Die Angabe zu § 36 erhält folgende Fassung:

„§ 36 Datenübermittlung zu archivarischen, wissenschaftlichen und statistischen Zwecken“.

2. In § 3 Abs. 1 Satz 3 werden die Wörter „, die oder der die Befähigung zum Richteramt besitzen muss“ gestrichen.

3. In der Überschrift des Abschnitts 5 werden die Wörter „Dokumentation, Datenerhebung und“ gestrichen.

4. § 32 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 2 werden die Wörter „erheben und“ gestrichen.

bb) Satz 3 wird wie folgt geändert:

aaa) In Nummer 7 wird das Komma am Ende durch einen Punkt ersetzt.

bbb) Die Nummern 8 und 9 werden aufgehoben.

b) Nach Absatz 1 wird folgender neuer Absatz 2 eingefügt:

„(2) Soweit im Zusammenhang mit dem Vollzug der Unterbringung, zur Abwehr von Gefahren für die Sicherheit oder das geordnete Zusammenleben oder zur Verhinderung weiterer rechtswidriger Taten erforderlich, darf die Einrichtung

1. Daten über Verwandte, über Personen aus dem beruflichen und sozialen Umfeld der untergebrachten Person sowie über Geschädigte,

2. Namen und Anschriften von Besuchenden, einschließlich eventueller Erkenntnisse über Verwandtschafts- oder Beziehungsverhältnisse zur untergebrachten Person

verarbeiten. Die über die Daten für eine Kontaktaufnahme hinausgehenden personenbezogenen Daten sind bei den betroffenen Personen zu erheben. Die nach diesem Absatz erhobenen Daten sind in einem gesonderten Teil der Behandlungsakte zu führen.“

c) Der bisherige Absatz 2 wird Absatz 3 und wie folgt geändert:

aa) Satz 1 erhält folgende Fassung:

„Die Leiterin oder der Leiter der Einrichtung oder die stellvertretende Leiterin oder der stellvertretende Leiter der Einrichtung hat der von der Datenverarbeitung nach den Absätzen 1 und 2 betroffenen Person auf Antrag das Auskunftsrecht zu gewähren.“

bb) In Satz 3 werden nach dem Wort „Soweit“ die Wörter „und solange“ eingefügt.

5. § 33 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 33 Optisch-elektronische Beobachtung und Verarbeitung von Bildaufzeichnungen“.

b) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 einleitender Satzteil werden nach dem Wort „zur“ die Wörter „optisch-elektronischen Beobachtung und die“ eingefügt.

bb) In Satz 2 Halbsatz 1 wird das Wort „Aufzeichnungen“ durch das Wort „Bildaufzeichnungen“ ersetzt und werden nach dem Wort „löschen“ die Wörter „oder zu vernichten“ eingefügt.

cc) In Satz 3 werden die Wörter „und Nutzung“ gestrichen.

c) In Absatz 2 Satz 2 Halbsatz 1 wird das Wort „Aufzeichnungen“ durch das Wort „Bildaufzeichnungen“ ersetzt.

d) In Absatz 4 wird nach den Wörtern „Mittel zur“ das Wort „optisch-elektronischen“ eingefügt und werden die Wörter „zur Anfertigung“ durch die Wörter „die Anfertigung“ ersetzt.

6. § 34 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 34
Datenverwendung“.

b) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 einleitender Satzteil wird das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.

bb) In Satz 3 wird das Wort „Nutzung“ durch das Wort „Verwendung“ ersetzt.

c) Absatz 2 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „gespeicherte“ gestrichen, das Wort „einsehen“ wird durch das Wort „verwenden“ und das Wort „mitteilen“ durch das Wort „bereitstellen“ ersetzt.

bb) In Satz 2 wird das Wort „eingesehen“ durch die Wörter „verwendet und anderen Beschäftigten der Einrichtung bereitgestellt“ ersetzt.

7. § 35 Abs. 1 Satz 1 wird wie folgt geändert:

a) Im einleitenden Satzteil werden die Wörter „erhoben und“ gestrichen.
b) In Nummer 11 wird das Wort „oder“ durch ein Komma ersetzt.
c) In Nummer 12 wird der Punkt durch das Wort „oder“ ersetzt.
d) Nach Nummer 12 wird folgend Nummer 13 angefügt:

„13. zur Unterrichtung des Landeskriminalamtes über Beginn, Unterbrechung und Beendigung des Maßregelvollzugs.“

8. § 36 erhält folgende Fassung:

„§ 36
Datenübermittlung zu archivarischen, wissenschaftlichen und statistischen Zwecken

Für die Übermittlung von Daten, die zu archivarischen, wissenschaftlichen und statistischen Zwecken verarbeitet werden sollen, gilt § 6 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt.“

9. § 37 wird wie folgt geändert:

a) In Satz 1 wird das Wort „gespeicherten“ durch das Wort „vorhandenen“ ersetzt und werden nach dem Wort „löschen“ die Wörter „oder zu vernichten“ angefügt.

b) Satz 2 wird aufgehoben.

10. § 38 einziger Satz erhält folgende Fassung:

„Für die Verarbeitung von personenbezogenen Daten zum Zwecke des Maßregelvollzugs gilt im Übrigen das Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt.“

Artikel 5
Änderung des Gesetzes zur Ausführung des Therapieunterbringungsgesetzes in Sachsen-Anhalt

§ 2 des Gesetzes zur Ausführung des Therapieunterbringungsgesetzes in Sachsen-Anhalt vom 15. Juli 2011 (GVBl. LSA S. 620), zuletzt geändert durch Artikel 8 des Gesetzes vom 5. Dezember 2014 (GVBl. LSA S. 512, 514), wird wie folgt geändert:

1. Nach der Angabe „(GVBl. LSA S. 510)“ werden die Wörter „in der jeweils geltenden Fassung“ eingefügt.

2. Nach der Angabe „(BGBl. I S. 2300, 2305)“ werden die Wörter „, zuletzt geändert durch Artikel 8 des Gesetzes vom 5. Dezember 2012 (BGBl. I S. 2425, 2430), in der jeweils geltenden Fassung“ eingefügt.

Artikel 6
Einschränkung von Grundrechten

Durch die Artikel 3 und 4 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.

Artikel 7
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

Allgemeiner Teil

Im Mai 2018 hat das bisher rein national geregelte Datenschutzrecht in der Bundesrepublik Deutschland und in den Ländern seinen größten Umbruch erlebt.

Nach Abschluss der Beratungen auf europäischer Ebene trat am 24. Mai 2016 die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) in Kraft. Die Datenschutz-Grundverordnung ist seit dem 25. Mai 2018 in allen 27 Mitgliedstaaten der EU unmittelbar geltendes europäisches Datenschutzrecht.

Soweit die Verarbeitung personenbezogener Daten durch Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zum Zwecke der Strafvollstreckung erfolgt, tritt die Datenschutz-Grundverordnung nach ihrem Artikel 2 Absatz 2 Buchstabe d hinter die Richtlinie (EU) 2016/680 vom 27. April 2016, die häufig auch als JI-Richtlinie bezeichnet wird, zurück. Als Abgrenzungskriterium zwischen den beiden Rechtsakten der Europäischen Union lässt sich also gerade nicht die Behördenzuständigkeit heranziehen, sondern die Abgrenzung erfolgt aufgabenbezogen. Insoweit wird also auch die kommunale Ebene, die mit ihrer Verwaltungstätigkeit grundsätzlich der unmittelbar geltenden Datenschutz-Grundverordnung unterfällt, jedenfalls dann die Richtlinie zu beachten haben, soweit die kommunalen Behörden im Bereich der Verfolgung von Ordnungswidrigkeiten tätig werden und diese Tätigkeiten nicht unmittelbar in den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) fallen. Die innerhalb der EU außer in Deutschland nur noch in Österreich bekannten Ordnungswidrigkeiten sind aus dem europäischen Blickwinkel betrachtet unter dem Begriff der Straftaten zu subsumieren.

Die Richtlinie (EU) 2016/680 trat am 5. Mai 2016 in Kraft. Sie war zum 6. Mai 2018 umzusetzen.

Während die Datenschutz-Grundverordnung als EU-Verordnung mit ihrer Geltung ab dem 25. Mai 2018 unmittelbar geltendes Datenschutzrecht in ganz Europa wurde, bedarf die Richtlinie jeweils der nationalen gesetzgeberischen Umsetzung in den Mitgliedstaaten. Insbesondere in den Bereich der Datenverarbeitung von Polizei und Justiz ist die Umsetzung durch ein Landesgesetz geboten, um das bislang auch für diesen Bereich geltende Datenschutzgesetz Sachsen-Anhalt (DSG LSA) europarechtskonform abzulösen.

Dazu bietet sich die überwiegend wörtliche Übernahme der in Teil 3 „Bestimmungen für die Verarbeitung zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680“ in Artikel 1 des Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097) enthaltenen Regelungen an. Dies entspricht §§ 45 ff. des am 25. Mai 2018 in Kraft getretenen „neuen“ BDSG.

Diese wörtliche Übernahme der Regelungen dient der Rechtssicherheit und Rechtseinheitlichkeit. Sie bietet den Vorteil, dass damit eine einheitliche Behandlung von Datenschutzfragen auf der Ebene der Strafverfolgungsbehörden (insbesondere der Staatsanwaltschaften und der ihr zuarbeitenden Polizeibehörden), die die Strafpro-

zessordnung (StPO) anzuwenden haben, und der Ebene der Polizeibehörden, die auch im Bereich der nur landesrechtlich geregelten Gefahrenabwehr zur Verhütung von Straftaten tätig werden, gewährleistet werden kann. Diese Verschränkung der beiden Strafverfolgungsbehörden wird insbesondere in § 483 der StPO deutlich. In § 483 Absatz 3 StPO ist geregelt, dass die Datenverarbeitung der Strafverfolgungsbehörden der Länder für Zwecke künftiger Strafverfahren dem Landesdatenschutzrecht unterliegt. In § 484 Absatz 4 StPO ist geregelt, dass die Datenverarbeitung der Polizei zum Zweck der Strafverfolgungsvorsorge sich nach dem Landesrecht richtet. Insofern bedarf eine Umsetzung der Richtlinie (EU) 2016/680 zwingend auch einer Anpassung des Datenschutzrechts im Bereich der Landespolizei. Mit dem vorliegenden Gesetzentwurf soll auf der Ebene der Bundespolizeibehörden und der Landespolizeibehörden ein einheitliches Querschnittsdatenschutzrecht umgesetzt werden.

Im Bereich des Justizvollzuges (insbesondere Untersuchungshaft, Strafhaft, Jugendstrafhaft, Sicherungsverwahrung und Jugendarrest) erfolgt die Umsetzung der Richtlinie (EU) 2016/680 auf der Grundlage eines bereits erarbeiteten Musterentwurfs für ein Justizvollzugsdatenschutzgesetz. In Umsetzung dieses Musterentwurfs sollen die bundeseinheitlichen Vorgaben auf Landesebene durch ein Justizvollzugsdatenschutzgesetz Sachsen-Anhalt umgesetzt werden. Ausgangsbasis auch für diesen Entwurf ist Teil 3 des neuen BDSG. Insoweit bleibt dieser Bereich mit dem vorliegenden Gesetzentwurf ausgeklammert.
Im Gegensatz zu dieser Verfahrensweise werden die notwendigen europarechtlich bedingten Änderungen beim Datenschutz im Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt, im Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt, im Maßregelvollzugsgesetz des Landes Sachsen-Anhalt sowie im Gesetz zur Ausführung des Therapieunterbringungsgesetzes in Sachsen-Anhalt jeweils in einem besonderen Artikel mit geregelt.

Das Gesetz dient im Wesentlichen der Umsetzung der Richtlinie (EU) 2016/680. Das Gesetz gilt nur für Verarbeitungen durch öffentliche Stellen und nach Artikel 3 Nr. 7 Buchstabe b der Richtlinie (EU) 2016/680 insoweit, als öffentliche Stellen geltende Beliehene, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind und auch nur, soweit sie zu diesen Zwecken Daten verarbeiten. Dies sind insbesondere die Polizeibehörden und die Staatsanwaltschaften des Landes, soweit sie die Daten zu den genannten Zwecken verarbeiten.

Zu den Vorschriften im Einzelnen:

Artikel 1 Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt - DSUG LSA)

Zu § 1 (Anwendungsbereich)

Für die Eröffnung des Anwendungsbereichs der Richtlinie (EU) 2016/680 genügt also eine Verarbeitung zu den o. g. Zwecken allein nicht; daneben muss auch eine grundsätzliche Befugnis- und Aufgabenzuweisung (Zuständigkeit) für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, ein-

schließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit vorliegen.

Die Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten ist vom Anwendungsbereich umfasst; dies wird durch Erwägungsgrund 13 der Richtlinie (EU) 2016/680 unterstützt. Hierdurch wird insbesondere erreicht, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Ordnungswidrigkeit in Rede steht. Aus dem Ziel, im Ordnungswidrigkeitenverfahren für alle Behörden einheitliche datenschutzrechtliche Regeln zu schaffen, folgt, dass auch diejenigen Behörden, die zwar Polizeibehörden sind, aber Ordnungswidrigkeiten verfolgen, ahnden und vollstrecken, das vorliegende Gesetz jedenfalls dann anzuwenden haben, wenn Teil 3 des BDSG keine unmittelbare Anwendung findet. Durch dieses Gesetz folgt die Datenverarbeitung in Ordnungswidrigkeitenverfahren immer denjenigen Regeln, welche die Richtlinie (EU) 2016/680 umsetzen.

Aus der Beschränkung auf Ordnungswidrigkeiten ergibt sich, dass die Datenverarbeitung bei Verwaltungsbehörden wie z. B. Waffen-, Gesundheits- oder Passbehörden, die Aufgaben der Gefahrenabwehr wahrnehmen, grundsätzlich solange und soweit nicht in den Anwendungsbereich der Richtlinie und damit unter dieses Gesetz fällt, wie die von ihnen geführten Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergehen. Bauaufsichtsbehörden, die also zur Gefahrenabwehr eine Abrissverfügung gegenüber dem Grundstückseigentümer erlassen, haben die Datenschutz-Grundverordnung anzuwenden und müssen erst dann dieses Gesetz beachten, wenn sie ein Ordnungswidrigkeitenverfahren einleiten.

Auftragsverarbeiter - ob öffentliche oder nichtöffentliche Stellen -, deren Tätigkeit sich grundsätzlich dadurch auszeichnet, dass sie Daten zur Erfüllung einer Auftragsverarbeitungsvereinbarung und nicht aufgrund eigener Aufgabenzuschreibung verarbeiten, sind für dieses Gesetz nur dann Adressaten, sofern sie konkret angesprochen sind. Die von ihnen durchgeführten Verarbeitungen richten sich im Übrigen nach den Regelungen der Datenschutz-Grundverordnung. Das schließt nicht aus, dass durch dieses Gesetz angesprochene Verantwortliche auch als Auftragsverarbeiter tätig sein können.

Zu § 2 (Begriffsbestimmungen)

Die Begriffsbestimmungen in den Nrn. 1 bis 22 sind zum Zweck der Umsetzung der Richtlinie (EU) 2016/680 aufgenommen worden. Sie schließen an die Begriffsbestimmungen in Artikel 3 der Richtlinie (EU) 2016/680 an. Zum Zweck der Übersichtlichkeit wurde die in Artikel 10 der Richtlinie (EU) 2016/680 enthaltene Definition besonderer personenbezogener Daten als Nr. 18 ergänzend aufgenommen. Zudem wurde die in § 7 angesprochene Einwilligung und der Begriff des Dritten unter Übernahme der Definitionen aus der Verordnung (EU) 2016/679 in Nrn. 13 und 22 aufgenommen.

Aus dem DSG LSA wurden die Begriffsdefinitionen für die Anonymisierung (Nummer 5) und die Verschlüsselung (Nummer 7) übernommen. Der Begriff der Akte in Nr. 9 wurde aus dem bisher in § 2 Absatz 3 DSG LSA definierten Aktenbegriff entwickelt. Da in der Praxis auch ganz oder überwiegend elektronisch geführte Akten, etwa die Kriminalakte nach dem SOG LSA oder die Behandlungsakte nach dem Maß-

regelvollzugsgesetz Sachsen-Anhalt (MVollzG LSA), vom Gesetzgeber als „Akte“ und eben nicht als „Dateisystem“ bezeichnet werden, wird aus Gründen der Rechtssicherheit klargestellt, dass Akten auch Dateisysteme im Sinne der Nr. 8 sein können, und zwar unabhängig davon, ob diese elektronisch oder in Papierform geführt werden. Dabei schließt die Definition Mischformen von elektronischen und papiergebundenen Akten (Hybridakten) nicht aus und bleibt damit zukunftssicher. In den nächsten Jahren ist zu erwarten, dass Akten in noch stärkerem Umfang elektronisch geführt werden und damit in immer größerer Zahl als „Dateisystem“ unmittelbar den europäischen Vorschriften unterfallen. Neben den Akten, die Dateisystemen entsprechen, umfasst der Aktenbegriff nach Nr. 9, wie bisher, auch alle weiteren amtlichen oder dienstlichen Zwecken dienenden Unterlagen einschließlich analoger Bild- und Tonträger, die nicht die Kriterien nach Nr. 8 erfüllen. Die Beibehaltung dieses aus § 2 Absatz 3 DSG LSA übernommenen Kataloges ist bereits deswegen geboten, weil bis heute zahlreiche Verwaltungsverfahren papiergebunden und noch nicht elektronisch durchgeführt werden. So entstehen neben Papierakten und analogen Bild- und Tonträgern , die auf Grund von Fristregelungen, aus dienstlicher Notwendigkeit oder zu wissenschaftlichen oder archivarischen Zwecken aufbewahrt werden auch heute noch neue papiergebundene Unterlagen und analoge Bild- und Tonträger, etwa in Bereichen, in denen die elektronische Akte noch nicht eingeführt worden ist oder in denen alte analoge Videoüberwachungssysteme mit Bandaufzeichnungsverfahren eingesetzt werden. Da die Erwägungsgründe der Richtlinie (EU) 2016/680, anders als diejenigen der Datenschutz-Grundverordnung, nicht unmittelbar gelten, wird mit der Regelung der Ansatz der Technologieneutralität aus Erwägungsgrund 18, Satz 1, sowie der negativ definierte Aktenbegriff aus Erwägungsgrund 18, Satz 3, der Richtlinie (EU) 2016/680, außerdem in rechtssicherer Art und Weise regelungsidentisch mit Erwägungsgrund 15 der Datenschutz-Grundverordnung in das sachsen-anhaltische Landesrecht überführt.

Zu § 3 (Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten)

§ 3 dient der Umsetzung von Artikel 4 Absatz 1 der Richtlinie (EU) 2016/680 und führt einige allgemeine Verarbeitungsgrundsätze, die in Teilen an späterer Stelle noch einmal aufgenommen werden, an zentraler Stelle zusammen.

Zu § 4 (Verarbeitung besonderer Kategorien personenbezogener Daten)

§ 4 dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680. Absatz 1 legt fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. Die Vorschrift schafft damit eine eigene Rechtsgrundlage für diese Verarbeitungen. Das kann auch die Verarbeitung in den in Artikel 10 Buchstabe b und c genannten Zusammenhängen, d. h. zur Wahrung lebenswichtiger Interessen der betroffenen Person oder eines Dritten oder wenn Daten verarbeitet werden sollen, die die betroffene Person offensichtlich öffentlich gemacht hat, umfassen. In Absatz 2 wird in Satz 1 klargestellt, dass bei der Verarbeitung geeignete Garantien für die Rechtsgüter der betroffenen Personen beachtet werden müssen. In Satz 2 werden Aussagen zu möglichen Maßnahmen zur Umsetzung dieser Vorgabe getroffen. Die Aufzählung gibt unverbindliche Beispielsfälle wieder, wie geeignete Garantien aussehen können. Die konkrete Ausgestaltung der Maßnahmen kann also von Einzelfall zu Einzelfall variieren.

Zu § 5 (Verarbeitung zu anderen Zwecken)

Satz 1 setzt Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 um. Somit wird klargestellt, dass Verantwortliche Daten so lange und so weit zu anderen Zwecken, als zu denen sie ursprünglich erhoben wurden, verarbeiten dürfen, so lange es sich bei diesen anderen Zwecken um einen der in § 1 genannten Zwecke handelt und diese Verarbeitung erforderlich und verhältnismäßig ist. Grundsätzlich eröffnet Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 stets die Möglichkeit, die Daten für einen der in § 1 genannten Zwecke zu verarbeiten und innerhalb der Palette der genannten Zwecke auch Zweckänderungen vorzunehmen, wobei der EU-Gesetzgeber offen lässt, ob in diesen Fällen überhaupt eine Zweckänderung vorliegt.

Satz 2 betrifft die Weiterverarbeitung von zu Zwecken des § 1 erhobenen Daten zu anderen als in § 1 genannten Zwecken. Eine solche ist zulässig, wenn dies in einer Rechtsvorschrift vorgesehen ist.

Zu § 6 (Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken)

§ 6 greift Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 auf, wonach Verantwortliche Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken verarbeiten dürfen, solange diese Verarbeitung unter die in § 1 genannten Zwecke gefasst werden kann. Als Beispiel kann hier die kriminologische oder kriminaltechnische Forschung angeführt werden. Voraussetzung hierfür ist das Vorliegen geeigneter Vorkehrungen zugunsten der Rechtsgüter der betroffenen Person; hierzu können insbesondere die gemessen am konkreten Forschungszweck so zeitnah wie möglich erfolgende Anonymisierung von Daten oder die räumliche und organisatorische Abtrennung der Forschung betreibenden Stellen gehören. Diese Vorkehrungen werden im einschlägigen Fachrecht weiter ausdifferenziert.

Zu § 7 (Einwilligung)

In § 7 finden sich die Voraussetzungen für eine wirksame Einwilligung.

Absatz 1 entspricht inhaltlich Artikel 7 Absatz 1, Absatz 2 entspricht Artikel 7 Absatz 2 und Absatz 3 entspricht Artikel 7 Absatz 3 der Verordnung (EU) 2016/679. In Absatz 4 wurde der Ansatz aus § 4a Absatz 1 BDSG a. F. mit dem Gedanken aus Artikel 7 Absatz 4 der Verordnung (EU) 2016/679 angereichert, wonach für die Beurteilung der Frage, ob die Freiwilligkeit der Einwilligung vorliegt, wesentlich auf die Umstände der Erteilung abzustellen ist. Die Richtlinie (EU) 2016/680 nennt in Erwägungsgrund 35 beispielhaft Einwilligungen im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung des Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung.

Zu § 8 (Verarbeitung auf Weisung des Verantwortlichen)

§ 8 setzt Artikel 23 der Richtlinie (EU) 2016/680 um.

Zu § 9 (Datengeheimnis)

§ 9 greift die Regelung des § 5 BDSG a. F. und § 5 DSG LSA zum Datengeheimnis auf.

Zu § 10 (Automatisierte Einzelentscheidung)

§ 10 setzt Artikel 11 der Richtlinie (EU) 2016/680 um und regelt das Verbot automatisierter, insbesondere auf Profiling basierender Einzelentscheidungen. Um eine in Absatz 1 genannte, nur unter bestimmten Umständen zulässige, „Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat“, zu sein, muss es sich bei einer solchen Entscheidung um einen Rechtsakt mit Außenwirkung gegenüber der betroffenen Person - regelmäßig einen Verwaltungsakt - handeln. Interne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter.

Zu § 11 (Allgemeine Informationen zu Datenverarbeitungen)

§ 11 dient der Umsetzung von Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680. Die Vorschrift regelt die aktiven Informationspflichten des Verantwortlichen gegenüber betroffenen Personen unabhängig von der Geltendmachung von Betroffenenrechten. Dieser Informationspflicht sollen Verantwortliche in allgemeiner Form nachkommen können. Durch die explizit in Erwägungsgrund 42 der Richtlinie (EU) 2016/680 aufgenommene Möglichkeit der Information über die Internetseite des Verantwortlichen wird im Zusammenhang der Sinn und Zweck der Regelung klargestellt: Betroffene Personen sollen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der beim Verantwortlichen durchgeführten Verarbeitungen verschaffen können und eine Übersicht über die ihnen zu Gebote stehenden Betroffenenrechte bekommen.

Zu § 12 (Benachrichtigung betroffener Personen)

§ 12 betrifft Fälle, in denen in fachgesetzlichen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Eine Festlegung dieser in Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 bezeichneten „besonderen Fälle“ ist nicht verallgemeinernd auf Ebene dieses Gesetzes möglich und muss somit im Fachrecht geleistet werden. Leitend für die Entscheidung, ob eine Benachrichtigung unabhängig von der Geltendmachung eines Betroffenenrechts angezeigt ist, dürfte z. B. sein, ob die Verarbeitung mit oder ohne Wissen der betroffenen Person, ggf. in Verbindung mit einer erhöhten Eingriffstiefe, stattfindet. In letztgenannten Fällen gibt eine aktive, ggf. nachträgliche Benachrichtigung der betroffenen Person die einzige Möglichkeit, von der Verarbeitung Kenntnis zu erlangen und ggf. deren Rechtmäßigkeit mithilfe der Geltendmachung von Betroffenenrechten zu prüfen.

Absatz 1 stellt klar, welche Informationen der betroffenen Person von dem Verantwortlichen in diesen Fällen aktiv übermittelt werden müssen und dient dabei der Umsetzung von Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680.

Absatz 2 ermöglicht es, in Umsetzung von Artikel 13 Absatz 3 der Richtlinie (EU) 2016/680, zu den dort genannten Zwecken von der Bereitstellung der in Ab-

satz 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 angesprochenen Beeinträchtigung - der genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll.

Absatz 3 statuiert ein Zustimmungserfordernis der dort genannten Stellen, wenn sich die Benachrichtigung auf die Übermittlung an diese Stellen (nach Absatz 1 Satz 1 Nr. 4) bezieht. Insofern besteht ein der Situation der aktiven Geltendmachung von Betroffenenrechten vergleichbarer Sachverhalt, weshalb die Übernahme geboten ist. Die Nutzung der Möglichkeit, von der Bereitstellung der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder aufzuschieben, muss Verhältnismäßigkeitsgrundsätzen genügen, mithin in ein angemessenes Verhältnis zur Bedeutung der Betroffeneninformation für die spätere Geltendmachung von Betroffenenrechten gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Bereitstellung etwa nur teil- oder zeitweise eingeschränkt werden kann („solange und soweit“).

Zu § 13 (Auskunftsrecht)

§ 13 thematisiert das Auskunftsrecht als zentrales Betroffenenrecht und normiert gleichzeitig dessen Einschränkungen. Die Vorschrift dient mithin der Umsetzung der Artikel 14 (Bestehen des Auskunftsrechts) und 15 (Ausnahmen) der Richtlinie (EU) 2016/680. Das Auskunftsrecht setzt - im Gegensatz zu in § 12 angesprochenen aktiven Benachrichtigungspflichten - einen entsprechenden Antrag der betroffenen Person voraus. Die Regelung entspricht im Wesentlichen dem Regelungsansatz im bisherigen § 15 DSG LSA.

Absatz 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Der in den Nrn. 1 und 4 genannte Begriff „Kategorie“ ermöglicht dem Verantwortlichen eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten sowie zu den Übermittlungsempfängern. Die Angaben nach Nr. 1 zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, welche Aufschluss über die Art und Weise der Speicherung oder Sichtbarkeit der Daten beim Verantwortlichen (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Der Verantwortliche muss sich bei der Angabe zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über Umfang und Art der verarbeiteten Daten zu erzeugen und es ihr zu ermöglichen, aufgrund dieser Informationen zu ermessen, ob die Verarbeitung rechtmäßig ist und - wenn Zweifel hieran bestehen - ggf. die Geltendmachung weitere Betroffenenrechte auf diese Informationen stützen zu können.

Absatz 2 überführt den Rechtsgedanken des § 19 Absatz 2 BDSG a. F. in das DSUG LSA. Die Regelung entspricht der bisherigen Regelung im § 15 Absatz 2 DSG LSA.

Absatz 3 überführt die Regelung des § 19 Absatz 1 Satz 3 BDSG a. F in das DSUG LSA. Die Regelung betrifft insbesondere die Auskunftserteilung aus papiergebundenen Akten. Auf Grund der Struktur dieser Akten sind dort personenbezogene Daten häufig nur durch das zeitintensive Studium der gesamten Akte auffindbar. Der Regelungsansatz entspricht demjenigen im bisherigen § 15 Absatz 1 Satz 3 DSG LSA.

Absatz 4 normiert, zu welchen Zwecken das Auskunftsrecht durch den Verantwortlichen vollständig oder teilweise eingeschränkt werden darf. 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 angesprochenen Beeinträchtigung - der genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Auskunftserteilung vollständig oder teilweise abzusehen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Auskunftserteilung geschützten Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Auskunftserteilung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Auskunft etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.

Absatz 5 nimmt § 19 Absatz 3 BDSG a. F. auf. Sie entspricht der bisherigen Regelung in § 15 Absatz 3 Satz 1 DSG LSA.

Absatz 6 Satz 1 und 2 dient der Umsetzung von Artikel 15 Absatz 3 Satz 1 und 2 der Richtlinie (EU) 2016/680. Hierdurch wird dem Verantwortlichen - auch gemeinsam mit der sich aus Absatz 4 ergebenden Variante, die Frage nach dem „Ob“ der Verarbeitung nicht zu beantworten, die Möglichkeit gegeben, das Auskunftsverlangen unbeantwortet zu lassen („neither confirm nor deny“). Satz 3 nimmt in Bezug auf das Absehen von einer Begründung der Auskunftsverweigerung zusätzlich einen aus § 19 Absatz 5 Satz 1 BDSG a. F. entnommenen Gedanken auf. Dies entspricht der bisher in § 15 Absatz 5 Satz 1 DSG LSA geregelten Einschränkung.

Absatz 7 thematisiert die Möglichkeiten, die der betroffenen Person im Fall des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Fall der überhaupt ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Sie entspricht dem bisher § 15 Absatz 6 DSG LSA tragenden Regelungsgedanken. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über den Landesbeauftragten für den Datenschutz ausüben. Dies dient der Umsetzung von Artikel 17 Absatz 1 der Richtlinie (EU) 2016/680. Satz 2 sieht in Umsetzung von Artikel 17 Absatz 2 der Richtlinie (EU) 2016/680 eine entsprechende Unterrichtung durch den Verantwortlichen vor, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Absatz 6 berechtigt ist, von einer Information des Antragstellers ganz abzusehen. Satz 3 nimmt § 19 Absatz 6 Satz 1 BDSG a. F. auf. Satz 4 und 5 betreffen den Inhalt der betroffenen Person seitens des Landesbeauftragten für den Datenschutz zur Verfügung gestellten Informationen im Ergebnis der dort durchgeführten Prüfung; hier wird Artikel 17 Absatz 3 Satz 1 der Richtlinie (EU) 2016/680 umgesetzt und zur Stärkung der Betroffenenrechte in Satz 5 über das von der Richtlinie Gefor-

derte hinausgegangen, indem die Mitteilung die Information enthalten darf, ob datenschutzrechtliche Verstöße festgestellt wurden, mithin die Auskunftsverweigerung oder teilweise Einschränkung der Auskunft rechtmäßig war. Satz 6 und 7 nimmt § 19 Absatz 6 Satz 2 BDSG a. F. auf. Satz 8 setzt Artikel 17 Absatz 3 Satz 2 der Richtlinie (EU) 2016/680 um.

Absatz 8 setzt Artikel 15 Absatz 4 der Richtlinie (EU) 2016/680 um.

Zu § 14 (Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung)

In § 14 werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen zusammengeführt. § 14 dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Betroffenenrecht.

Absatz 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Hier wird Artikel 16 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt. In Satz 2 wird ein in Erwägungsgrund 47 der Richtlinie (EU) 2016/680 enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf die betroffene Person betreffende Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen; Gleiches gilt etwa für polizeifachliche Bewertungen. In Satz 3 wird Artikel 16 Absatz 3 Satz 1 Buchstabe a der Richtlinie (EU) 2016/680 umgesetzt. Zwar sieht der Richtlinientext im beschriebenen Fall die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird der in der Richtlinie beschriebene Sachverhalt systematisch korrekt in Absatz 1 verortet, indem für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung tritt. Für das Bestreiten der Richtigkeit der beim Verantwortlichen verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus; vielmehr müssen die Zweifel an der Unrichtigkeit durch Beibringung geeigneter Tatsachen substantiiert werden. Dies dient dem Schutz der polizeifachlichen Arbeit und der Vermeidung unverhältnismäßigen Prüfaufwands.

Absatz 2 statuiert das Betroffenenrecht auf Löschung und dient der Umsetzung von Artikel 16 Absatz 2 der Richtlinie (EU) 2016/680, in dem sowohl die unabhängig von der Geltendmachung des Betroffenenrechts durch die betroffene Person bestehende Löschungspflicht des Verantwortlichen als auch das entsprechende Betroffenenrecht angesprochen sind.

Absatz 3 betrifft die Voraussetzungen, unter denen an die Stelle einer Löschung nach Absatz 2 eine Verarbeitungseinschränkung treten kann. Es werden Elemente aus Artikel 16 Absatz 3 Satz 1 Buchstabe b der Richtlinie (EU) 2016/680 (Absatz 3 Satz 1 Nr. 2) aufgenommen. Absatz 3 Satz 1 Nr. 1 übernimmt zudem einen in Erwägungsgrund 47 Satz 4 der Richtlinie (EU) 2016/680 enthaltenen Gedanken. Die Möglichkeit, von der Löschung wegen unverhältnismäßigen Aufwands abzusehen, ist als restriktiv auszulegende Ausnahmeregelung anzusehen. Im Grundsatz sollte die bei Verantwortlichen zum Einsatz kommende IT-Infrastruktur darauf ausgelegt sein, eine

Löschungsverpflichtung auch technisch nachvollziehen zu können. Satz 2 behandelt die Verarbeitung von in ihrer Verarbeitung nach Satz 1 eingeschränkten Daten.

Absatz 4 entspricht der bisherigen Regelung zum „Sperren“ von Daten in § 16 Absatz 2 Satz 2 DSG LSA. Sie stellt auf den Aktenbegriff nach § 2 Nr. 9 ab und bezieht sich dabei in erster Linie auf Datenträger aus der analogen Welt, wie etwa die papiergebundene Akte, Videobänder usw.

Absatz 5 fordert, dass die Verarbeitungseinschränkung im Kontext automatisierter Verarbeitung erkennbar sein muss.

Die in Absatz 6 enthaltene Verpflichtung zur Meldung der Berichtigung an Stellen, von denen die unrichtigen Daten stammen, setzt Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680 um.

Absatz 7 dient der Umsetzung von Artikel 16 Absatz 4 der Richtlinie (EU) 2016/680 und betrifft das zur Anwendung kommende Verfahren, wenn der Verantwortliche einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt.

Zu § 15 (Verfahren für die Ausübung der Rechte der betroffenen Person)

In § 15 werden Elemente des Artikels 12 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 1 setzt Artikel 12 Absatz 1, Absatz 2 setzt Artikel 12 Absatz 3, Absatz 3 setzt Artikel 12 Absatz 4 und Absatz 4 setzt Artikel 12 Absatz 5 der Richtlinie (EU) 2016/680 um.

Wenngleich es Absatz 5 der Richtlinie (EU) 2016/680 dem Verantwortlichen in begründeten Zweifelsfällen ermöglicht, zusätzliche Informationen zur Identitätsklärung anzufordern, ist hierdurch keine Änderung der bisherigen verbreiteten Praxis angezeigt, den Nachweis der Identität auch weiterhin als Grundvoraussetzung für die Antragsstellung anzusehen.

Zu § 16 (Anrufung des Landesbeauftragten für den Datenschutz)

§ 16 stellt auch für den Bereich der Verarbeitung durch Verantwortliche zu den in § 1 genannten Zwecken klar, dass sich Jedermann mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung personenbezogener Daten an den Landesbeauftragten für den Datenschutz wenden kann. Mit Absatz 1 dieser Vorschrift werden gleichzeitig Artikel 52 der Richtlinie (EU) 2016/680 umgesetzt als auch § 19 DSG LSA in die Neuregelung überführt. Absatz 2 entspricht der bisherigen Regelung in § 19 Satz 2 DSG LSA.

Zu § 17 (Verfahren bei Beschwerden, die in die Zuständigkeit einer anderen Aufsichtsbehörde eines EU-Mitgliedstaats fallen)

§ 17 setzt Artikel 52 Absatz 2 der Richtlinie (EU) 2016/680 um.

Zu § 18 (Auftragsverarbeitung)

§ 18 dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680 und stellt Anforderungen auf, wenn der Verantwortliche Auftragsverarbeitungsverhältnisse eingehen will. Am bisherigen Regelungsansatz, wonach der Verantwortliche für die Datenübermittlung an den Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, ändert sich durch die Richtlinienumsetzung 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 jeder Auftragsverarbeitung die Kontrolle durch den Landesbeauftragten für den Datenschutz sichergestellt werden muss. Dies hat ggf. durch vertragliche Festlegung zu erfolgen.

Absatz 2 beschreibt an den Auftragsverarbeiter zu stellende Anforderungen und setzt Artikel 22 Absatz 1 der Richtlinie (EU) 2016/680 um.

In Absatz 3 werden Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen normiert und dadurch Artikel 22 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt.

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

In Absatz 5 werden die erforderlichen Inhalte einer der Auftragsverarbeitung 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 Nr. 1 Elemente aus Artikel 28 Absatz 3 Buchstabe a der Verordnung (EU) 2016/679, in Nr. 5 Elemente aus Artikel 28 Absatz 3 Buchstabe h, in Nr. 7 Elemente aus Artikel 28 Absatz 3 Buchstabe c und in Nr. 8 Elemente aus Artikel 28 Absatz 3 Buchstabe f der Verordnung (EU) 2016/679 aufgenommen.

Absatz 6 trifft in Umsetzung von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680 Aussagen zur Form der Vereinbarung.

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

Absatz 8 überführt die bisher in § 7 Absatz 2 Satz 2 und § 8 Absatz 2 Satz 2 DSG LSA geregelten Festlegungen zum Tätigwerden von Fachaufsichtsbehörden in das neue Recht.

Zu § 19 (Gemeinsam Verantwortliche)

§ 19 dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2016/680.

Zu § 20 (Anforderungen an die Sicherheit der Datenverarbeitung)

§ 20 dient der Umsetzung von Artikel 29 der Richtlinie (EU) 2016/680. Er verpflichtet den Verantwortlichen dazu, erforderliche technisch-organisatorische Maßnahmen zu treffen. Gleichzeitig wird klargestellt, dass die Ausgestaltung der Maßnahmen Ergeb-

nis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die entstehenden Kosten, die näheren Umstände der Verarbeitung und die in Aussicht zu nehmende Gefährdung für die Rechtsgüter der betroffenen Person einzustellen sind. Weiterhin wird klarstellend geregelt, dass bei der Festlegung der technisch-organisatorischen Maßnahmen die einschlägigen Standards und Empfehlungen, insbesondere Technische Richtlinien, des Bundesamts für Sicherheit in der Informationstechnik zu berücksichtigen sind.

Absatz 1 liegt der Gedanke zugrunde, wonach die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, aufgenommen.

In Absatz 2 werden Inhalte aus Artikel 32 Absatz 1 Buchstaben a bis c Verordnung (EU) 2016/679 übernommen.

Absatz 3 nimmt den tragenden Gedanken von § 6 DSG LSA auf und überführt ihn in die Neuregelung. Er benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen.

Zu § 21 (Meldung von Verletzungen des Schutzes personenbezogener Daten an den Landesbeauftragten für den Datenschutz)

§ 21 dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680 und legt den Umfang und die Modalitäten der Meldung von „Verletzungen des Schutzes personenbezogener Daten“ nach § 2 Nr. 12 an den Landesbeauftragten für den Datenschutz fest. Ansatzpunkt der Meldung sind, wie sich auch aus der systematischen Stellung der Vorschrift im Bereich Sicherheit der Verarbeitung ergibt, Vorfälle wie etwa Datenabflüsse.

Die in Absatz 5 geforderte Dokumentation muss in Qualität und Quantität so beschaffen sein, dass sie dem Landesbeauftragten für den Datenschutz die Überprüfung der Einhaltung der gesetzlichen Vorgaben ermöglicht.

In Absatz 7 wird geregelt, dass die Motivation zur Meldung einer Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung 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 § 22 (Benachrichtigung betroffener Personen bei Verletzung des Schutzes personenbezogener Daten)

§ 22 setzt Artikel 31 der Richtlinie (EU) 2016/680 um. In Absatz 6 wird der im § 21 Absatz 7 enthaltenen Gedanke aufgegriffen, wonach auch bei einer Benachrichtigung der betroffenen Person die Motivation zu dieser Benachrichtigung über eine

Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung eines Strafverfahrens führen können.

Zu § 23 (Durchführung einer Datenschutz-Folgenabschätzung)

§ 23 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680. Die Datenschutz-Folgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes. Die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung können nur unvollkommen gesetzlich konkret ausgestaltet werden. So lässt sich dennoch feststellen, dass hinsichtlich des Umfangs der Verarbeitung nicht eine Einzelverarbeitung, sondern lediglich die Verwendung maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten mithilfe einer Datenschutz-Folgenabschätzung vorab in den Blick genommen werden müssen. Insoweit lässt sich - abseits der prozeduralen Verbindung - eine Vergleichbarkeit mit den Voraussetzungen der Durchführung einer Anhörung des Landesbeauftragten für den Datenschutz begründen. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Risiken für die Rechtsgüter der betroffenen Person in sich birgt, können beispielsweise der Kreis der betroffenen Personen, die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein.

Die Konkretisierung der in Absatz 1 genannten Voraussetzungen obliegt letztlich der 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 Datenschutz-Folgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden gilt.

Absatz 2 nimmt Artikel 35 Absatz 1 Nr. 2, Absatz 3 Artikel 35 Absatz 2 der Verordnung (EU) 2016/679 auf. Absatz 4 legt den Inhalt der Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 enthaltenen allgemeinen Angaben unter Übernahme der Angaben aus Artikel 35 Absatz 7 der Verordnung (EU) 2016/679 enthaltenen Punkte. Absatz 5 nimmt Artikel 35 Absatz 11 der Verordnung (EU) 2016/679 auf.

Zu § 24 (Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz)

§ 24 setzt Artikel 26 der Richtlinie (EU) 2016/680 um. Die hier angesprochene Pflicht des Verantwortlichen zur Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz fasst die sich ohnehin aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperationsbeziehungen zwischen Verantwortlichem und dem Landesbeauftragten für den Datenschutz zusammen. Satz 2 übernimmt dabei den Regelungsansatz aus § 23 Absatz 1 Satz 2 DSG LSA, greift dabei allerdings zur Wahrung größtmöglicher Rechtseinheitlichkeit auf den Wortlaut der im BDSG in § 16 Absatz 4 neu gefassten Regelung zurück.

Zu § 25 (Anhörung des Landesbeauftragten für den Datenschutz)

§ 25 dient der Umsetzung von Artikel 28 der Richtlinie (EU) 2016/680. Die Vorkonsultation - hier als Anhörung bezeichnet - des Landesbeauftragten für den Datenschutz

dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen 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 Datenschutz-Folgenabschätzung aus der Datenschutz-Grundverordnung. Prozedural wird diese Verbindung dadurch hergestellt, dass nach Absatz 1 Nr. 1 eine Anhörung durchzuführen ist, wenn im Ergebnis einer Datenschutz-Folgenabschätzung eine erhöhte Gefährdung angenommen wird und der Verantwortliche 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.

Artikel 28 der Richtlinie (EU) 2016/680 knüpft an die Einleitung der Konsultation an, setzt aber nicht voraus, dass diese zwingend abgeschlossen sein muss, bevor personenbezogene Daten entsprechend verarbeitet werden. Zwar wird man im Regelfall den Abschluss der Konsultation im Interesse der betroffenen Person abwarten. Im Ausnahmefall können jedoch Abweichungen geboten sein. Die in Absatz 4 vorgesehene Eilfallregelung trägt solchen operativen und (polizei-)fachlichen Erfordernissen in Abweichung von Absatz 3 Satz 1 Rechnung. Die Nutzung der Eilfallregelung entbindet den Verantwortlichen gleichwohl nicht davon, die Empfehlungen des Landesbeauftragten für den Datenschutz nach pflichtgemäßem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen. Weiterhin schmälert die Eilfallregelung nicht die dem Landesbeauftragten für den Datenschutz zur Verfügung stehenden Befugnisse.

Zu § 26 (Verzeichnis von Verarbeitungstätigkeiten)

§ 26 dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680 und verpflichtet den Verantwortlichen, wie schon jetzt § 14 Absatz 3 DSG LSA, zur Führung eines Verzeichnisses über bei ihm durchgeführten Datenverarbeitungstätigkeiten. 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 die beim Verantwortlichen durchgeführten Datenverarbeitungen 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) Beauftragten für den Datenschutz und die Regelung zum umfassenden Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen.

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 Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht. Es kann sich anbieten, die nach Satz 1 Nr. 2 aufzunehmenden Angaben zu den Zwecken der Verarbeitung an den gesetzlichen Aufgabenzuschreibungen der betreffenden öffentlichen Stelle auszurichten. Satz 2 übernimmt die bisher in § 14 Absatz 4 Nr. 1 DSG LSA enthaltene Regelung.

Absatz 2 verpflichtet den Verantwortlichen, ein Verzeichnis, wenngleich in geringerem Umfang, auch für Verarbeitungen zu führen, wenn er personenbezogene Daten im Auftrag verarbeitet.

In Absatz 3 werden Aussagen zur Form des Verzeichnisses und dessen Führung 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 wird das Verzeichnis und seine Aktualisierungen dem Landesbeauftragten für den Datenschutz auf Anfrage zur Verfügung gestellt.

Zu § 27 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)

Durch § 27 soll Artikel 20 der Richtlinie (EU) 2016/680 umgesetzt werden, der generische Anforderungen an die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Grundeinstellungen (Privacy by Default) formuliert. Der Norm liegt der Gedanke zugrunde, dass der Aufwand zur Verfolgung der hier formulierten Ziele und Anforderungen im Sinne eines effektiven Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen sollte.

Die in Absatz 2 angesprochene Anforderung, die automatisierte umfassende Zugänglichmachung personenbezogener Daten zu verhindern, mündet letztlich in die Anforderung, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen.

Zu § 28 (Unterscheidung zwischen verschiedenen Kategorien betroffener Personen)

§ 28 dient der Umsetzung von Artikel 6, bei Absatz 2 der Umsetzung von Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit werden dem Fachrecht überlassen.

Zu § 29 (Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen)

§ 29 dient der Umsetzung von Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit werden dem Fachrecht überlassen.

Zu § 30 (Verfahren bei Übermittlungen)

Absatz 1 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680. Im Hinblick auf die Vervollständigung unvollständiger Daten als möglichem Sinn und

Zweck einer Datenübermittlung wurden die in der Richtlinie (EU) 2016/680 enthaltene Vermeidung der Übermittlung „unvollständiger“ Daten nicht übernommen. Ferner ist bei der Anwendung und Auslegung der Anforderungen des § 30 zu beachten, dass sich die Frage nach der „Aktualität“ von Daten und der damit verbundenen Vorgabe, keine „nicht mehr aktuellen“ Daten zu übermitteln bzw. bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten wie alte Meldeadressen, alte (Geburts-)namen etc. für die Aufgabenerfüllung erforderlich sein.

Absatz 2 wiederum setzt Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 um. Beispiele für die im Fachrecht vorgesehene Mitgabe besonderer Bedingungen können Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

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

Zu § 31 (Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung)

§ 31 dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Pflicht des Verantwortlichen. Systematisch werden in § 31 Pflichten des Verantwortlichen zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung thematisiert, die unabhängig davon bestehen, ob eine betroffene Person darum nachsucht. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung, Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen finden sich in § 14.

In Absatz 1 wird neben der Pflicht des Verantwortlichen zur Berichtigung Artikel 16 Absatz 5 der Richtlinie (EU) 2016/680 umgesetzt.

Absatz 2 dient der Umsetzung von Artikel 16 Absatz 2 der Richtlinie (EU) 2016/680, in dem gleichzeitig das Betroffenenrecht auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung erwähnt wird. Die Erweiterung des Katalogs der Tatbestände, bei deren Vorliegen eine Verarbeitungseinschränkung an die Stelle einer Löschung treten kann, um Satz 2 Nr. 2 nimmt ein entsprechendes Element aus Artikel 16 Absatz 3 Buchstabe b der Richtlinie (EU) 2016/680 auf und versteht den dort verwendeten Begriff „Beweiszwecke“ im Sinne von „Zwecke eines gerichtlichen Verfahrens“. Im Übrigen wird auf die Ausführungen zu § 14 Absatz 3 verwiesen.

Absatz 3 dient der Umsetzung von Artikel 5 der Richtlinie (EU) 2016/680.

Absatz 4 dient der Umsetzung von Artikel 16 Absatz 6 und Artikel 7 Absatz 3 der Richtlinie (EU) 2016/680.

Absatz 5 übernimmt die bisher in § 16 Absatz 7 DSG LSA enthaltene Verpflichtung, Unterlagen vor einer Löschung dem zuständigen Archiv anzubieten.

Zu § 32 (Protokollierung)

§ 32 dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und statuiert in Absatz 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen.

Absatz 2 enthält konkrete Vorgaben an den Inhalt der Protokolle, Absatz 3 Verwendungsbeschränkungen. Von der durch die Richtlinie (EU) 2016/680 eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus wird auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten Gebrauch gemacht.

In Absatz 4 wird eine Löschfrist für die Protokolldaten generiert.

In Absatz 5 wird festgelegt, dass die Protokolle dem Datenschutzbeauftragten und dem Landesbeauftragten für den Datenschutz zum Zweck der Datenschutzkontrolle zur Verfügung stehen müssen.

Zu § 33 (Vertrauliche Meldung von Verstößen)

§ 33 dient der Umsetzung von Artikel 48 der Richtlinie (EU) 2016/680. Der Verantwortliche hat im Zusammenhang mit der Meldung von Verstößen sowohl interne Meldungen als auch Hinweise von betroffenen Personen oder sonstigen Dritten in den Blick zu nehmen. Für beide Stränge bietet sich als Kontakt- und Beratungsstelle der Datenschutzbeauftragte an.

Zu § 34 (Allgemeine Voraussetzungen)

§ 34 dient der Umsetzung von Artikel 35 der Richtlinie (EU) 2016/680 und statuiert Voraussetzungen, die bei jeder Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen vorliegen müssen. Darüber hinaus enthält die Vorschrift zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen - auch an die insbesondere nach den §§ 34 bis 37 erforderliche Abwägungsentscheidung - aufgrund der Rechtsprechung des Bundesverfassungsgerichts (so etwa in BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 u. 1 BvR 1140/06). In besonderer Ausprägung dessen fordert Absatz 2 ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen weiter besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist; hierbei ist besonders zu berücksichtigen, wenn der Empfänger einen angemessenen Schutz der Daten garantiert.

Zu § 35 (Datenübermittlung bei geeigneten Garantien)

§ 35 dient der Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680. In § 35 werden den § 34 ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 gefasst hat, formuliert. Bei solchen Konstellationen kommt dem Verantwortlichen - insbesondere nach § 35 Absatz 1 Absatz 1 Nr. 2 - die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Die auf Grundlage des § 26 Absatz 5 Satz 4 SOG

LSA bestehende polizeiliche Praxis, nach einer solchen Beurteilung die Datenübermittlung mit der Mitgabe von Verarbeitungsbedingungen - etwa Löschverpflichtungen nach Zweckerreichung, Weiterübermittlungsverbote, Zweckbindungen - zu verbinden, ist dazu geeignet, diese Beurteilung zu dokumentieren und ihr Ergebnis zu sichern. Im Zusammenhang mit dem auch hier anwendbaren § 34 Absatz 2 entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaats bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Absatz 2 dient der Umsetzung von Artikel 37 Absatz 3 der Richtlinie (EU) 2016/680 zur Dokumentation der Übermittlungen nach § 35.

Absatz 3 dient der Umsetzung von Artikel 37 Absatz 2 der Richtlinie (EU) 2016/680, der die Unterrichtung des Landesbeauftragten für den Datenschutz über Kategorien von Übermittlungen vorsieht, die ohne Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach entsprechender Beurteilung durch den übermittelnden Verantwortlichen erfolgen.

Zu § 36 (Datenübermittlung ohne geeignete Garantien)

§ 36 dient der Umsetzung von Artikel 38 der Richtlinie (EU) 2016/680 und beleuchtet Konstellationen, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in § 35 erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Zu § 37 (Sonstige Datenübermittlung an Empfänger in Drittstaaten)

§ 37 dient der Umsetzung 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 der Strafverfolgung tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind. Für solche Übermittlungen „im besonderen Einzelfall“ gelten die in § 37 Absatz 1 genannten strengen Voraussetzungen. In Absatz 4 ist eine verstärkte Zweckbindung der gemäß § 37 übermittelten Daten vorgesehen.

Zu § 38 (Gegenseitige Amtshilfe)

§ 38 dient der Umsetzung des Artikels 50 der Richtlinie (EU) 2016/680.

Zu § 39 (Schadensersatz und Entschädigung)

Die Vorschrift setzt Artikel 56 der Richtlinie (EU) 2016/680 um.

Zu § 40 (Strafvorschriften)

Die Vorschrift setzt Artikel 57 der Richtlinie (EU) 2016/680 um. Durch § 40 wird keine dem deutschen Recht grundsätzlich fremde Strafbarkeit öffentlicher Stellen eingeführt.

Zu § 41 (Sprachliche Gleichstellung)

Da *generell* im Zusammenhang mit dem Landesbeauftragten für den Datenschutz die männliche Form benutzt wird, muss eine sprachliche Gleichstellungsklausel eine geschlechtergerechte Sprache herstellen.

Zu § 42 (Einschränkung von Grundrechten)

Mit dem DSUG 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 die Beachtung des Zitiergebots für den Gesetzgeber kenntlich zu machen.

Artikel 2 Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt

Artikel 2 bewahrt den bisherigen Stand des Datenschutzes im Gesetz über den Verfassungsschutz durch statischen Verweis auf die letzte amtlich bekannt gemachte Fassung des DSG LSA. Damit wird klargestellt, dass die Tätigkeit des Verfassungsschutzes auch in Zukunft keinen europäischen Vorgaben unterliegt. Die bisherigen Zuständigkeiten des Landesbeauftragten für den Datenschutz verändern sich dadurch nicht. Zur Klarstellung wurden obsolet gewordene organisatorische Regelungen von der Anwendung ausgenommen.

Artikel 3 Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt

Allgemeines

Die Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung (SOG LSA) dient der Umsetzung der EU-Datenschutzreform mit deren beiden EU-Rechtsakten der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 im bereichsspezifischen Datenschutzrecht des SOG LSA und der Anpassung bestehender Befugnisnormen zur sicherheits- und polizeibehördlichen Aufgabenerfüllung. Sowohl das Erfordernis zur Umsetzung der Richtlinie (EU) 2016/680 bis zum 6. Mai 2018 als auch die ab dem 25. Mai 2018 unmittelbare Geltung beanspruchende Verordnung (EU) 2016/679 lösen aufgrund der zahlreichen bereichsspezifischen datenschutzrechtlichen Regelungen im SOG LSA einen bedeutenden Anpassungs- und Umsetzungsbedarf aus. Hierbei ist zu berücksichtigen, dass sich die beiden EU-Rechtsakte ausgehend von Art. 2 Absatz 1 der Richtlinie (EU) 2016/680 insoweit voneinander abgrenzen, dass die Richtlinie Anwendung findet bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, und Art. 2 Buchstabe d der Verordnung (EU) 2016/679 dies aufgreifend die Verordnung für die Verarbeitung personenbezogener Daten zu den vorgenannten Zwecken der Richtlinie für nicht anwendbar erklärt. In diesem Zusammenhang ist die landesrechtliche Konturierung des Anwendungsbereichs der Richtlinie in § 1 des Entwurfs des Datenschutzrichtlinienums-

etzungsgesetzes Sachsen-Anhalt (DSUG LSA-E) von besonderer Bedeutung. Vor dem Hintergrund, dass die zur Aufgabenerfüllung erfolgende Verarbeitung personenbezogener Daten durch die Sicherheits- und Polizeibehörden nicht ausschließlich dem Anwendungsbereich der Richtlinie (EU) 2016/680 unterfällt, sind neben den erforderlichen Arbeiten zur Umsetzung der vorgenannten Richtlinie in dem vorliegenden Entwurf sowie dem subsidiär zur Anwendung kommenden DSUG LSA auch die Maßgaben der Verordnung (EU) 2016/679 und die deren Durchführung dienenden Vorschriften des DSUG LSA zu berücksichtigen. Weitere Regelungskomplexe des Entwurfs stellen die Vorschriften zur Übermittlung personenbezogener Daten sowie die Ausgestaltung der datenschutzrechtlichen Betroffenenrechte dar.

Die Änderungen im SOG LSA dienen zum anderen der teilweisen Umsetzung der Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 20. April 2016, welche das Bundesverfassungsgericht im Zusammenhang mit der Prüfung bestimmter Normen des Bundeskriminalamtsgesetzes (BKAG) gemacht hat. Das Bundesverfassungsgericht hat in seiner Entscheidung u.a. Ausführungen zu Kernbereichsregelungen, besonderen datenschutzaufsichtlichen Kontrollen bei eingriffsintensiven und verdeckten Maßnahmen und Datenübermittlungen im internationalen Bereich gemacht sowie das von ihm geprägte Kriterium der hypothetischen Datenneuerhebung für eingriffsintensive Maßnahmen weiter konturiert und als allgemeinen datenschutzrechtlichen Grundsatz geprägt. Zwar beschäftigt sich das Urteil des Bundesverfassungsgerichts mit spezifischen Normen des BKAG, jedoch sind die Ausführungen im Urteil an vielen Stellen auch für das polizeiliche Gefahrenabwehrrecht in den Ländern von grundsätzlicher und allgemeingültiger Bedeutung und müssen daher auch im SOG LSA nachvollzogen werden.

Zu Nr. 1 (Inhaltsübersicht)

Es handelt sich um redaktionelle Änderungen.

Zu Nr. 2 (§ 6 Absatz 3 - Benachteiligungsverbot)

Das Benachteiligungsverbot wird zur Umsetzung der Richtlinie (EU) 2016/680 um die Ethnie und die Gewerkschaftszugehörigkeit ergänzt. Es handelt sich nach Artikel 10 der Richtlinie (EU) 2016/680 um besondere Kategorien personenbezogener Daten für die geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorzusehen sind.

Zu Nr. 3 (§ 12)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 4 (§ 13a Geltung von anderen Vorschriften zum Schutz personenbezogener Daten)

Absatz 1

Der Absatz 1 übernimmt die bestehende Regelung des § 13a.

Absatz 2

Die Regelung hat deklaratorische Bedeutung und soll den Rechtsanwendern der Sicherheitsbehörden und der Polizei Folgendes verdeutlichen: Das SOG LSA stellt im Anwendungsbereich der Datenschutz-Grundverordnung nach Maßgabe des Artikels 6 Absatz 2 Datenschutz-Grundverordnung als bereichsspezifisches Datenschutzrecht lediglich spezifischere Anforderungen für die Verarbeitung personenbezogener Daten, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung personenbezogener Daten zu gewährleisten. Soweit keine spezifischeren Anforderungen im SOG LSA gestellt werden oder die Pflichten oder Rechte nach Art. 23 Abs. 1 Datenschutz-Grundverordnung eingeschränkt werden, ist die Datenschutz-Grundverordnung als unmittelbar geltendes Recht der Europäischen Union anzuwenden.

Absatz 3

Die Regelung stellt für den Rechtsanwender das Verhältnis des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt zum SOG LSA klar. Das Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt geht dem SOG LSA als Datenschutzquerschnittsrecht des Landes Sachsen-Anhalt im Anwendungsbereich der Richtlinie (EU) 2016/680 vor, soweit das SOG LSA als bereichsspezifisches Datenschutzrecht nichts anderes bestimmt.

Zu Nr. 5 (§§ 13b bis 13f [neu])

§ 13b [neu] - Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung)

Die Regelung setzt das vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 konkretisierte und geprägte Kriterium der hypothetischen Datenneuerhebung für besonders eingriffsintensive Maßnahmen bei der Polizei um.

In seinem oben genannten Urteil hat das Bundesverfassungsgericht festgestellt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung und sich die Reichweite der Zweckbindung nach der jeweiligen Ermächtigung für die Datenerhebung richten. Die Datenerhebung selbst bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren.

Das Bundesverfassungsgericht führt in seinem Urteil (BVerfG, aaO, Randnummer 286 und 287) aus, dass die Ermächtigung zu einer Zweckänderung am Verhältnismäßigkeitsgrundsatz zu messen ist und sich die Verhältnismäßigkeitsanforderungen für eine Zweckänderung der Verarbeitung von Daten, die aus besonders eingriffsin-

tensiven Maßnahmen stammen, am Grundsatz der hypothetischen Datenneuerhebung orientieren: „Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken benutzt werden (vgl. BVerfGE 100, 313 <394>; 109, 279 <377>; 133, 277 <372 f. Rn. 225> m. w. N.). Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen wie denen des vorliegenden Verfahrens kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften."
Das Kriterium der hypothetischen Datenneuerhebung wird als allgemeiner Grundsatz formuliert, der bei jeder Datenverarbeitung durch die Polizei - unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme - zu beachten ist.

Absatz 1

Satz 1 stellt klar, dass die Verarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten durch die Polizei nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung unterliegt. Das Bundesverfassungsgericht führt hierzu in seinem Urteil (BVerfG, aaO, Randnummern 278 f., 282) aus:

„Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben. Er kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung. Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. [….] Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt."

Satz 2 trägt den besonderen Anforderungen des Bundesverfassungsgerichts (BVerfG, aaO, Randnummer 283) an die Zweckbindung für Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 17) Rechnung. Aufgrund des besonderen Eingriffsgewichts solcher Datenerhebungen gilt hier eine besonders enge Bindung jeder weiteren Nutzung der bei diesen Maßnahmen gewonnenen Daten an die Voraussetzungen und Zwecke der Datenerhebung. Das Bundesverfassungsgericht führt hierzu aus: „Weiter reicht die Zweckbindung allerdings für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen: Hier ist jede

weitere Nutzung der Daten nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. BVerfGE 109, 279 <377, 379>) oder im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.>) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht."

Für die Verarbeitung von personenbezogenen Daten, die aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 17) sowie zur Erhebung von Telekommunikationsinhalten und -umständen (§ 17b) erlangt wurden, sieht Satz 2 daher vor, dass im Einzelfall eine Gefahrenlage im Sinne des § 17 Absatz 4 bzw. § 17b Absatz 1 (gegenwärtige Gefahr für Leib oder Leben einer Person) vorliegen muss, was eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz ausschließt.

Absatz 2

Satz 1 Nr. 1 setzt die Vorgaben des Bundesverfassungsgerichts an die zweckändernde Verarbeitung von personenbezogenen Daten um und führt damit den Grundsatz der hypothetischen Datenneuerhebung in das SOG LSA ein. Das Bundesverfassungsgericht (BVerfG, aaO, Randnummern 288 bis 290) hat zum Grundsatz der hypothetischen Datenneuerhebung ausgeführt: „Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten [...]. Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses.

Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten - sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde - ein konkreter Ermittlungsansatz ergibt. Der Gesetzgeber kann danach - bezogen auf die Datennutzung von Polizeibehörden - eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist."

Satz 1 Nr. 1 erfüllt diese verfassungsrechtlichen Anforderungen vollumfänglich und lässt demgemäß die Verarbeitung personenbezogener Daten zur Erfüllung der Aufgaben des Bundeskriminalamtes zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, nur zu, wenn mindestens vergleichbar gewichtige Straftaten

verhütet, aufgedeckt, verfolgt oder mindestens vergleichbar gewichtige Rechtsgüter geschützt werden können und sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für solche Rechtsgüter erkennen lassen, zu deren Schutz die entsprechende Datenerhebung verfassungsrechtlich zulässig wäre. Der Grundsatz der hypothetischen Datenneuerhebung wird hierbei als allgemeiner Grundsatz in das Landespolizeirecht eingeführt und ist nicht auf besonders eingriffsintensive Maßnahmen beschränkt.

Mit der Formulierung „vergleichbar schwer wiegend“ werden keine gleichgewichtigen Zwecke vorausgesetzt. Die „Vergleichbarkeit“ folgt aus den rechtsgutsbezogenen Erhebungsschwellen, nämlich gewissermaßen einer Gewichtungsklasse, welche die Zwecke oberhalb dieser Schwelle umfasst. Wenn beispielsweise bei einer Telekommunikationsüberwachung, die nach § 17b Absatz 1 zur Abwehr einer Gefahr für Leib oder Leben (Lebensgefahr) erfolgt, Zufallserkenntnisse zu einem anderen Lebenssachverhalt mit Anhaltspunkten für eine Freiheitsgefahr anfallen, kann auch diese andere Gefahr mit diesem Spurenansatz weiter erforscht werden. Die Abwehr der Freiheitsgefahr erscheint zwar gegenüber der Abwehr der Lebensgefahr (als ursprünglicher Erhebungszweck) nicht gleichgewichtig, mit Blick auf die Erhebungsschwelle der Art der jeweiligen Maßnahme aber vergleichbar gewichtig.

Der Begriff des Rechtsgutes bezeichnet das rechtlich geschützte Interesse einzelner Rechtspersonen (Individualrechtsgüter) und der Gesellschaft sowie des Staates als solcher (Universalrechtsgüter).

Besonders bedeutsame Rechtsgüter sind Rechtsgüter nach § 3 Nr. 3 Buchstabe c SOG LSA. Hierzu gehört aber auch die körperliche Unversehrtheit oder die sexuelle Selbstbestimmung. Satz 2 stellt klar, dass der Grundsatz der hypothetischen Datenneuerhebung die Nutzung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung (§ 25a [neu]), der Ausbildung (§ 25b Absatz 1 [neu]) und der Vorgangsdokumentation (§ 22 Absatz 5) nicht ausschließt.

Absatz 3

Satz 1 trägt den besonderen Anforderungen des Bundesverfassungsgerichts an die zweckändernde Nutzung von Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen Rechnung und berücksichtigt auch den schwerwiegenden Eingriff der Erhebung von Telekommunikationsinhalten und -umständen. Das Bundesverfassungsgericht stellt in seinem Urteil als Anforderung an das Kriterium der hypothetischen Datenneuerhebung die Voraussetzung auf, dass die Verwendung der erhobenen personenbezogenen Daten zu einem neuen Zweck nur zulässig ist, wenn für den neuen Zweck eine entsprechende Datenerhebung nach verfassungsrechtlichen Maßstäben zulässig wäre. Die Datenverwendung zu einem geänderten Zweck ist im Falle des Vorliegens einer Gefahr nur möglich, wenn im Einzelfall eine gegenwärtige Gefahr für Leib oder Leben vorliegt. Das SOG LSA berücksichtigte dies bereits in § 17 Absatz 4e bzw. § 17b Absatz 5 Satz 3. Die Regelung wird aus systematischen Gründen in den § 13b [neu] übernommen.

Satz 2 untersagt, dass Erkenntnisse aus optischen Wohnraumüberwachungen zu Strafverfolgungszwecken verwendet werden dürfen. Das Bundesverfassungsgericht (BVerfG, aaO, Randnummer 317) führt hierzu aus: „Verfassungsrechtlich zu bean-

standen ist weiterhin, dass Daten aus optischen Wohnraumüberwachungen von einer Übermittlung an die Strafverfolgungsbehörden nicht ausgeschlossen sind. Artikel 13 Absatz 3 GG erlaubt für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung. Dies darf durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden.“

Absatz 4

Absatz 4 sieht vor, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die Grunddaten einer Person zu Identifizierungszwecken verwendet werden sollen. Da die Datenverwendung so in doppelter Weise eng begrenzt ist - nur Grunddaten und nur zum Zweck der Identifizierung - ist das Eingriffsgewicht dieser Maßnahme mit der Rechtsprechung des Bundesverfassungsgerichts zu vereinbaren. Weitere Daten - etwa die weiteren zu einer als „Treffer“ identifizierten Person gespeicherten Ereignisse - sind hingegen nach Absatz 4 nicht verfügbar; insoweit bleibt es bei den Begrenzungen nach den Absätzen 2 und 3.

Die zweifelsfreie Klärung der Identität einer Person ist notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte von unbeteiligten Personen stattfinden. Die Polizei muss daher zur Erfüllung ihrer Aufgaben die Grunddaten einer Person stets zu diesem Zweck verarbeiten können.

Absatz 5

Absatz 5 sieht die Verpflichtung der verantwortlichen Polizeibehörde vor, bei der Verarbeitung von personenbezogenen Daten durch technische und organisatorische Vorkehrungen sicherzustellen, dass die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung beachtet werden. Die in Absatz 5 geregelte Verpflichtung findet ihre nähere Ausgestaltung in den §§ 13d (Kennzeichnung) und 13e (Regelung von Zugriffsberechtigungen), die festlegen, wie der Grundsatz der hypothetischen Datenneuerhebung technisch im Informationssystem der Polizei umzusetzen ist. Die hierfür erforderlichen grundsätzlichen Änderungen der IT-Architektur erfordern einen erheblichen technischen Aufwand und lassen sich nicht kurzfristig realisieren.

Bis zum Abschluss des entsprechenden IT-Projekts zur Neugestaltung des Informationssystems der Polizei und der vollständigen technischen Umsetzung der §§ 13d und 13e im Informationssystem treffen die Polizeibehörden geeignete Maßnahmen, die ein hohes Maß an Beachtung des Grundsatzes der hypothetischen Datenneuerhebung gewährleisten. Absatz 5 gilt für die Erhebung von neuen Daten sowie grundsätzlich auch für Altdatenbestände. Personenbezogene Daten, die aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen (§ 17) sowie zur Erhebung von Telekommunikationsinhalten und -umständen (§ 17b) erlangt wurden, sind bereits aufgrund bestehender Normen besonders zu kennzeichnen (§ 17 Absatz 4e, § 17b Absatz 5 SOG LSA).

§ 13c [neu] - Informationssystem der Polizei

Die Polizei betreibt zur Erfüllung ihrer Aufgaben nach § 2 Absatz 1 SOG LSA (vorbeugende Bekämpfung von Straftaten und Vorsorge für die Verhütung von Straftaten) und der ihr nach anderen Rechtsvorschriften zugewiesenen weiteren Aufgaben im Rahmen der Strafverfolgung ein Informationssystem. Da die Polizei in diesem Informationssystem personenbezogene Daten zum Zwecke der Durchführung von Strafverfahren und für Zwecke künftiger Strafverfahren zusammen mit personenbezogenen Daten speichert, deren Speicherung sich nach den Polizeigesetzen richtet, findet insoweit das für die Landespolizei geltende Datenschutzquerschnittsrecht des Landes sowie das bereichsspezifische Datenschutzrecht des SOG LSA Anwendung (vgl. § 483 Absatz 3, § 484 Absatz 4 StPO).

Die Regelung beschreibt die Grundfunktionen des Informationssystems der Polizei. Die einzelnen regelbeispielhaft aufgezählten Grundfunktionen beschreiben Kernelemente polizeilicher Arbeit, bei denen das Informationssystem die Bediensteten der Polizei bei der Wahrnehmung ihrer Aufgaben unterstützt.

§ 13d [neu] - Kennzeichnung personenbezogener Daten

Absatz 1

Der Grundsatz der hypothetischen Datenneuerhebung lässt sich im Informationssystem der Polizei und im Falle der Übermittlung von Daten an die Polizeien des Bundes und der Länder in deren Informationssystemen nur umsetzen, wenn die darin gespeicherten personenbezogenen Daten mit den notwendigen Zusatzinformationen versehen, das heißt gekennzeichnet, sind. Satz 1 sieht dementsprechend vor, dass personenbezogene Daten durch Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden (Nummer 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie nach § 23 (Nummer 2), durch die Angabe der Rechtsgüter, deren Schutz die Erhebung dient oder Straftaten, deren Verfolgung oder Verhütung die Erhebung dient (Nummer 3), und durch die Angabe der Stelle, die sie erhoben hat, zu kennzeichnen sind. Diese umfassende Kennzeichnung, die nach § 29 BKAG-neu auch für den Informationsverbund zwischen Bund und Ländern gilt, schafft die Voraussetzung für eine konsistente Anwendung des Grundsatzes der hypothetischen Datenneuerhebung. Nach Satz 2 kann die Kennzeichnung auch durch eine Angabe der Rechtsgrundlage der der Erhebung zugrundeliegenden Mittel ergänzt werden.

Absatz 2

Zur Vermeidung des Weiterverarbeitens von Daten, die nicht dem Grundsatz der hypothetischen Datenneuerhebung entspricht, bestimmt Absatz 2, dass personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, solange nicht weiterverarbeitet werden dürfen, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

Absatz 3

Damit der Grundsatz der hypothetischen Datenneuerhebung auch beim Weiterverarbeiten von Daten bei anderen Stellen beachtet werden kann, regelt Absatz 3, dass die nach Absatz 1 vorzunehmende Kennzeichnung im Falle der Übermittlung der Daten durch die empfangende Stelle aufrechtzuerhalten ist.

§ 13e [neu] - Regelung von Zugriffsberechtigungen für das Informationssystem der Polizei

Absatz 1

Die Anforderungen der Zweckbindung und des Grundsatzes der hypothetischen Datenneuerhebung sind im Informationssystem der Polizei durch ein geeignetes System von Zugriffsberechtigungen auf personenbezogene Daten umzusetzen. Die Nr. 1 bestimmt dementsprechend, dass - auf Grundlage der Kennzeichnungen nach § 13d - die Beachtung der Vorgaben des § 13b bei der Erteilung von Zugriffberechtigungen sicherzustellen ist. Damit ist bei der Polizei die Beachtung des Grundsatzes der hypothetischen Datenneuerhebung technisch zu implementieren. Durch die Zugriffsberechtigung wird festgelegt, wer auf welche - der nach § 13d gekennzeichneten - personenbezogenen Daten zugreifen kann. Die Nr. 2 legt ergänzend fest, dass die Zugriffsberechtigungen so auszugestalten sind, dass der Zugriff nur auf diejenigen personenbezogenen Daten erfolgen kann, deren Kenntnis für die Erfüllung der jeweiligen Dienstpflichten erforderlich ist. In Kombination mit der Nr. 1 bedeutet dies, dass die sich aus dem jeweiligen Dienstposten eines Bedienteten ergebenden Dienstpflichten (zum Beispiel Durchführung von Ermittlungen im Bereich „Delikte der Organisierten Kriminalität“) bestimmen, wie die Zugriffsberechtigung auszugestalten ist.

Absatz 2

Absatz 2 regelt klarstellend in Ergänzung zu Absatz 1, dass bei der Vergabe von Zugriffberechtigungen auch sicherzustellen ist, dass Änderungen, Berichtigungen und Löschungen personenbezogener Daten nur von hierzu befugten Personen erfolgen können.

Absatz 3

Satz 1 bestimmt, dass die Polizei alle zur Umsetzung des Absatzes 1 erforderlichen organisatorischen und technischen Vorkehrungen und Maßnahmen, die dem Stand der Technik entsprechen, zu treffen hat. Durch die Orientierung am Stand der Technik wird betont, dass die Polizei das System der Vergabe von Zugriffsberechtigungen, insbesondere auch wegen des notwendigen hohen Datenschutzniveaus fortdauernd an neue technische Entwicklungen anzupassen hat. Satz 2 regelt, dass Grundlage der Vergabe von Zugriffberechtigungen ein abgestuftes Rechte- und Rollenkonzept sein muss. In diesem Rechte- und Rollenkonzept muss die Polizei festlegen, für welche Funktionen und Dienstposten welche Berechtigungen - sowohl hinsichtlich des Zutritts zu Arbeitsbereichen als auch hinsichtlich des Zugriffs auf Daten - erforderlich sind. Die Erstellung und Fortschreibung des Konzepts erfolgt im Benehmen mit der oder dem Landesbeauftragten für den Datenschutz.

§ 13f [neu] - Verordnungsermächtigungen zur Sicherstellung erforderlicher organisatorischer und technischer Vorkehrungen im Informationssystem der Polizei

Mit der Regelung wird das für öffentliche Sicherheit und Ordnung zuständige Ministerium ermächtigt, durch Verordnung einer Polizeibehörde Pflichten zur Sicherstellung organisatorischer und technischer Vorkehrungen nach § 13b Absatz 5 oder § 13e Absatz 3 oder 4 zu übertragen, wenn dies zur sachgerechten Erfüllung der Pflichten erforderlich ist. Es kann dabei auch die Weisungsbefugnis gegenüber anderen Polizeibehörden regeln.

Zu Nr. 6 (§ 15)

Buchstabe a) (Absatz 4)

Es handelt sich um eine redaktionelle Anpassung an den im SOG LSA neu eingeführten Begriffs „Weiterverarbeiten“.

Buchstabe b) (Absatz 7)

Mit der Neufassung des § 24 erfolgt eine Harmonisierung der Regelungen des Landespolizeirechts mit den Regelungen des BKAG-neu (vgl. § 75 BKAG-neu). Daher sind in § 15 Absatz 7 die mit § 24 korrespondierenden Regelungen überflüssig und werden gestrichen.

Zu Nr. 7 (§ 16)

Buchstabe a) (Absatz 5)

Es handelt sich zum einen um eine Anpassung an die technische Entwicklung im Bereich der Speicherung von Bild- und Tonaufzeichnung. Videokassetten, die durch Speicherung neuer die alten Aufzeichnungen löschen (Überspielen) werden so gut wie nicht mehr verwandt. Zum anderen wird der Begriff „Datei“ durch den Begriff „Dateisystem“ (vgl. § 2 Nr. 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt) ersetzt. Zudem erfolgen redaktionelle Anpassungen.

Buchstabe b) (Absatz 5a)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 8 (§ 17)

Buchstabe a) (Absatz 2)

Es handelt sich um eine redaktionelle Änderung.

Buchstabe b) (Absatz 4e)

Die Regelung des Absatzes 4e ist aufgrund der Regelungen des § 13b Absatz 3 [neu] und § 13d [neu] an dieser Stelle entbehrlich und wird daher gestrichen.

Buchstabe c) (Absatz 7)

Mit der Änderung wird Absatz 7 an den Sprachgebrauch des § 12 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Zu Nr. 9 (§ 17b)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 10 (§ 18)

Mit der Änderung wird Absatz 6 an den Sprachgebrauch des § 12 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Zu Nr. 11 (§ 19)

Mit der Änderung wird Absatz 1 an die Begriffsbestimmungen des § 2 Nr. 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Zu Nr. 12 (§ 20a)

Mit der Änderung wird Absatz 1 an die Begriffsbestimmung des § 2 Nr. 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Zu Nr. 13 (§ 22)

Buchstabe a) (Absatz 1)

Mit der Änderung wird Absatz 1 an die Begriffsbestimmung des § 2 Nr. 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Buchstabe b) (Absatz 2)

Mit der Änderung wird Absatz 2 an die Begriffsbestimmungen des § 2 Nr. 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Buchstabe c) (Absatz 3 [neu])

Es wird über § 32 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt hinausgehend und ergänzend für Verarbeitungen im Informationssystem der Polizei geregelt, dass die Protokolle den Datenschutzbeauftragten und dem Landesbeauftragten für den Datenschutz in elektronisch auswertbarer Form zum Zwecke der Datenschutzkontrolle zur Verfügung stehen müssen, um eine effiziente und IT-gestützte Datenschutzkontrolle zu ermöglichen. Die Protokollierung muss es außerdem ermöglichen zu überprüfen, ob die Regelungen über Zugriffsberechtigungen (§ 13e [neu]) eingehalten werden. Die Löschung der Protokolldaten bestimmt sich nach § 32 Absatz 4 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt.

Zu Nr. 14 - (§§ 23 [neu] Weiterverarbeiten von personenbezogenen Daten aus strafrechtlichen Ermittlungsverfahren; Daten zu Verurteilten, Beschuldigten, Tatverdächtigen, sonstigen Anlasspersonen und anderen Personen)

Die Neufassung der Norm dient insbesondere der Umsetzung des Artikels 6 der Richtlinie (EU) 2016/680. Er fordert, dass die Mitgliedstaaten für die Unterscheidbarkeit zwischen den personenbezogenen Daten verschiedener Personenkategorien Sorge zu tragen haben. Hierunter fallen insbesondere Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden, verurteilte Straftäter, Opfer einer Straftat oder Personen, bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und andere Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeugen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit Verurteilten, Beschuldigten oder Tatverdächtigen in Kontakt oder in Verbindung stehen.

Die Unterscheidbarkeit zwischen den personenbezogenen Daten verschiedener Personenkategorien bei der Datenverarbeitung bei der Polizei wurde bisher durch die Verwaltungsvorschrift („Führung von personenbezogenen Sammlungen und Dateien bei der Polizei“, RdErl. des MI vom 10. Februar 1994, MBl. LSA 1994, S. 1343; zuletzt geändert durch Verwaltungsvorschrift vom 20. Oktober 2000 MBl. LSA 2000, S. 1339) und dateibezogenen Festlegungen nach § 14 Absatz 3 DSG LSA sichergestellt.

Alle Regelungen des neuen § 23 stellen Zweckänderungsbefugnisse dar und erlauben ausschließlich der Polizei, personenbezogene Daten, die sie im Rahmen von strafrechtlichen Ermittlungsverfahren oder aber auch zur Klärung der Frage, ob in einem Sachverhalt ein strafrechtliches Ermittlungsverfahren zu führen ist (z. B. Vermisstensachen, Todesursachenermittlungen), gewonnen hat, für andere jeweils konkret bestimmte Zwecke zu verarbeiten. Zu den gewonnenen Daten zählen erhobene, aufgedrängte oder in sonstiger Weise erlangte Daten.

Absatz 1

Absatz 1 regelt, dass die Polizei zur Abwehr einer Gefahr, vorbeugenden Bekämpfung von Straftaten oder Vorsorge für die Verfolgung von Straftaten personenbezogene Daten von Verurteilten, Beschuldigten, Tatverdächtigen oder Personen, bei denen ein Anlass dafür besteht (Anlasspersonen) verarbeiten kann. Eine Erweiterung der Befugnisse der Polizei findet damit nicht statt.

Absatz 2

Der Absatz 2 systematisiert in den Nrn. 1 bis 3 die Kategorien der personenbezogenen Daten, die von den in Absatz 1 aufgeführten Personen gespeichert werden dürfen. Die Grunddaten von Verurteilten, Beschuldigten, Tatverdächtigen oder Anlasspersonen bilden die entscheidenden Faktoren für die zweifelsfreie, schnelle und effektive Identifizierung der betreffenden Person im Informationssystem der Polizei.

Absatz 3

Der Absatz 3 regelt sogenannte Prüffälle. Die Praxis hat gezeigt, dass bei der Polizei durch Hinweisgeber Erkenntnisse und Angaben zu Personen eingehen, die der Polizei bislang unbekannt waren und bei denen daher auch noch nicht feststeht, ob die betroffenen Personen einer der in Absatz 1 genannten Kategorien unterfallen. Nachdem die Polizei im Rahmen eines ersten Prüfungsschritts feststellen muss, ob die mitgeteilten personenbezogenen Daten und Erkenntnisse zu dieser Person zur Erfüllung ihrer Aufgaben benötigt werden, hat sie in einem zweiten Schritt zu ermitteln, welcher Personenkategorie die betroffenen Personen unterfallen. Die neuen Sätze 1 und 2 legen für diesen zweiten Prüfungsschritt strenge datenschutzrechtliche Maßstäbe fest. Die Verarbeitung und gegebenenfalls Anreicherung der personenbezogenen Daten darf nur zu dem Zweck erfolgen, festzustellen, ob die betroffenen Personen den Kategorien als Verurteilte, Beschuldigte, Tatverdächtige oder Personen mit Negativprognose unterfallen. Der Satz 3 sieht vor, dass die personenbezogenen Daten im Informationssystem gesondert zu speichern sind. Satz 4 bestimmt, dass die Daten nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu löschen sind, soweit nicht festgestellt wurde, dass die betreffende Person die Voraussetzungen nach Absatz 1 erfüllt. Aufgrund der vorhandenen Erfahrungen im internationalen polizeilichen Dienstverkehr und unter Berücksichtigung der teilweise erheblichen Dauer von aufwendigen Ermittlungs- bzw. Strafverfahren im In- und Ausland ist eine Frist von zwölf Monaten notwendig und angemessen.

Absatz 4

Die Regelung entspricht § 18 Absatz 4 BKAG-neu und dient der Vermeidung unnötiger Fahndungsausschreibungen, der Gewinnung von Anhaltspunkten bei Alibi-Überprüfungen und der Gefahrenabwehr durch Information über bevorstehenden Haftentlassungen.

Absatz 5

Die bisherige polizeiliche Befugnis (§ 23 alt) gestattete die Speicherung, Veränderung oder Nutzung personenbezogener Daten durch die Polizei, soweit Bestimmungen der StPO oder andere gesetzliche Regelungen nicht entgegenstehen. Nunmehr wird der Regelungsinhalt von § 484 Absatz 2 Satz 2 StPO ausdrücklich ins SOG LSA übernommen. Zudem entspricht die Regelung dem § 18 Absatz 5 BKAG-neu.

Absatz 6

Die Regelung dient im Wesentlichen der Umsetzung von Artikel 6 Buchstabe d der Richtlinie (EU) 2016/680 und harmonisiert das SOG LSA mit dem § 19 Absatz 1 BKAG-neu.

Absatz 7

Die Regelung entspricht § 19 Absatz 2 BKAG-neu und lässt die Verarbeitung von personenbezogenen Daten von Vermissten, Unbekannten und unbekannten Toten zu. Die Berechtigung der Verarbeitung dieser Daten ist nicht ausschließlich zu Zwecken der Identifizierung, sondern auch zur Abwehr einer erheblichen Gefahr für die genannten Personen oder soweit es sonst zur Erfüllung der Aufgaben der Polizei er-

forderlich ist, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um Täter, Opfer oder sonstige Personen im Zusammenhang mit einer Straftat handelt, erlaubt.

Absatz 8

Hier werden - wie auch in § 23 Absatz 3 [neu] - die sogenannten Prüffälle für die in Absätze 6 und 7 bezeichneten Personengruppen geregelt.

Zu Nr. 15 (§ 23a [neu] Verarbeiten von personenbezogenen Daten, von Strafverfolgungsbehörden der Mitgliedstaaten der europäischen Union an die Polizei übermittelt worden sind)

Der neue § 23a regelt das Weiterverarbeiten von personenbezogenen Daten, die von Strafverfolgungsbehörden der Mitgliedstaaten der europäischen Union an die Polizei übermittelt worden sind. Dies war bisher in § 23 Absatz 2 geregelt. Der dort in Bezug genommene Rahmenbeschluss 2006/960/JI des Rates der EU wurde durch die Richtlinie (EU) 2016/680 aufgehoben und wird daher nicht mehr in Bezug genommen.

Als Strafverfolgungsbehörden der Mitgliedstaaten im Sinne dieser Regelung können insbesondere jene Stellen gelten, die von diesem Staat gemäß Artikel 2 Buchstabe a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15.3.2007, S. 26) benannt wurden.

Zu Nr. 16 (§ 23b [neu] Aufzeichnung von Telefon- und Funkgesprächen)

Es handelt sich um eine redaktionelle Anpassung.

Zu Nr. 17 (§ 23c [neu] Ermittlung des Aufenthaltsort gefährdeter Personen)

Es handelt sich zum einen um eine redaktionelle Anpassung und zum anderen um eine Anpassung an den in § 12 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt verwandten Begriff „Benachrichtigung“.

Zu Nr. 18 (§ 23d [neu] Speicherung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren)

Die Regelung sieht die Möglichkeit vor, bei der Polizei eine DNA-Referenzdatenbank zu führen, um sogenannte DNA-Trugspuren, die durch Verunreinigungen der betreffenden Spurenträger bei der kriminaltechnischen Untersuchung entstehen können, auszuschließen. Hierdurch können aufwendige Ermittlungsverfahren aufgrund von DNA-Trugspuren verhindert werden.

Die DNA-Analyse nimmt für die Aufklärung von Straftaten mittlerweile eine zentrale Rolle ein. Die Methoden der DNA-Analyse haben sich ständig weiterentwickelt und die für die Analysen notwendige Menge an DNA-Material hat sich beständig verringert. Da mittlerweile bereits in etwa 20 Nanogramm DNA-Material, was der Menge von ca. zwei bis drei DNA-Biomolekülen entspricht, ausreichend ist, um das DNA-

Identifizierungsmuster feststellen zu können, können selbst kleinste Verunreinigungen zu sogenannten Trugspuren führen. Ein öffentlichkeitswirksames Beispiel für DNA-Trugspuren stellt der Fall des sogenannten „Phantoms von Heilbronn“ dar. Nachdem am 25. April 2007 in Heilbronn auf der Theresienwiese eine Polizistin getötet wurde und ihr Kollege durch einen Kopfschuss schwerste Verletzungen erlitten hatte, wurde am Tatort ein DNA-Identifizierungsmuster einer weiblichen Unbekannten entdeckt. Bei Abgleichen dieses DNA-Identifizierungsmuster mit den polizeilichen Datenbanken wurde festgestellt, dass in 40 weiteren Fällen übereinstimmende genetische Spuren gefunden wurden. Diese Feststellungen führten zu umfangreichen Ermittlungs- und Fahndungsmaßnahmen in den Jahren 2007 bis 2009 in Süddeutschland, Österreich und Frankreich. Letztendlich stellte sich heraus, dass das fragliche DNA-Identifizierungsmuster von einer Mitarbeiterin der Herstellerfirma der für die Spurensicherung eingesetzten Wattestäbchen stammte und es sich damit um eine DNA-Trugspur handelte. Eine unter Datenschutzgesichtspunkten weniger belastende anonymisierte Speicherung der DNA-Identifizierungsmuster ist nicht möglich. Denn neben der Feststellung, dass es sich um eine Trugspur handelt, ist es von wesentlicher Bedeutung zu ermitteln, auf welche Weise das Spurenmaterial verunreinigt wurde. Nur auf diese Weise lässt sich für künftige Fälle das Risiko einer erneuten Verunreinigung minimieren. Mit einer anonymisierten Speicherung ist dies nicht möglich.

Derzeit werden personenbezogene von Bediensteten der Polizei und Mitarbeitern externer Dienstleister (z. B. Reinigungskräfte und Wartungspersonal) auf der Grundlage einer informierten Einwilligungserklärung in einer entsprechenden Datenbank nach Maßgabe des Runderlasses des Ministeriums für Inneres und Sport vom 10. August 2017 (MBl. LSA 2017, S. 455) verarbeitet. Da die Datenverarbeitung mittelbar dem Zweck der Ermittlung von Straftaten dient, ist der Anwendungsbereich der Richtlinie (EU) 2016/680 eröffnet und eine gesetzliche Ausgestaltung erforderlich.

Absatz 1

Der neue Absatz 1 ermöglicht der Polizei, von ihren Mitarbeiterinnen und Mitarbeitern, die Umgang mit Spurenmaterial haben oder die Bereiche in ihren Liegenschaften und Einrichtungen betreten müssen, in denen mit Spurenmaterial umgegangen oder dieses gelagert wird, mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen zu entnehmen, hieraus das DNA-Identifizierungsmuster festzustellen und dieses mit an Spurenmaterial festgestellten DNA-Identifizierungsmustern automatisiert abzugleichen. Der Abgleich darf nur zu dem Zweck erfolgen, DNA-Trugspuren zu erkennen.

Satz 2 und 3 legen enge Zweckbindungen der Nutzung der Daten fest: Die entnommenen Körperzellen dürfen nur zur Feststellung des DNA-Identifizierungsmuster genutzt werden. Sie sind unverzüglich zu vernichten, sobald sie hierfür nicht mehr erforderlich sind. Andere Feststellungen als diejenigen, die zur Ermittlung des DNA-Identifizierungsmusters erforderlich sind, dürfen bei der Untersuchung des DNA-Identifizierungsmusters nicht getroffen werden.

Absatz 2

Der Absatz 2 gibt der Polizei die Möglichkeit, unter den Voraussetzungen des Absatzes 1 DNA-Identifizierungsmuster von anderen Personen zum Aufdecken von DNA-

Trugspuren zu untersuchen und abzugleichen. Die Untersuchungen und Abgleiche dürfen nur mit dem schriftlichem Einverständnis der betreffenden Person erfolgen. Andere Personen im Sinne dieser Regelung sind insbesondere Mitarbeiter der Polizeien des Bundes und der Länder, die - ggf. im Rahmen der Amtshilfe - in Kontakt mit dem auszuwertenden Spurenträger geraten sind.

Absatz 3

Nach Satz 1 sind die DNA-Identifizierungsmuster zu pseudonymisieren und darüber hinaus im Informationssystem der Polizei gesondert zu speichern. Satz 2 verbietet eine Verwendung der DNA-Identifizierungsmusters zu anderen als den in den Absätzen 1 bis 3 genannten Zwecken. Satz 3 sieht vor, dass die DNA-Identifizierungsmuster unverzüglich zu löschen sind, wenn ihre Verarbeitung für die Zwecke nicht mehr erforderlich ist. Nach Satz 4 hat die Löschung spätestens 3 Jahre nach dem letzten Umgang der betreffenden Person mit Spurenmaterial oder dem letzten Zutritt zu einem Bereich, in dem mit Spurenmaterial umgegangen wird, zu erfolgen. Satz 5 sieht vor, dass betroffene Personen schriftlich über den Zweck und die Verarbeitung der erhobenen Daten zu informieren sind.

Zu Nr. 19 (§ 24 Benachrichtigung beim Speichern von personenbezogenen Daten von Kindern [neu])

Mit der Neufassung des § 24 erfolgt eine Harmonisierung der Regelungen des Landespolizeirechts mit den Regelungen des BKAG-neu (vgl. § 75 BKAG-neu). Die bisher durch § 24 Absatz 1 normierte Unterrichtungspflicht bei einer länger als drei Jahre andauernden Speicherung in automatisierten Dateien widerspricht dem Ziel der Harmonisierung datenschutzrechtlicher Regelungen. Gerade im Hinblick auf Speicherungen im Informationsverbund zwischen Bund und Ländern führt dies zu einer nicht gerechtfertigten Ungleichbehandlung der betroffenen Person.

Zu Nr. 20 (§25 [neu] Weiterverarbeiten für die wissenschaftliche Forschung)

Die Verarbeitung personenbezogener Daten zu Ausbildungszwecken, statistischen oder wissenschaftlichen Zwecken ist bisher für die Sicherheitsbehörden und die Polizei einheitlich in § 25 in Verbindung mit dem § 27 DSG LSA geregelt. Die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken durch die Sicherheitsbehörden und die Polizei außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 ist nicht mehr Regelungsgegenstand. Hierauf ist die Verordnung (EU) 2016/679 anzuwenden soweit nicht abweichende Regelungen des Bundes- oder Landesrechts zu berücksichtigen sind. Im Anwendungsbereich der Richtlinie (EU) 2016/680 finden für die Polizei die Regelungen der neuen §§ 25a und 25b Anwendung. Diese Regelungen sind den §§ 21 und 22 des BKAG-neu mit dem Ziel der Harmonisierung des Polizeirechts des Bundes und der Länder im Bereich der Verarbeitung personenbezogener Daten nachgebildet. Grund für diese Harmonisierungsbestrebungen ist der Umstand, dass die Landespolizei personenbezogene Daten nicht nur im Informationssystem der Landespolizei sondern auch - soweit es insbesondere um die Verhütung von Straftaten von erheblicher Bedeutung geht - zugleich auch im polizeilichen Informationsverbund zwischen Bund und Ländern (auf den die Regelungen des BKAG-neu anzuwenden sind) speichert.

Absatz 1

Der Satz 2 stellt klar, dass eine Verarbeitung personenbezogener Daten, die aus besonders eingriffsintensiven Maßnahmen erlangt wurden, nicht zulässig ist. Damit trägt die Regelung dem Grundsatz der hypothetischen Datenneuerhebung Rechnung.

Absatz 2

Der Satz 2 stellt klar, dass eine Übermittlung personenbezogener Daten, die aus besonders eingriffsintensiven Maßnahmen erlangt wurden, nicht zulässig ist. Damit trägt die Regelung dem Grundsatz der hypothetischen Datenneuerhebung Rechnung.

Absatz 3

Da die Akten der Polizei zukünftig elektronisch geführt werden sollen, regeln die Sätze 2 bis 3 die Form der Einsicht in die elektronische Akte. Regelform ist das Bereitstellen des Inhalts der Akte zum Abruf. Die Akte kann dazu auch in ein anderes Format übertragen (etwa im Wege eines „Exports“ in das PDF-Format) und den Antragstellern mittels einer besonders gesicherten Verbindung über ein öffentliches Telekommunikationsnetz zum Abruf bereitgestellt werden. Der Begriff „Abruf“ schließt dabei die Möglichkeit eines Herunterladens des Datenpakets ein. Bereitstellen zum Abruf bedeutet nicht Akteneinsicht „in Echtzeit“. Bezugspunkt für die Akteneinsicht ist grundsätzlich der Aktenstand im Zeitpunkt ihrer Bewilligung. Sofern der Antragsteller hieran ein berechtigtes Interesse hat, kann die Akteneinsicht auch durch einen Aktenausdruck oder einen Datenträger mit dem Inhalt der elektronischen Akten auf besonders zu begründenden Antrag übermittelt werden. Ein solcher Fall kann insbesondere dann vorliegen, wenn die zum Abruf benötigte Hard- und Software auf Seiten des Antragstellers nicht vorhanden ist. Satz 4 und 5 regeln die Einsicht in papiergebundene Akten. Grundsätzlich wird hier Akteneinsicht durch das Bereitstellen der Akte zur Einsichtnahme in den Diensträumen der Polizei gewährt. Nur auf besonderen Antrag kann die Einsicht durch Übersendung von Kopien, durch Übergabe zur Mitnahme oder durch Übersendung der Akten gewährt werden. Die Übersendung von Kopien soll immer dann erfolgen, wenn die Gefahr der nachträglichen Veränderung von Akteninhalten nicht ausgeschlossen werden kann.

Absatz 6

Die Vorschrift ist darauf zugeschnitten, dass die Aktenführung bei der Polizei zukünftig elektronisch erfolgen soll. Künftig kommt es nicht mehr entscheidend darauf an, dass die Akten räumlich getrennt aufzubewahren sind. Entscheidend ist vielmehr, dass die die wissenschaftliche Forschung betreibende Stelle gewährleisten muss, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind und die hierfür notwendigen technischen und organisatorischen Maßnahmen zu treffen hat.

Zu Nr. 21 (§ 25b [neu] Weiterverarbeiten von Daten zur Aus- und Fortbildung sowie und zu statistischen Zwecken)

Absatz 1

Der Satz 4 bestimmt, dass personenbezogene Daten aus besonders eingriffsintensiven Maßnahmen nicht zu Aus- und Fortbildungszwecken verarbeitet oder übermittelt werden dürfen.

Zu Nr. 22 (§ 26)

Buchstabe a)

Es handelt sich um eine redaktionelle Änderung.

Buchstabe b)

Mit der Änderung erfolgt eine Harmonisierung mit den Regelungen des Bundeszentralregistergesetzes. Das Bundesrecht (vgl. § 10 Absatz 5 BKAG, § 25 Absatz 5 BKAG [neu]) enthält vergleichbare Regelungen.

Zu Nr. 23 (§ 27)

Buchstabe a)

Es handelt sich um eine Anpassung an den in § 12 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt verwandten Begriff „Benachrichtigung“.

Buchstabe b)

Die Einfügung des neuen Absatzes 3a soll zur Klarstellung eine ausdrückliche korrespondierende landesrechtliche Grundlage für die Akteneinsicht durch Mitglieder 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 - CPT) oder der Länderkommission der Nationalen Stelle zur Verhütung von Folter schaffen.

Die Einrichtung der Nationale Stelle geht auf das Fakultativprotokoll zu dem Übereinkommen der Vereinten Nationen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe (CAT) vom 10. Dezember 1984 zurück. Das Fakultativprotokoll (auch OPCAT genannt) vom 18. Dezember 2002 sieht in Artikel 3 die Einrichtung nationaler Mechanismen zur Verhütung von Folter vor, die die Arbeit des neu geschaffenen Unterausschusses für Prävention (SPT) ergänzen sollen. Deutschland hat das Zusatzprotokoll am 20. September 2006 unterzeichnet und mit Zustimmungsgesetz vom 26. August 2008 (BGBl. II 2008, Nr. 23) in innerstaatliches Recht umgesetzt. Mit Organisationserlass des Bundesministeriums der Justiz vom 20. November 2008 (Bundesanzeiger Nr. 182, S. 4277) wurde die Bundesstelle zur Verhütung von Folter geschaffen. Die Bundesstelle hat am 1. Mai 2009 ihre Arbeit aufgenommen.

Die Länderkommission zur Verhütung von Folter wurde mit Staatsvertrag über die Einrichtung eines nationalen Mechanismus aller Länder nach Artikel 3 des Fakultativprotokolls vom 18. Dezember 2002 zu dem Übereinkommen der Vereinten Nationen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behand-

lung oder Strafe vom 25. Juni 2009 (u.a. abgedruckt in GBl. BW vom 7. Dezember 2009, S. 681) eingerichtet. Am 24. September 2010 wurde die Länderkommission zur Verhütung von Folter offiziell vom Hessischen Minister der Justiz, für Integration und Europa in ihr Amt eingeführt.

Zu Nr. 24 (§ 27a)

Buchstabe a)

Der in der bestehenden Regelung in Bezug genommene Rahmenbeschluss 2006/960/JI des Rates der EU wurde durch die Richtlinie (EU) 2016/680 aufgehoben. Daher ist diese Regelung zu streichen.
Als Strafverfolgungsbehörden der Mitgliedstaaten im Sinne des § 27a können insbesondere jene Stellen gelten, die von diesem Staat gemäß Artikel 2 Buchstabe a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15.3.2007, S. 26) benannt wurden.

Buchstaben b) und c)

Es handelt sich um redaktionelle Änderungen.

Zu Nr. 25 (§ 28 Absatz 3 [neu])

Buchstabe a)

Mit dem neuen Absatz 3 wird eine ausdrückliche gesetzliche Regelung zum Zweck der Übermittlung personenbezogener Daten an nicht öffentliche Beratungsstellen geschaffen. Das Verfahren war bisher ausschließlich in Verwaltungsvorschriften geregelt. Für eine zielgerichtete (aufsuchende) Beratung von Opfern von Straftaten oder Personen, die aufgrund tatsächlicher Anhaltspunkte Opfer von Straftaten werden könnten, ist es erforderlich, personenbezogene Daten, die für eine - auch kurzfristige - Kontaktaufnahme geeignet sind (z. B. Anschrift des Aufenthaltsorts, Telefonnummer, E-Mail-Adresse) an Beratungsstellen zu übermitteln. Die Beratungsangebote werden zumeist durch Vereine unterbreitet. Die Anforderungen an die Einwilligung der betroffenen Person ergeben sich aus § 7 DSUG LSA. Von einer Einwilligung kann abgesehen werden, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies in Interesse der Person liegt und sie in Kenntnis des Zwecks einwilligen würde. Die tatsächlichen Anhaltpunkte sind aktenkundig zu machen; dies ergibt sich bereits aus den allgemeinen Grundsätzen zur Dokumentation behördlichen Handels und bedarf daher keiner ausdrücklichen gesetzlichen Regelung.

Buchstabe b)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 26 (§ 29 Datenübermittlungen zum Zweck von Zuverlässigkeitsüberprüfungen [neu])

Zuverlässigkeitsüberprüfungen sind teilweise gesetzlich geregelt. Beispiele hierfür sind das Luftsicherheitsgesetz sowie die Sicherheitsüberprüfung nach den Sicherheitsüberprüfungsgesetzen des Bundes und der Länder. Die Notwendigkeit, die Zuverlässigkeit festzustellen, ergibt sich jedoch in zahlreichen weiteren Fällen, in denen die Überprüfungen mangels ausdrücklicher gesetzlicher Regelung bisher allein auf die informierte Einwilligung der betroffenen Personen gestützt wurden. Es geht dabei um den Schutz von Veranstaltungen, den Schutz von Behörden oder anderen gefährdeten Objekten sowie die Einstellung in den Polizeivollzugsdienst.

Die Richtlinie (EU) 2016/680 sieht im Gegensatz zur Verordnung (EU) 2016/679 nicht ausdrücklich die Datenverarbeitung auf der Grundlage einer informierten Einwilligung vor. Nach dem Erwägungsgrund 35 zu dieser Richtlinie sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten zum Zweck der Verhütung von Straftaten durch die zuständigen Behörden darstellen. Allen oben beschriebenen Zuverlässigkeitsüberprüfungen liegt auch die Verarbeitung personenbezogener Daten zugrunde, die die Polizei aus strafrechtlichen Ermittlungen gewonnen hat und die nach § 23 [neu] zur vorbeugenden Bekämpfung von Straftaten oder Vorsorge für die Verfolgung von Straftaten im Informationssystem der Polizei (vergleiche § 13c [neu]) gespeichert werden. Insoweit ist es zur Umsetzung der Richtlinie (EU) 2016/680 erforderlich, diese bisher ausschließlich auf eine informierte Einwilligungserklärung gestützte Datenverarbeitung durch die Polizei gesetzlich zu regeln. Dies schließt nicht aus, dass eine entsprechende Rechtsvorschrift vorsieht, dass die betroffene Person der Verarbeitung personenbezogener Daten zustimmen kann (vergleiche Erwägungsgrund 35 zur Richtlinie (EU) 2016/680).

Absatz 1

Absatz 1 regelt, dass eine Zuverlässigkeitsüberprüfung nur auf der Grundlage einer Einwilligung erfolgen kann. Die Anforderungen, die an eine Einwilligung zu stellen sind, ergeben sich aus § 7 des Entwurfes für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt. Zum Zweck einer Zuverlässigkeitsüberprüfung dürfen die personenbezogenen Daten der betroffenen Person mit den im Informationssystem der Polizei des Landes Sachsen-Anhalt gespeicherten oder im polizeilichen Informationsverbund zwischen Bund und Ländern zum Abruf durch die Polizei bereitstehenden personenbezogenen Daten weiterverarbeitet (abgeglichen) werden. Die Befugnis schließt die Erhebung personenbezogener Daten allein zum Zweck der Durchführung der Zuverlässigkeitsüberprüfung - mit Ausnahme der in Satz 2 beschriebenen personenbezogenen Daten - aus.

§ 23 Absatz 5 [neu] sichert, dass bestimmte strafprozessuale Entscheidungen in die Zuverlässigkeitsüberprüfung nicht einbezogen werden, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

Absatz 2

Nummer 1 gestattet Zuverlässigkeitsüberprüfungen zum Schutz von Veranstaltungen. Zulässig ist die Maßnahme nur, wenn es sich um eine besonders gefährdete Veranstaltung handelt. Musterbeispiel hierfür ist die Fußball-Weltmeisterschaft 2006 in Deutschland. Der betroffene Personenkreis wird durch den Begriff „privilegierter Zutritt“ eingeschränkt. Hierunter fallen insbesondere Servicepersonal und Journalisten. Nicht erfasst wird das normale Publikum bei einer öffentlichen Veranstaltung.

Nummer 2 gestattet eine Zuverlässigkeitsüberprüfung von Personen, denen ein privilegierter Zugang zu einem Amtsgebäude oder einem anderen gefährdeten Objekt eingeräumt werden soll, sofern dies aufgrund der Gefährdungslage erforderlich ist.

Nummer 3 gestattet eine Zuverlässigkeitsüberprüfung von Personen, die selbständige Dienstleistungen zur Unterstützung von Vollzugsaufgaben erbringen (z. B. Dolmetscher).

Nummer 4 gestattet eine Zuverlässigkeitsüberprüfung von Personen, die eine Einstellung in eine Laufbahn des Polizeivollzugsdienstes anstreben. Die Regelung gilt auch für Personen, die eine Einstellung in die Polizei des Bundes und der Länder anstreben und ihren Hauptwohnsitz in Sachsen-Anhalt haben.

Absatz 3

Auch bei diesen Datenübermittlungen sind die allgemeinen Regeln der Datenübermittlung des § 26 zu berücksichtigen. Besonderer Bedeutung kommt dabei § 26 Absatz 4 zu. Die Übermittlung darf nicht zu einer Erweiterung des Kreises der Stellen nach § 41 des Bundeszentralregistergesetzes führen, die von Eintragungen, die in ein Führungszeugnis nicht aufgenommen werden, Kenntnis erhalten, und muss das Verwertungsverbot im Bundeszentralregister getilgter oder zu tilgender Eintragungen nach §§ 51 und 52 des Bundeszentralregistergesetzes berücksichtigen.

Die Datenübermittlung an die nicht öffentliche Stelle muss im Falle von Erkenntnissen auf die Mitteilung beschränkt sein, dass Sicherheitsbedenken bestehen. Der Veranstalter entscheidet dann, ob er der betroffenen Person gleichwohl den privilegierten Zutritt ermöglicht, indem er ihr eine Akkreditierung erteilt oder durch sie Dienstleistungen erbringen lässt. Folgt er der Entscheidung nicht, muss er dies der Polizei unverzüglich mitteilen. Die Polizei wird dadurch in die Lage versetzt, ggf. anderweitige Maßnahmen zur Verhütung von Straftaten (z. B. die Erteilung einer Meldeauflage) zu treffen.

Zu Nr. 27 (§ 30)

Es handelt sich um eine redaktionelle Anpassung an den in § 2 Absatz 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt definierten Begriff „Dateisystem“.

Zu Nr. 28 (§ 31)

Es handelt sich um eine redaktionelle Anpassung an § 12 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt.

Zu Nr. 29 (§ 32 [neu] Anbietungspflicht)

Der bisherige § 32 wird neu strukturiert. Weiterhin erforderliche Regelungen werden beibehalten und in die §§ 32 [neu], 32a [neu] und 32b [neu] überführt. Einzelne Regelungen können aufgrund der in dem Entwurf für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt bereits enthaltenen Regelungen im SOG LSA entfallen.

Die in § 32 Absatz 2 SOG LSA enthaltene Regelung kann im SOG LSA gänzlich entfallen. Die Regelungsinhalte finden sich in § 31 Absatz 2 und Absatz 4 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt.

Die in § 32 Absatz 7 SOG LSA enthaltene Regelung kann im SOG LSA gänzlich entfallen. Die Regelungsinhalte finden sich in § 14 Absatz 3 und Absatz 4 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt sowie § 25a [neu] SOG LSA.

Die in § 32 Absatz 9 SOG LSA enthaltene Regelung zur Anbietung wird in § 32 [neu] überführt und redaktionell an den in § 2 Absatz 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt definierten Begriff „Dateisystem“ angepasst.

Zu Nr. 30 (§§ 32a bis 32c [neu])

§ 32a Aussonderungsprüffristen und Löschfristen [neu]

§ 32a nimmt im Wesentlichen den Regelungsinhalt des bisherigen § 32 Absatz 4 und 5 auf und konkretisiert die sich aus § 31 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt ergebende Verpflichtung, Lösch- bzw. Aussonderungsprüffristen vorzusehen. Zudem erfolgt eine Harmonisierung mit den Regelungen mit § 77 BKAG-neu. Weiterhin wird die bereits bestehende polizeiliche Praxis, die Beachtung der Einhaltung vergebener Aussonderungsprüffristen durch geeignete Maßnahmen technisch sicherzustellen, ausdrücklich als Anforderung normiert.

§ 32b Berichtigung personenbezogener Daten sowie Einschränkung der Verarbeitung in Akten sowie Vernichtung von Akten [neu]

Die Berichtigung personenbezogener Daten war nach dem bisherigen § 13a i. V. m. § 16 Absatz 1 DSG LSA für die Sicherheitsbehörden und die Polizei bisher einheitlich geregelt. Mit dem Inkrafttreten der Verordnung (EU) 2016/679 sind durch die Sicherheitsbehörden und die Polizei außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 für die Berichtigung sowie Einschränkung der Verarbeitung personenbezogener Daten die Verordnung (EU) 2016/679 als unmittelbar geltendes Recht anzuwenden. Die Regelungen des neuen § 32 sind daher ausschließlich durch die Polizei bei der Verarbeitung personenbezogener Daten in Akten im Anwendungsbe-

reich der Richtlinie (EU) 2016/680 anzuwenden. Sie konkretisieren die hierzu die in dem Entwurf für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt getroffenen Regelungen.

Absatz 1

Die Regelung entspricht im Wesentlichen dem bisher über § 13a anwendbaren § 16 Absatz 1 DSG LSA. Es werden begriffliche - jedoch nicht den Inhalt ändernde - Anpassungen vorgenommen sowie die Tatbestände, bei denen eine Verarbeitungseinschränkung an die Stelle einer Vernichtung tritt, an § 32 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angeglichen.

Absatz 2

Der Regelungsinhalt war bisher in § 32 Absatz 2 und 7 enthalten.

Absatz 3

Der Regelungsinhalt war bisher in § § 32 Absatz 8 enthalten.

§ 32c Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten [neu]

§ 32c trifft Sonderregelungen im Hinblick auf die Beauskunftung betroffener Personen sowie die Berichtigung, Löschung und Verarbeitungseinschränkung personenbezogener Daten im Kontext des Informationssystems der Polizei. Die Aufgabenübertragung an das Landeskriminalamt ist im Sinne der im § 79 geregelten Funktion des Landeskriminalamts.

Zu Nr. 31 (§ 109a Übergangsvorschrift für die Verarbeitung personenbezogener Daten durch die Polizei [neu])

In einer Übergangsphase ist es erforderlich, die bestehenden Datenverarbeitungssysteme der Polizei den neuen Anforderungen anzupassen. Die in § 13d [neu] normierte Kennzeichnungspflicht wird von den bestehenden Datenverarbeitungssysteme der Polizei nicht erfüllt. Dies würde bedeuten, dass diese Daten zwischenzeitlich noch nicht einmal zu Abfragezwecken verwendet werden dürften (vergleiche § 13d Absatz 2 [neu]). Um die Datenverarbeitungssysteme in ihrer Struktur, ihrem Geschäftsprozess und in ihrer Datenhaltung grundsätzlich weiter und gegebenenfalls sogar neu zu entwickeln, ist ein Übergangszeitraum erforderlich. Auch das BKAG-neu sieht in § 91 eine entsprechende Übergangsvorschrift vor.

Artikel 4 Änderung des Maßregelvollzugsgesetzes Sachsen-Anhalt

Zu Nr. 1 (Inhaltsübersicht)

Redaktionelle Anpassungen des Inhaltsverzeichnisses an die in nachfolgenden Ziffern geänderten Überschriften von datenschutzrechtlichen Regelungen.

Zu Nr. 2 (§ 3)

Inhaltliche Änderung.

Mit dem Maßregelvollzug ist, wie es § 3 Absatz 1 Satz 2 MVollzG LSA ermöglicht, die Salus gGmbH beliehen worden. Der nach § 3 Absatz 1 Satz 3 und 4 MVollzG LSA bestellte Einrichtungsleiter scheidet im Herbst 2018 aus Altersgründen aus. Die bisherige Festschreibung der Qualifikation verhindert - sofern der die Beliehene vertretende Geschäftsführer der Salus gGmbH nicht Jurist ist - eine Personalunion. Dies führt in der Praxis häufig zu Problemen. Daher soll das Qualifikationserfordernis „Richteramt“ gestrichen werden.

Zu Nr. 3 (Abschnitt 5)

Redaktionelle Anpassung.

Nach § 2 Nr. 2 DSUG LSA umfasst der Begriff der „Verarbeitung“ (von Daten) „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“

Die Verwendung der Begriffe „Datenerhebung“, „Datennutzung und „Datenübermittlung“ usw. ist daher nur noch notwendig, wenn Abgrenzungen vorzunehmen sind. Ansonsten ist der Oberbegriff „Datenverarbeitung“ zu verwenden.

Da der Abschnitt 5 mehrere Bereiche der Datenverarbeitung umfasst, wurde die Überschrift entsprechend angepasst.

Zu Nr. 4 (§ 32)

Buchstabe a)

aa) Redaktionelle Anpassung.

Der Begriff des „Erhebens“ von Daten ist nach der Begriffsbestimmung in § 2 Nr. 2 DSUG LSA (vgl. Begründung zu Nr. 3) ein Unterfall des „Verarbeitens“. Die bereits bestehende Erlaubnis zur Datenverarbeitung umfasst somit auch die Erlaubnis zur Datenerhebung, so dass Letztere gestrichen werden kann.

bb) Inhaltliche Änderungen.

Bei den in den Nr.n 8 und 9 aufgeführten Angaben handelt es sich nicht um personenbezogene Daten der untergebrachten Personen, sondern um Daten Dritter (z. B. Opfer, Verwandte, Arbeitgeber und Besucher), die mit der untergebrachten Person in Verbindung stehen.

Soweit die Daten nicht untergebrachter Personen für den Maßregelvollzug (z. B. für Entscheidungen über die Einschränkung von Kommunikationsrechten, Aufenthaltsbeschränkungen bei Vollzugslockerungen oder Maßnahmen der Ausbildung und Re-

sozialisierung gegenüber untergebrachten Personen) benötigt werden, dürfen auch sie nach den Bestimmungen des DSUG LSA verarbeitet werden.

Allerdings kann nunmehr durch die in § 28 DSUG LSA vorgesehene Kategorisierung der unterschiedlichen Betroffenheit von untergebrachten und nicht untergebrachten Personen Rechnung getragen werden.

Die Kategorisierung setzt sich im neu gefassten § 32 Absatz 2 Satz 1 MVollzG LSA fort und trägt der stärkeren Schutzbedürftigkeit personenbezogener Daten nicht untergebrachter Personen Rechnung.

Absatz 1 bezieht sich nunmehr nur noch auf personenbezogene Daten der untergebrachten Person.

Buchstabe b)

Inhaltliche Änderungen.

Absatz 2 erfasst die für den Maßregelvollzug benötigten personenbezogenen Daten nicht untergebrachter Personen und führt die mit der Änderung des Absatzes 1 begonnene Kategorisierung fort.

Zugleich erfolgt über Satz 1 eine strukturelle Berichtigung, da die bisherige Fassung von Absatz 1 Satz 2 einen Widerspruch enthielt. Bisher wurde der dort aufgestellte Grundsatz, dass „Daten über die untergebrachte Person“ erhoben, in der Behandlungsakte organisiert/geordnet und verarbeitet werden, mit den nach Satz 3 Nrn. 8 und 9 aufgeführten personenbezogenen Daten Dritter aufgeweicht.

Satz 2 soll die Qualität der über nicht untergebrachte Personen erhobenen Daten verbessern, da sie der untergebrachten Person oftmals nicht im benötigten Umfang bekannt sind. Andererseits wird eine darüber hinausgehende Ermittlungstätigkeit der Einrichtung auf Ausnahmefälle beschränkt. Die Datenerhebung bei der betroffenen Person erleichtert zudem die Erfüllung der in § 12 DSUG LSA beschriebenen Benachrichtigungspflichten.

Über die in Satz 3 enthaltene Verpflichtung, personenbezogene Daten von Dritten in einem gesonderten Teil der Behandlungsakte zu führen, wird zum Einen sichergestellt, dass keine „Nebenakte“ zur Behandlungsakte geführt wird, zum Anderen erleichtert diese Organisationsform die Umsetzung der Löschungsverpflichtung nach § 37 MVollzG LSA bzw. nach § 38 MVollzG LSA i. V. m. §§ 3 Nr. 5, 14 Absatz 2 DSUG LSA.

Buchstabe c)

Durch die Einfügung des Absatzes 2 verschiebt sich die Nummerierung des nachfolgenden Absatzes.

aa) Redaktionelle Anpassungen.

Die Regelung dient der Umsetzung des Auskunftsrechtes nach § 13 DSUG LSA.

Von der Datenverarbeitung in den Einrichtungen des Maßregelvollzugs ist nicht nur der in der bisherigen Fassung der Vorschrift benannte Personenkreis umfasst. Im Einzelfall können auch personenbezogene Daten weiterer Personen, z. B. von ehemaligen Arbeitgebern, verarbeitet werden. Insofern war der Kreis der auskunftsberechtigten Personen umfassender zu beschreiben.

Das Auskunftsrecht nach § 13 DSUG LSA ist nicht auf die „zur Person verarbeiteten Daten“ und die Einsichtnahme in die Behandlungsakte beschränkt, so dass der Umfang der Auskunftsrechte entsprechend anzupassen war.

Zudem erfolgte eine sprachliche Korrektur, da z. B. Besuchende keinen Anspruch auf Einsicht in die komplette Behandlungsakte der besuchten untergebrachten Person haben.

bb) Redaktionelle Anpassung.

Das nach § 13 Absatz 1 DSUG LSA bestehende Auskunftsrecht der betroffenen Person kann nach den Bestimmungen des Absatzes 4 eingeschränkt werden. Einschränkungen sind nicht nur hinsichtlich des Umfang des Auskunftsrechtes („soweit“), sondern nun nach § 13 Absatz 4 i. V. m. § 12 Absatz 2 DSUG LSA auch hinsichtlich der Dauer der Einschränkung („solange“) zulässig.

Durch den in § 38 aufgenommenen Verweis auf das ergänzend geltende DSUG LSA wird sichergestellt, dass der Verantwortliche seinen Pflichten nach § 13 Absatz 6 und 7 DSUG LSA nachzukommen hat.

Zu Nr. 5 (§ 33)

Buchstabe a)

Redaktionelle Anpassung.

Die optisch-elektronische Beobachtung ist Voraussetzung für die Anfertigung von Bildaufzeichnungen. Beides erfolgt mit technischen Mitteln.

Eine akustische Überwachung mit technischen Mitteln, die die Möglichkeit der Anfertigung von Tonaufzeichnungen eröffnet, ist in den Einrichtungen des Maßregelvollzugs aktuell nicht möglich. Sie ist auch für die Zukunft nicht vorgesehen.

Die optisch-elektronische Beobachtung wird regelmäßig über Kameras durchgeführt, die dabei entstehenden Bilder werden unmittelbar Monitore wiedergegeben. Die technische Möglichkeit, die wiedergegebenen Bilder auch aufzuzeichnen und bei Bedarf zu verarbeiten, stellt einen noch über die optisch-elektronische Beobachtung hinausgehenden Eingriff in die Persönlichkeitsrechte der untergebrachten Personen dar, so dass in Übereinstimmung mit § 3 Ziffern 2, 3 und 5 DSUG LSA gesonderte Regelungen hierfür erforderlich bleiben.

Der Unterscheidung der beiden technischen Möglichkeiten und die unterschiedliche Eingriffstiefe wird nun bereits in der Überschrift Rechnung getragen.

Buchstabe b)

aa) Redaktionelle Anpassung.

Es handelt sich um eine Folgeänderung aus den Gründen zu Buchstabe a).

bb) Redaktionelle Anpassung.

Zum einen wird eine begriffliche Klarstellung vorgenommen. Zum anderen wird in Übereinstimmung mit den Begriffsdefinitionen in § 2 Nr. 2 DSUG LSA neben der Löschung der Bildlaufzeichnungen auch die praktisch denkbare Vernichtung des entsprechenden Datenträges ermöglicht.

cc) Redaktionelle Anpassung.

Da auch die Datennutzung nach § 2 Nr. 2 DSUG LSA unter den Begriff der (Daten)Verarbeitung zu subsumieren ist, wurden mit der Streichung der Worte „und Nutzung“ die verwendeten Begrifflichkeiten angepasst.

Buchstabe c)

Redaktionelle Anpassung.

Es erfolgte eine begriffliche Klarstellung.

Buchstabe d)

Redaktionelle Anpassung.

Es werden Begrifflichkeiten eindeutiger dargestellt.

Zu Nr. 6 (§ 34)

Buchstabe a)

Redaktionelle Anpassung.

Der Begriff der „Datennutzung“/„Nutzung von Daten“ wird im DSUG LSA nicht definiert oder im weiteren Text angeführt.

Der gewählte Begriff des „Verwendens“ der Daten, wie in der Begriffsbestimmung zur „Verarbeitung“ in § 2 Nr. 2 DSUG LSA dargelegt, kommt dem Inhalt der Regelungen in diesem Paragrafen am Nächsten.

Buchstabe b)

aa) Redaktionelle Anpassung.

Folgeänderung entsprechend der in Buchstabe a).

bb) Redaktionelle Anpassung.

Folgeänderung entsprechend der in Buchstabe a).

Buchstabe c)

aa) Redaktionelle Anpassungen.

Die bisherige Einschränkung der Regelungen in § 34 Absatz 2 MVollzG LSA auf „gespeicherte“ personenbezogenen Daten ist nicht nachvollziehbar. In der derzeitigen Praxis des Maßregelvollzugs werden sowohl „papiergebundene“ als auch „elektronische“ Daten verarbeitet. Da zwar in § 2 Nrn. 8 und 9 DSUG LSA bestimmte Manifestationen der personenbezogenen Daten definiert werden („Dateisystem“ bzw. „Akte“), sie aber hinsichtlich ihrer Verarbeitung nicht differenziert behandelt werden, wurde die Einschränkung aufgehoben.

Bei den weiteren Änderungen handelt es sich um Anpassung der bisherigen Begrifflichkeiten an die in § 2 Nr. 2 DSUG LSA verwendeten Begriffe (siehe auch Begründung zu Ziffer 3. Die Begriffe des „Einsehens“ oder „Mitteilens“ werden nicht mehr verwendet. Vielmehr bezeichnet der Begriff der (Daten)Verarbeitung den Unterfall der (Daten)Verwendung und als weiteren Unterfall die „Offenlegung“ von Daten, was „durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung“ erfolgen kann. Die gewählten Begriffe des „Verwendens“ bzw. „Bereitstellens“ von Daten kommen dem Inhalt der Regelungen in diesem Paragrafen am Nächsten.

bb) Redaktionelle Anpassung

Es handelt sich um Folgeänderungen zu Buchstabe aa).

Zu Nr. 7 (§ 35)

Buchstabe a)

Redaktionelle Anpassung.

Nach § 2 Nr. 2 DSUG LSA umfasst der Begriff der „Datenverarbeitung“ die „Datenerhebung“.

Buchstaben b) und c)

Folgeänderungen zu Buchstabe d)

Buchstabe d)

Inhaltliche Änderungen.

Mit Ziffer 13 wird der Einrichtungsleitung die Befugnis eingeräumt, personenbezogene Daten hinsichtlich des Beginns, der Unterbrechung und der Beendigung des Maßregelvollzugs gegenüber dem Landeskriminalamt offen zu legen. Bislang fehlte die nach § 13 Absatz 6 Bundeskriminalamtgesetz (BKAG) erforderliche korrespondierende Regelung im MVollzG LSA. Der Umfang der offen zu legenden Daten ent-

spricht der Formulierung in § 13 Absatz 1 Satz 3 BKAG. Entsprechend der Gesetzesbegründung der Bundesregierung (BT-Drs. 13/1550, Begründung zu § 13 Absatz 1 Satz 3) zählen Vollzugslockerungen als Unterbrechungen des Maßregelvollzugs, wobei aus Praktikabilitätsgründen nur die Tatsache der grundsätzlichen Gewährung sowie ihres Widerrufs mitgeteilt werden müssen.

Zu Nr. 8 (§ 36)

Inhaltliche Änderung und redaktionelle Anpassung.

Mit der Neufassung der Regelungen wird auf die Benennung der Empfänger der Daten verzichtet, da auch von den Beschäftigten der Einrichtungen des Maßregelvollzugs geforscht wird und für diese keine anderen Verarbeitungsregelungen gelten sollten.

Der Bezug auf das SGB X ist nach aktuellen Überlegungen nicht sachgerecht, da sich die Forschung nicht nur auf Inhalte der Sozialgesetzbücher bezieht (z. B. auch in Richtung „Kriminalistik“). Soweit im Rahmen des Maßregelvollzugs personenbezogene Daten in archivarischer, wissenschaftlicher und statistischer Form verarbeitet werden, enthält § 6 DSUG LSA eine spezifische Norm, auf die daher verwiesen wird.

Zu Nr. 9 (§ 37)

Buchstabe a)

Redaktionelle Anpassungen.

Das DSUG LSA unterscheidet hinsichtlich der Verarbeitung nicht zwischen personenbezogenen Daten in elektronischer Form und solchen in Papierform. Darüber hinaus werden einheitliche „Aufbewahrungsfristen“ für sachgerecht erachtet.

Zudem wird in Übereinstimmung mit den Begriffsdefinitionen in § 2 Nr. 2 DSUG LSA neben der Löschung der Daten auch ihre praktisch denkbare Vernichtung ermöglicht.

Buchstabe b)

Redaktionelle Anpassung.

Der bisherige Verweis auf § 84 Absatz 2 Satz 2 SGB X (lt. aktueller Fassung: „(Sozialdaten)… sind auch zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden.“) wird durch die Neufassung des § 38 MVollzG LSA (ergänzende Geltung des DSUG LSA) i. V. m. § 14, insbesondere Absatz 2, DSUG LSA obsolet.

Zu Nr. 10 (§ 38)

Inhaltliche Änderung.

Die bisherigen statischen Verweise auf Gesetzesfassungen sind nicht sachgerecht und mit der Einführung des EU-Datenschutzrechts wird der Verweis auf das SGB X nicht mehr benötigt.

Das MVollzG LSA regelt jedoch den Datenschutz nicht vollumfänglich, so dass für die Belange des Maßregelvollzugs ergänzend das DSUG LSA erforderlich ist. Für die nicht diesem Zweck unterliegende Verarbeitung personenbezogener Daten gelten die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; ABl. L 119 vom 4. Mai 2016, S. 1, L 314 vom 22. November 2016, S. 72) sowie das diese Verordnung ausfüllende Datenschutzgesetz des Landes unmittelbar, ohne dass es einer entsprechenden Regelung im MVollzG LSA bedarf.

Artikel 5 Änderung des Gesetzes zur Ausführung des Therapieunterbringungsgesetzes in Sachsen-Anhalt

Artikel 5 nimmt redaktionelle Anpassungen am Gesetz zur Ausführung des Therapieunterbringungsgesetzes in Sachsen-Anhalt vor.

Artikel 6 Einschränkung von Grundrechten

Mit den Artikeln 3 und 4 zu bereichsspezifischen Regelungen des Datenschutzes im Gesetz über die öffentliche Sicherheit und Ordnung sowie im Maßregelvollzugsgesetz wird in das durch Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes und Artikel 6 Absatz 1 Satz 1 der Landesverfassung geschützte Recht auf den Schutz personenbezogener Daten eingegriffen. Diese bereichsspezifischen Einschränkungen sind durch die Beachtung des Zitiergebots für den Gesetzgeber kenntlich zu machen.

Artikel 7 Inkrafttreten

Da die Richtlinie (EU) 2016/680 durch Gesetz zum 6. Mai 2018 umzusetzen war, sollen das DSUG LSA und die Anpassungen im bereichsspezifischen Datenschutzrecht möglichst zeitnah zu diesem Termin in Kraft treten.