

B e g r ü n d u n g

zum Gesetzentwurf 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

Allgemeiner Teil

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

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 ab 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 ist 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 wird, 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 tretenden „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 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 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 Querschnittsdatschutzrecht 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 derzeit erarbeiteten Musterentwurfs für ein Justizvollzugsdatenschutzgesetz. Dazu tagt eine vom Strafvollzugsausschuss der Länder eingesetzte länderübergreifende Arbeitsgruppe. Die bundeseinheitlichen Vorgaben sollen entweder weiterhin in Form des Abschnitts 23 oder als Justizvollzugsgesetzbuch Sachsen-Anhalt – Viertes Buch – Datenschutz im Justizvollzug (JVollzGB IV LSA) umgesetzt werden. 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, einschließlich 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 eine Polizeibehörden sind, die aber Ordnungswidrigkeiten verfolgen,

anwenden 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 Handlungsakte nach dem Maßregelvollzugsgesetz 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 regelungsideologisch 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 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.

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 Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder sie aufzuschieben. Die Vorschrift geht zum Schutz der betroffenen Person über das durch die Richtlinie (EU) 2016/680 Gebotene hinaus, indem tatbestandlich jeweils eine Gefährdung – gegenüber einer in der Richtlinie 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 weiterer 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 Geforderte 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 Richtlinienentwurf 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 Lösungsverpflichtung 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 Ergebnis 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 enthaltene 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.

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 Datenschutzrichtlinienumsetzungsgesetzes 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 Bundeskriminalamtgesetzes (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 (§ 3 Nr. 12 [neu])

Auch im SOG LSA wird, wie von der Richtlinie (EU) 2016/680 gefordert, der neue einheitliche Begriff der Verarbeitung personenbezogener Daten eingeführt. Aus rechtssystematischen Gründen und aufgrund der weiteren europarechtlichen Vorgaben kann der einheitliche Begriff der Verarbeitung im SOG LSA allerdings nicht für die Datenerhebung, die Datenübermittlung, die Einschränkung der Datenverarbeitung und das Löschen der Daten Anwendung finden. Die übrigen Aspekte der Verarbeitung wie die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung werden, dem Vorbild des Gesetzes zur Neuregelung des Bundeskriminalamtes vom 1. Juni 2017 (BGBl. I S. 1354) (im Folgenden BKAG-neu) folgend zusammenfassend als „Weiterverarbeiten“ bezeichnet. Dem § 2 DSUG LSA folgend wird der Begriff „Weiterverarbeiten“ legal definiert. Da der Begriff jedoch nur im

SOG LSA Verwendung finden soll, erfolgt die Begriffsbestimmung aus rechtssystematischen Gründen im SOG LSA.

Zu Nr. 3 (§ 4 Absatz 2 und 3 [neu])

Buchstabe a) (Absatz 2 [neu])

Die Regelung wonach das SOG LSA keine Anwendung findet, soweit das Recht der Europäischen Union, im Besonderen 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. EU L 119 vom 4.5.2016, S. 1) in der jeweils geltenden Fassung, unmittelbar gilt, hat deklaratorische Bedeutung und soll den Rechtsanwendern der Sicherheitsbehörden und der Polizei Folgendes verdeutlichen: Das SOG LSA stellt im Anwendungsbereichs 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, ist die Datenschutz-Grundverordnung als unmittelbar geltendes Recht der Europäischen Union anzuwenden.

Buchstabe b) (Absatz 3 [neu])

Für die Wahrnehmung von Aufgaben der Gefahrenabwehr durch die Sicherheitsbehörden oder die Polizei, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 bzw. des Entwurfs für ein Datenschutzrichtliniengesetz Sachsen-Anhalt fallen, ist es erforderlich, zur Verordnung (EU) 2016/679 ergänzende oder auch die Rechte der betroffenen Person einschränkende Regelungen zu treffen. Solche Regelungen sind in dem BDSG vom 30. Juni 2017 (BGBl. I S. 2097), das am 25. Mai 2018 in Kraft tritt, enthalten. Mangels vergleichbarer landesrechtlicher Regelungen werden die Regelungen des Bundes für anwendbar erklärt. Ggf. kann diese Regelung im Laufe der Fortentwicklung und vollständigen Umsetzung der EU-Datenschutzreform im Landesrecht wieder entfallen, wenn sich der Landesgesetzgeber dazu entschließt, dem Bundesrecht vergleichbare Regelungen im Datenschutzquerschnittsrecht des Landes zu verankern.

Zu Nr. 4 (§ 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. 5 (§ 12)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 6 (§ 13a Geltung des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt)

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. 7 (§§ 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 eingriffsintensiven 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 beanstanden 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 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 Zugriffsberechtigungen 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 Zugriffsberechtigungen 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 Zugriffsberechtigungen 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. 8 (§ 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. 9 (§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. 10 (§ 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. 11 (§ 17b)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 12 (§ 18)

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

Zu Nr. 13 (§ 19)

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

Zu Nr. 14 (§ 20a)

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

Zu Nr. 15 (§ 22)

Buchstabe a) (Absatz 1)

Mit der Änderung wird Absatz 1 an die Begriffsbestimmung des § 3 Nr. 12 [neu] und des § 2 Nr. 8 des Entwurfs für ein Datenschutzrichtlinienumsetzungsgesetz Sachsen-Anhalt angepasst.

Buchstabe b) (Absatz 2)

Mit der Änderung wird Absatz 2 an die Begriffsbestimmung des § 3 Nr. 12 [neu] 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. 16 (§§ 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 Nr.n 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 erforderlich 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. 17 (§ 23a [neu] Weiterverarbeiten 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. 18 (§ 23b [neu] Aufzeichnung von Telefon- und Funkgesprächen)

Es handelt sich um eine redaktionelle Anpassung.

Zu Nr. 19 (§ 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. 20 (§ 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 (MBI. 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.

Nach Satz 2 darf die Entnahme der Körperzellen nicht erzwungen werden. Satz 3 und 4 legen enge Zweckbindungen der Nutzung der Daten fest: Die entnommenen Körperzellen dürfen nur zur Feststellung des DNA-Identifizierungsmusters 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 Spureenträger 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. 21 (§ 24 Benachrichtigung beim Weiterverarbeiten personenbezogener 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. 22 (§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 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. 23 (§ 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. 24 (§ 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. 25 (§ 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 Behandlung 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. 26 (§ 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. 27 (§ 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 Anhaltspunkte sind aktenkundig zu machen; dies ergibt sich bereits aus den allgemeinen Grundsätzen zur Dokumentation behördlichen Handelns und bedarf daher keiner ausdrücklichen gesetzlichen Regelung.

Buchstabe b)

Es handelt sich um eine redaktionelle Änderung.

Zu Nr. 28 (§ 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. 29 (§ 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. 30 (§ 31)

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

Zu Nr. 31 (§ 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. 32 (§§ 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 DSGVO 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 Anwendungsbereich 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 DSGVO 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. 33 (§ 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 Resozialisierung 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 Paragraphen 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 Paragraphen 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

Die Einfügung der neuen Ziffer 13 soll die bislang fehlende landesrechtliche Grundlage für die Akteneinsicht des CPT schaffen. Sie wurde vorsorglich weit gefasst, da sich auch andere Institutionen (z. B. der UN-Ausschuss gegen Folter – Committee Against Torture, CAT) der Wahrung/Überprüfung der Menschenrechte in freiheitsentziehenden Systemen widmen und ihnen durch völkerrechtliche Übereinkommen Überprüfungsrechte eingeräumt sind, die ohne eine korrespondierende landesrechtliche Befugnis zur zweckentsprechenden Datenverarbeitung ins Leere geht.

Mit Ziffer 14 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 entspricht 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 eine korrespondierende Regelung zum DSUG LSA erforderlich ist. Für die nicht diesem Zweck unterliegende Verarbeitung personenbezogener Daten gilt, ohne dass es einer entsprechenden Regelung im MVollzG LSA bedarf, das – an die Datenschutz-Grundverordnung angepasste – DSG LSA.

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 die Landesverfassung in Artikel 6 Absatz 1 Satz 1 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 ist, sollen das DSUG LSA und die Anpassungen im bereichsspezifischen Datenschutzrecht möglichst zeitnah zu diesem Termin in Kraft treten.