

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

Artikel 1

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

Inhaltsübersicht

Kapitel 1

Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze
für die Verarbeitung personenbezogener Daten

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

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

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

Kapitel 3

Rechte der betroffenen Person

- § 11 Allgemeine Informationen zu Datenverarbeitungen
- § 12 Benachrichtigung betroffener Personen

- § 13 Auskunftspflicht
- § 14 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung
- § 15 Verfahren für die Ausübung der Rechte der betroffenen Person
- § 16 Anrufung des Landesbeauftragten für den Datenschutz
- § 17 Verfahren bei Beschwerden, die in die Zuständigkeit einer anderen Aufsichtsbehörde eines EU-Mitgliedstaats fallen

Kapitel 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

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

Kapitel 5

Datenübermittlung an Drittstaaten und an internationale Organisationen

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

Kapitel 6
Zusammenarbeit der Aufsichtsbehörden

§ 38 Gegenseitige Amtshilfe

Kapitel 7
Haftung und Sanktionen

§ 39 Schadensersatz und Entschädigung

§ 40 Strafvorschriften

Kapitel 8
Schlussbestimmungen

§ 41 Sprachliche Gleichstellung

§ 42 Einschränkung von Grundrechten

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

§ 1
Anwendungsbereich

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

1. für die

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

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

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

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

§ 2

Begriffsbestimmungen

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung,

der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Anonymisierung“ die Verarbeitung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können;
6. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;
7. „Verschlüsselung“ eine technische Maßnahme, die Daten unter Anwendung kryptographischer Verfahren in eine für Dritte unverständliche Form umwandelt, so dass diese nach dem Stand von Wissenschaft und Technik ausschließlich von einem Schlüsselinhaber wieder in eine allgemein verständliche Form überführt (entschlüsselt) werden können;
8. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
9. „Akte“ jede amtlichen, dienstlichen oder Geschäftszwecken dienende Unterlage, einschließlich Bild und Tonträger, jedoch ohne Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen; soweit die Unterlagen die in Nummer 8 festgelegten Kriterien erfüllen, können Akten auch Dateisysteme sein;
10. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

11. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
12. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
13. „Dritter“ eine natürliche oder juristische Person, Behörde oder Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiter befugt sind, die personenbezogenen Daten zu verarbeiten;
14. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;
15. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden;
16. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;
17. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

18. „besondere Kategorien personenbezogener Daten“

- a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
- b) genetische Daten,
- c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- d) Gesundheitsdaten und
- e) Daten zum Sexualleben oder zur sexuellen Orientierung;

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

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

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

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

§ 3

Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

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

Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 4

Verarbeitung besonderer Kategorien personenbezogener Daten

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

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

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

§ 5

Verarbeitung zu anderen Zwecken und gemeinsame Dateisysteme

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

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

Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können.

§ 6

Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

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

§ 7

Einwilligung

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

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

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

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

Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

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

§ 8

Verarbeitung auf Weisung des Verantwortlichen

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

§ 9

Datengeheimnis

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

§ 10

Automatisierte Einzelentscheidung

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

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

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

Kapitel 3

Rechte der betroffenen Person

§ 11

Allgemeine Informationen zu Datenverarbeitungen

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

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

§ 12

Benachrichtigung betroffener Personen

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

1. die in § 11 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

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

1. die Erfüllung der in § 1 genannten Aufgaben,
2. die öffentliche Sicherheit oder
3. Rechtsgüter Dritter

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

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

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

§ 13

Auskunftsrecht

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

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,

4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,
5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,
7. das Recht nach § 16, den Landesbeauftragten für den Datenschutz anzurufen, sowie
8. Angaben zur Erreichbarkeit des Landesbeauftragten für den Datenschutz.

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

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

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

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

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

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über den Landesbeauftragten für den Datenschutz ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 16 den Landesbeauftragten für den Datenschutz anrufen oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Der Landesbeauftragte für den Datenschutz hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung des Landesbeauftragten für den Datenschutz an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. Der Landesbeauftragte für den Datenschutz hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

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

§ 14

Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In

diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

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

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

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,
2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 1 dienen, weiter aufbewahrt werden müssen oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

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

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

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

(6) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen

der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche Empfänger, denen die Daten übermittelt werden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

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

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

§ 15

Verfahren für die Ausübung der Rechte der betroffenen Person

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

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

(3) Die Erteilung von Informationen nach § 11, die Benachrichtigungen nach den §§ 12 und 22 und die Bearbeitung von Anträgen nach den §§ 13 und 14 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 13 und 14 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrages belegen können.

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

§ 16

Anrufung des Landesbeauftragten für den Datenschutz

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

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

§ 17

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

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

Kapitel 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 18

Auftragsverarbeitung

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

Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

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

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

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

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

2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;
4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;
5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 32 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;
6. Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;
7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
8. alle gemäß § 20 erforderlichen Maßnahmen ergreift und
9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 20 bis 23 und § 25 genannten Pflichten unterstützt.

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

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

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

§ 19

Gemeinsam Verantwortliche

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

§ 20

Anforderungen an die Sicherheit der Datenverarbeitung

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

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

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

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

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschsens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
9. Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit). Ein Zweck nach den Nummern 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 21

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

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

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

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

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,
2. den Namen und die Kontaktdaten des Landesbeauftragten für den Datenschutz oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

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

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

(7) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314

vom 22.11.2016, S. 72) oder eine Benachrichtigung nach Artikel 34 Abs. 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

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

§ 22

Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

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

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

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

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

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

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

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

§ 23

Durchführung einer Datenschutz-Folgenabschätzung

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

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

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

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

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

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

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

§ 24

Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz

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

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

§ 25

Anhörung des Landesbeauftragten für den Datenschutz

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

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

2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.

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

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

1. die nach § 23 durchgeführte Datenschutz-Folgenabschätzung,
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,
4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5. Name und Kontaktdaten des Landesbeauftragten für den Datenschutz.

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

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

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

§ 26

Verzeichnis von Verarbeitungstätigkeiten

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

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten des Landesbeauftragten für den Datenschutz,
2. die Zwecke der Verarbeitung,
3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. gegebenenfalls die Verwendung von Profiling,
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7. Angaben über die Rechtsgrundlage der Verarbeitung,
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und

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

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

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

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Landesbeauftragten für den Datenschutz,
2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und
3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 20.

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

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

§ 27

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den

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

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

§ 28

Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

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

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,
2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,
3. verurteilte Straftäter,
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

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

§ 29

Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

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

§ 30

Verfahren bei Übermittlungen

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

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

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 31

Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

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

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

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

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

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

(5) Vor der Löschung nach Absatz 2 Nrn. 2 und 3 ist die Übermittlung personenbezogener Daten an das zuständige Archiv zulässig, wenn das Archiv die Daten für archivwürdig hält und es die Aufbewahrung im Interesse der historischen Forschung oder zur Rechtesicherung für geboten erachtet.

§ 32

Protokollierung

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

1. Erhebung,
2. Veränderung,
3. Abfrage,

4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. Löschung.

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

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

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

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

§ 33

Vertrauliche Meldung von Verstößen

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

Kapitel 5

Datenübermittlungen an Drittstaaten und an internationale Organisationen

§ 34

Allgemeine Voraussetzungen

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

1. die Stelle oder internationale Organisation für die in § 1 genannten Zwecke zuständig ist und
2. die Europäische Kommission gemäß Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

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

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine gegenwärtige und erhebliche Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

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

zulässig wäre. Die Zuständigkeit für die Entscheidung über die Erteilung der Genehmigung kann abweichend geregelt werden.

§ 35

Datenübermittlung bei geeigneten Garantien

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

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

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

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

§ 36

Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 34 Abs. 1 Nr. 2 kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 35 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 34 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,

2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in § 1 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 1 genannten Zwecken.

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

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

§ 37

Sonstige Datenübermittlung an Empfänger in Drittstaaten

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

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 34 Abs. 1 Nr. 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

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

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

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

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

Kapitel 6

Zusammenarbeit der Aufsichtsbehörden

§ 38

Gegenseitige Amtshilfe

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

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

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

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

(4) Der Landesbeauftragte für den Datenschutz hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen

nachzukommen. Er hat im Fall des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

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

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

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

Kapitel 7

Haftung und Sanktionen

§ 39

Schadensersatz und Entschädigung

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

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

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

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

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

§ 40

Strafvorschriften

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

Kapitel 8

Schlussbestimmungen

§ 41

Sprachliche Gleichstellung

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

§ 42

Einschränkung von Grundrechten

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

Artikel 2

Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt

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

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

Artikel 3

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

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

1. Die Inhaltsübersicht wird wie folgt geändert:

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

„§ 13a Geltung des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt“.

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

„§ 13b Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

§ 13c Informationssystem der Polizei

§ 13d Kennzeichnung personenbezogener Daten

§ 13e Regelung von Zugriffsberechtigungen für das Informationssystem der Polizei

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

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

„§ 22 Grundsätze des Datenweiterverarbeitens

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

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

§ 23b Aufzeichnung von Telefon- und Funkgesprächen“.

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

„§ 23c Ermittlung des Aufenthaltsorts gefährdeter Personen

§ 23d Speicherung von DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren“.

e) Die Angabe zu § 24 erhält folgende Fassung:

„§ 24 Benachrichtigung beim Weiterverarbeiten personenbezogener Daten von Kindern“.

f) Die Angabe zu § 25 erhält folgende Fassung:

„§ 25 Weiterverarbeiten für die wissenschaftliche Forschung“.

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

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

h) Die Angabe zu § 29 erhält folgende Fassung:

„§ 29 Datenübermittlungen zum Zweck von Zuverlässigkeitsüberprüfungen“.

i) Die Angabe zu § 32 erhält folgende Fassung:

„§ 32 Anbietungspflicht“.

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

„§ 32a Aussonderungsprüffristen und Löschfristen

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

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

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

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

2. § 3 wird wie folgt geändert:

a) In Nummer 11 wird das Wort „Ein“ durch das Wort „ein“ und der Punkt am Ende durch ein Semikolon ersetzt.

b) Nach Nummer 11 wird folgende Nummer 12 angefügt:

„12. Weiterverarbeiten:

jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, den Abgleich, die Verknüpfung.“

3. § 4 wird wie folgt geändert:

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

„(2) Die Vorschriften dieses Gesetzes finden keine Anwendung, 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. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72) in der jeweils geltenden Fassung, unmittelbar gilt.“

b) Nach Absatz 2 wird folgender Absatz 3 angefügt:

„(3) Bei der Verarbeitung personenbezogener Daten im Rahmen der Wahrnehmung von Aufgaben der Gefahrenabwehr durch die Sicherheitsbehörden oder die Polizei, die nicht in den Anwendungsbereich des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt fallen, sind die Vorschriften der §§ 27 bis 29 und 32 bis 36 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) anzuwenden.“

c) Der bisherige Absatz 2 wird Absatz 4.

4. In § 6 Abs. 3 werden nach dem Wort „Rasse,“ die Wörter „seiner Ethnie,“ und nach dem Wort „Anschauungen“ die Wörter „, seiner Gewerkschaftszugehörigkeit“ eingefügt.
5. In § 12 Abs. 4 Satz 4 wird die Angabe „§§ 25 und 32 Abs. 7 bis 9“ durch die Angabe „§§ 25, 25a und 32 Abs. 9“ ersetzt.¹
6. § 13a erhält folgende Fassung:

„§ 13a

Geltung des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt

Bei der Verarbeitung personenbezogener Daten durch

1. die Polizei zum Zweck

a) der Verhütung, Erforschung, Verfolgung oder Ahndung von Straftaten einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (straftatenbezogene Gefahrenabwehr) oder

b) der Erforschung, Verfolgung, Ahndung oder Vollstreckung von Ordnungswidrigkeiten

oder

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

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

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

„§ 13b

Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung

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

1. zur Erfüllung derselben Aufgabe und

2. zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten.

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

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

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

1. mindestens

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

2. sich im Einzelfall

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

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

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

(4) Abweichend von Absatz 2 kann die Polizei die vorhandenen Grunddaten (§ 23 Abs. 2 Nr. 1 Buchst. a) weiterverarbeiten, um diese Person zu identifizieren.

(5) Beim Weiterverarbeiten von personenbezogenen Daten stellt die verantwortliche Polizeibehörde durch organisatorische und technische Vorkehrungen sicher, dass die Absätze 1 bis 4 beachtet werden.

§ 13c

Informationssystem der Polizei

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

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

§ 13d

Kennzeichnung personenbezogener Daten

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

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

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

(2) Personenbezogene Daten, die nicht entsprechend den Anforderungen des Absatzes 1 gekennzeichnet sind, dürfen so lange nicht weiterverarbeitet oder übermittelt

werden, bis eine Kennzeichnung entsprechend den Anforderungen des Absatzes 1 erfolgt ist.

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

§ 13e

Regelung von Zugriffsberechtigungen für das Informationssystem der Polizei

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

1. auf Grundlage der nach § 13d Abs. 1 vorzunehmenden Kennzeichnungen die Vorgaben des § 13b bei der Nutzung des Informationssystems beachtet werden und
2. der Zugriff nur auf diejenigen personenbezogenen Daten und Erkenntnisse möglich ist, deren Kenntnis für die Erfüllung der jeweiligen dienstlichen Pflichten erforderlich ist.

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

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

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

§ 13f

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

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

8. § 15 wird wie folgt geändert:

a) In Absatz 4 Satz 3 werden die Wörter „Die Verarbeitung oder Nutzung“ durch die Worte „Das Weiterverarbeiten“ ersetzt.

b) Absatz 7 wird wie folgt geändert:

aa) Die Sätze 3 und 4 werden aufgehoben.

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

9. § 16 wird wie folgt geändert:

a) Absatz 5 erhält folgende Fassung:

„(5) Die Aufzeichnungen sind nach Ablauf des Zeitraumes, der für die Feststellung ausreicht, ob die Aufzeichnungen im Sinne des Satzes 3 benötigt werden, zu löschen. Im Übrigen sind Bild- und Tonaufzeichnungen, in einem Dateisystem gespeicherte personenbezogene Daten spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten. Dies gilt nicht, wenn die Daten zur Verfolgung von Straftaten benötigt werden oder tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. In den in Satz 3 genannten Fällen müssen personenbezogene Daten unbeteiligter Personen gelöscht oder unkenntlich gemacht werden, soweit dies ohne unverhältnismäßig hohen Aufwand möglich ist. § 15 Abs. 7 Satz 3 Halbsatz 2 gilt entsprechend. Die §§ 25 und 25a bleiben unberührt.“

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

10. § 17 wird wie folgt geändert:

a) In Absatz 2 Satz 5 wird die Angabe „§ 15 Abs. 7 Satz 5 Halbsatz 2“ durch die Angabe „§ 15 Abs. 7 Satz 3“ ersetzt.

b) Absatz 4e wird aufgehoben.

c) Absatz 7 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ ersetzt.

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

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

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

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

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

15. § 22 wird wie folgt geändert:

a) In Absatz 1 werden die Wörter „Dateien speichern, verändern oder nutzen“ durch die Wörter „Dateisystemen weiterverarbeiten“ ersetzt.

b) Absatz 2 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „speichern, verändern oder nutzen“ durch das Wort „weiterverarbeiten“ ersetzt.

bb) In Satz 2 werden die Wörter „Speichern, Verändern oder Nutzen“ durch das Wort „Weiterverarbeiten“ ersetzt.

c) Absatz 3 erhält folgende Fassung:

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

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

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

d) Absatz 4 wird aufgehoben.

e) Absatz 5 erhält folgende Fassung:

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

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

16. § 23 erhält folgende Fassung:

„§ 23

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

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

1. Verurteilten,
2. Beschuldigten,
3. Personen, die einer Straftat verdächtig sind, sofern das Weiterverarbeiten der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und

4. Personen, bei denen Anlass zum Weiterverarbeiten der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).

(2) Die Polizei kann weiterverarbeiten:

1. von Personen nach Absatz 1 Nrn. 1 bis 4
 - a) die Grunddaten wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Anschrift und
 - b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale,
 - c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,
 - d) die Tatzeiten und Tatorte,
 - e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten;
2. von Personen nach Absatz 1 Nrn. 1 und 2 weitere personenbezogene Daten, soweit das Weiterverarbeiten der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind;
3. von Personen nach Absatz 1 Nrn. 3 und 4 weitere personenbezogene Daten.

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

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

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

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

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

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

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

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

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

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

wurde, dass die betreffende Person die Voraussetzungen nach Absatz 6 oder Absatz 7 erfüllt.“

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

„§ 23a

Weiterverarbeiten von personenbezogenen Daten, die von Strafverfolgungsbehörden der Mitgliedstaaten der europäischen Union an die Polizei übermittelt worden sind

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

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

a) In Satz 3 wird das Wort „sperren“ durch die Wörter „in der Verarbeitung einzuschränken“ ersetzt.

b) Satz 4 erhält folgende Fassung:

„Die §§ 25, 25a und 32 Abs. 9 bleiben unberührt.“

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

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

„§ 23d

Speicherung von DNA-Identifizierungsmustern
zur Erkennung von DNA-Trugspuren

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

1. mittels eines Mundschleimhautabstrichs oder einer hinsichtlich ihrer Eingriffsintensität vergleichbaren Methode Körperzellen entnehmen,

2. diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen und
3. die festgestellten DNA-Identifizierungsmuster mit den an Spurenmaterial festgestellten DNA-Identifizierungsmustern automatisiert abgleichen, um zur Erkennung von DNA-Trugspuren festzustellen, ob an Spurenmaterial festgestellte DNA-Identifizierungsmuster von diesen Personen stammen.

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

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

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

21. § 24 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 24

Benachrichtigung beim Weiterverarbeiten von personenbezogener Daten von Kindern.“

b) Absatz 1 wird aufgehoben.

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

d) In Satz 1 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ ersetzt.

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

22. § 25 erhält folgende Fassung:

„§ 25

Weiterverarbeiten für die wissenschaftliche Forschung

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

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

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

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

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

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

Verpflichtungsgesetzes findet auf die Verpflichtung zur Geheimhaltung entsprechende Anwendung.

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

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

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

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

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

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

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

24. § 26 wird wie folgt geändert:

a) In Absatz 1 Satz 2 Halbsatz 2 wird das Wort „Abrufverfahren“ durch die Wörter „Verfahren auf Abruf“ ersetzt.

- b) In Absatz 4 wird die Angabe „§ 41“ durch die Angabe „§§ 41 und 61“ und die Angabe „§§ 51 und 52“ durch die Angabe „§§ 51, 52 und 63“ ersetzt.

25. § 27 wird wie folgt geändert;

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

„(3a) Die Polizei kann personenbezogene Daten einschließlich nicht gefahren- oder tatbezogener persönlicher Merkmale von Personen, die nach diesem Gesetz oder anderen Rechtsvorschriften von ihr festgehalten werden, an Stellen, die aufgrund völkerrechtlicher Übereinkommen zur Überprüfung der Einhaltung der Rechte festgehaltener Personen zuständig sind, übermitteln.“

26. § 27a wird wie folgt geändert:

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

27. § 28 wird wie folgt geändert:

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

„(3) Die Polizei kann personenbezogene Daten, die der Kontaktaufnahme zu einer Person dienen, zum Zweck der persönlichen Beratung dieser Person an nichtöffentliche Stellen übermitteln, wenn die betroffene Person oder ein Sorgeberechtigter in Kenntnis des Zwecks der Datenübermittlung eingewilligt hat oder tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies im Interesse der Person liegt und sie in Kenntnis des Zwecks einwilligen würde.“b) Der bisherige Absatz 3 wird Absatz 4.

28. § 29 erhält folgende Fassung:

„§ 29

Datenübermittlungen zum Zweck von Zuverlässigkeitsüberprüfungen

(1) Die Polizei kann auf der Grundlage der Einwilligung einer betroffenen Person ihre im Informationssystem der Polizei des Landes Sachsen-Anhalt gespeicherten oder im

polizeilichen Informationsverbund zwischen Bund und Ländern zum Abruf durch die Polizei bereitstehenden personenbezogenen Daten zum Zweck der Durchführung einer Zuverlässigkeitsüberprüfung weiterverarbeiten. Die Polizei kann hierfür die Identität der betroffenen Person feststellen und von ihr vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern.

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

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

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

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

29. In § 30 Abs. 1 Satz 1 und Abs. 2 wird jeweils das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.
30. In § 31 Abs. 5 Satz 1 wird das Wort „unterrichten“ durch das Wort „benachrichtigen“ und das Wort „Datennutzung“ durch das Wort „Datenverwendung“ ersetzt.
31. § 32 erhält folgende Fassung:

„§ 32
Anbietungspflicht

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

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

„§ 32a

Aussonderungsprüffristen und Löschfristen

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

(2) In den Fällen des § 23 Abs. 6 dürfen die Aussonderungsprüffristen bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre nicht überschreiten. Personenbezogene Daten der in § 23 Abs. 6 Satz 1 Nrn. 1 bis 4 bezeichneten Personen können ohne Zustimmung der betroffenen Person nur für die Dauer eines Jahres gespeichert werden. Die Speicherung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des § 23 Abs. 6 weiterhin vorliegen. Die maßgeblichen Gründe für die Aufrechterhaltung der Speicherung nach Satz 3 sind aktenkundig zu machen. Die Speicherung nach Satz 2 darf jedoch insgesamt drei Jahre und bei der Verhütung und Verfolgung von Straftaten nach § 129a, auch in Verbindung mit § 129b Abs. 1 des Strafgesetzbuchs sowie nach den §§ 6 bis 13 des Völkerstrafgesetzbuchs fünf Jahre nicht überschreiten.

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

§ 32b

Berichtigung personenbezogener Daten

sowie Einschränkung der Verarbeitung in Akten sowie Vernichtung von Akten

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

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

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

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

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

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

(3) In ihrer Verarbeitung eingeschränkte Daten dürfen nur für den Zweck verarbeitet werden, für den die Vernichtung der Akte unterblieben ist; sie dürfen auch verarbeitet werden, wenn dies zur Behebung einer bestehenden Beweisnot unerlässlich ist oder die betroffene Person einwilligt.

(4) § 31 Abs. 4 des Datenschutzrichtlinienumsetzungsgesetzes Sachsen-Anhalt gilt entsprechend.

§ 32c

Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten

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

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

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

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

„§ 109a

Übergangsvorschrift für die Verarbeitung personenbezogener Daten durch die Polizei

Abweichend von § 13d Abs. 2 ist das Weiterverarbeiten oder die Übermittlung personenbezogener Daten mit Hilfe automatisierter Verfahren auch zulässig nach den Bestimmungen des für die Daten am 24. Mai 2018 jeweils geltenden Verzeichnisses nach § 14 Abs. 3 des Datenschutzgesetzes Sachsen-Anhalt in der bis zum 24. Mai 2018 geltenden Fassung.“

Artikel 4

Änderung des Maßregelvollzugsgesetzes Sachsen-Anhalt

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

1. Die Inhaltsübersicht wird wie folgt geändert:

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

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

„§ 33 Optisch-elektronische Beobachtung und Verarbeitung von Bildaufzeichnungen

§ 34 Datenverwendung“.

c) Die Angabe zu § 36 erhält folgende Fassung:

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

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

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

4. § 32 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

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

bb) Satz 3 wird wie folgt geändert:

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

bbb) Die Nummern 8 und 9 werden aufgehoben.

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

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

1. Daten über Verwandte, über Personen aus dem beruflichen und sozialen Umfeld der untergebrachten Person sowie über Geschädigte,
2. Namen und Anschriften von Besuchenden, einschließlich eventueller Erkenntnisse über Verwandtschafts- oder Beziehungsverhältnisse zur untergebrachten Person

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

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

aa) Satz 1 erhält folgende Fassung:

„Die Leiterin oder der Leiter der Einrichtung oder die stellvertretende Leiterin oder der stellvertretende Leiter der Einrichtung hat der von der Datenverarbeitung nach

den Absätzen 1 und 2 betroffenen Person auf Antrag das Auskunftsrecht zu gewähren.“

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

5. § 33 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 33

Optisch-elektronische Beobachtung und Verarbeitung von Bildaufzeichnungen“.

b) Absatz 1 wird wie folgt geändert:

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

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

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

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

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

6. § 34 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

„§ 34

Datenverwendung“.

b) Absatz 1 wird wie folgt geändert:

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

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

c) Absatz 2 wird wie folgt geändert:

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

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

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

a) Im einleitenden Satzteil werden die Wörter „erhoben und“ gestrichen.

b) In Nummer 11 wird das Wort „oder“ durch ein Komma ersetzt.

c) In Nummer 12 wird der Punkt durch ein Komma ersetzt.

d) Nach Nummer 12 werden folgende Nummern 13 und 14 angefügt:

„13. in Umsetzung völkerrechtlicher Übereinkommen zur Überprüfung der Einhaltung der Rechte der untergebrachten Personen oder

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

8. § 36 erhält folgende Fassung:

„§ 36

Datenübermittlung zu archivarischen, wissenschaftlichen und statistischen Zwecken

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

9. § 37 wird wie folgt geändert:

- a) In Satz 1 wird das Wort „gespeicherten“ durch das Wort „vorhandenen“ ersetzt und werden nach dem Wort „löschen“ die Wörter „oder zu vernichten“ angefügt.
- b) Satz 2 wird aufgehoben.

10. § 38 einziger Satz erhält folgende Fassung:

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

Artikel 5

Änderung des Gesetzes zur Ausführung des Therapieunterbringungsgesetzes in Sachsen-Anhalt

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

- 1. Nach der Angabe „(GVBl. LSA S. 510)“ werden die Wörter „in der jeweils geltenden Fassung“ eingefügt.
- 2. Nach der Angabe „(BGBl. I S. 2300, 2305)“ werden die Wörter „, zuletzt geändert durch Artikel 8 des Gesetzes vom 5. Dezember 2012 (BGBl. I S. 2425, 2430), in der jeweils geltenden Fassung“ eingefügt.

Artikel 6

Einschränkung von Grundrechten

Durch die Artikel 2, 3 und 4 wird das Grundrecht auf Schutz personenbezogener Daten im Sinne des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes und des Artikels 6 Abs. 1 Satz 1 der Verfassung des Landes Sachsen-Anhalt eingeschränkt.

Artikel 7
Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.