

Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt - DSG LSA)

In der Fassung der Bekanntmachung vom 13. Januar 2016
(GVBl. LSA S. 24) zuletzt geändert durch
Artikel 1 des Gesetzes vom 21. Februar 2018 (GVBl. LSA S. 10)

Inhaltsübersicht

Erster Abschnitt:

Allgemeine Bestimmungen

- § 1 - Zweck des Gesetzes
- § 2 - Begriffsbestimmungen
- § 3 - Anwendungsbereich
- § 4 - Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
- § 4 a - Automatisierte Einzelentscheidungen
- § 5 - Datengeheimnis
- § 6 - Technische und organisatorische Maßnahmen
- § 7 - Einrichtung automatisierter Abrufverfahren
- § 7a - Gemeinsame Verfahren
- § 8 - Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Zweiter Abschnitt:

Rechtsgrundlagen der Datenerhebung, -verarbeitung und -nutzung

- § 9 - Datenerhebung
- § 10 - Datenspeicherung, -veränderung und -nutzung
- § 11 - Datenübermittlung an öffentliche Stellen
- § 12 - Datenübermittlung an nicht-öffentliche Stellen
- § 13 - Datenübermittlung ins Ausland sowie an über- oder zwischenstaatliche Stellen
- § 14 - Durchführung des Datenschutzes
- § 14 a - Beauftragter für den Datenschutz
- § 14 b - Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Dritter Abschnitt:**Rechte des Betroffenen**

- § 15 - Auskunft
- § 16 - Berichtigung, Löschung und Sperrung von Daten
- § 17 - Unabdingbare Rechte des Betroffenen
- § 18 - Schadensersatz
- § 19 - Anrufung des Landesbeauftragten für den Datenschutz

Vierter Abschnitt:**Landesbeauftragter für den Datenschutz**

- § 20 - Berufung des Landesbeauftragten für den Datenschutz
- § 21 - Rechtsstellung
- § 22 - Aufgaben und Befugnisse
- § 23 - Durchführung der Aufgaben
- § 24 - Beanstandungen durch den Landesbeauftragten

Fünfter Abschnitt:**Sondervorschriften**

- § 25 - Automatisierte Verfahren mittels mobiler personenbezogener Datenträger
- § 26 - Erhebung, Verarbeitung oder Nutzung besonders geschützter personenbezogener Daten
- § 27 - Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen
- § 28 - Erhebung, Verarbeitung oder Nutzung von Personal- und Bewerberdaten
- § 28 a - Gendiagnostik in öffentlich-rechtlichen Dienstverhältnissen
- § 29 - Fernmessen und Fernwirken
- § 30 - Optisch-elektronische Beobachtung
- § 30 a - Öffentliche Auszeichnungen

**Sechster Abschnitt:
Schlussvorschriften**

- § 31 - Strafvorschriften
- § 31 a - Bußgeldvorschriften
- § 31 b - Gerichtlicher Rechtsschutz
- § 32 - Übergangsvorschriften
- § 33 - Personalrechtliche Überleitungsvorschriften zum Gesetz zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes Sachsen-Anhalt
- § 34 - Evaluierung
- § 35 - (weggefallen)
- § 36 - Sprachliche Gleichstellung
- § 36 a - Einschränkung von Grundrechten
- § 37 - In-Kraft-Treten

Erster Abschnitt
Allgemeine Bestimmungen

§ 1

Zweck des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang öffentlicher Stellen des Landes mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Die öffentlichen Stellen haben die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 2

Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Handelt es sich dabei um Angaben über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, sind diese personenbezogene Daten besonderer Art. Allgemein zugänglich sind personenbezogene Daten, die jedermann ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts verwenden kann.

(2) Automatisiert ist ein Verfahren, wenn personenbezogene Daten programmgesteuert erhoben, verarbeitet oder genutzt werden (automatisiertes Verfahren); jede hierdurch entstehende Sammlung personenbezogener Daten, die programmgesteuert ausgewertet werden kann, ist eine automatisierte Datei.

(2a) Eine nicht-automatisierte Datei ist jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

(3) Eine Akte ist jede sonstige amtlichen, dienstlichen oder Geschäftszwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten

a) an einen Dritten in der Weise, dass

aa) die Daten an den Dritten weitergegeben werden oder

bb) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen oder

b) durch Veröffentlichung,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.

(7 a) Pseudonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der verwendeten Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.

(7 b) Verschlüsselung ist eine technische Maßnahme, die Daten unter Anwendung kryptografischer 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) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(9) Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Inland, in einem anderen Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(10) Empfänger ist mit Ausnahme des Betroffenen jeder, der Daten erhält; Empfänger ist auch eine andere Organisationseinheit der verantwortlichen Stelle, die Daten zur Erfüllung eines anderen Zwecks erhält.

(11) Ein mobiler personenbezogener Datenträger im Sinne dieses Gesetzes ist ein Speicher- oder Verarbeitungsmedium,

1. das zur Verfügung durch den Betroffenen bestimmt ist,
2. auf dem über die erstmalige Speicherung hinaus personenbezogene Daten automatisiert verarbeitet oder durch das personenbezogene Daten automatisiert erhoben, verarbeitet oder genutzt werden können und
3. bei dem die Erhebung, Verarbeitung oder Nutzung nach Nummer 2 durch andere als den Betroffenen erfolgt und der Betroffene dies nur durch den Gebrauch des Mediums beeinflussen kann.

§ 3

Anwendungsbereich

(1) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden, der Landkreise und sonstiger

der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen, ungeachtet ihrer Rechtsform (öffentliche Stellen). Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(2) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:

1. Soweit öffentliche Stellen als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie und ihre Vereinigungen die §§ 14, 14 a, 19, 22 bis 24, 28 und 29. Im Übrigen gelten mit Ausnahme der §§ 4 d bis 4 g und 38 die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes, einschließlich der Straf- und Bußgeldvorschriften.

2. Für öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen gilt § 28, im Übrigen gelten anstelle dieses Gesetzes alle Vorschriften des Bundesdatenschutzgesetzes, die auf privatrechtliche Unternehmen anzuwenden sind.

3. Dieses Gesetz gilt nicht für die Ausübung des Gnadenrechts.

(3) Soweit andere Rechtsvorschriften auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes für das Land Sachsen-Anhalt vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten erhoben, verarbeitet oder genutzt werden.

§ 4

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.

(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf die Bedeutung der Einwilligung, den Zweck der Erhebung, Verarbeitung und Nutzung sowie auf sein Recht und die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung

bedarf der Schriftform und muss die Art der Daten und die Dritten, an die Übermittlungen vorgesehen sind, bestimmen, soweit nicht wegen besonderer Umstände eine andere Form oder ein anderer Inhalt angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Der Betroffene kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen.

(3) *(aufgehoben)*

(4) Auch wenn die rechtlichen Voraussetzungen vorliegen, dürfen personenbezogene Daten nicht erhoben, verarbeitet oder genutzt werden, soweit sich der Betroffene hiergegen wegen einer besonderen persönlichen Situation wendet und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen gegenüber dem Interesse der verantwortlichen Stelle oder eines Dritten an der Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht

1. für die Verfassungsschutzbehörde im Rahmen ihrer Aufgabenstellung nach § 4 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt,
2. für öffentliche Stellen der Polizei im Rahmen der Gefahrenabwehr oder Strafverfolgung,
3. für die Strafverfolgungsorgane im Rahmen der Strafverfolgung und
4. für die Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichert.

§ 4 a

Automatisierte Einzelentscheidungen

(1) Entscheidungen, die zu einer rechtlichen Beschwer des Betroffenen führen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung oder Nutzung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

(2) Dies gilt nicht, wenn

1. ein Gesetz dies vorsieht oder

2. es dem Betroffenen vor der Entscheidung ermöglicht wird, seine Interessen geltend zu machen.

§ 5

Datengeheimnis

Den bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

§ 6

Technische und organisatorische Maßnahmen

(1) Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die nach den Absätzen 2 und 3 erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Art und Weise der Maßnahmen richtet sich nach dem jeweiligen Stand der Technik.

(2) Werden personenbezogene Daten automatisiert erhoben, verarbeitet oder genutzt, sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, zu gewährleisten, dass

1. diese nur Befugte zur Kenntnis nehmen können (Vertraulichkeit),
2. diese während der Erhebung, Verarbeitung oder Nutzung unversehrt, vollständig und aktuell bleiben (Integrität),
3. diese zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können (Verfügbarkeit),
4. diese ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat (Revisionsfähigkeit),

6. die Verfahren zur Erhebung, Verarbeitung oder Nutzung nachvollziehbar und aktuell dokumentiert sind (Transparenz).

(3) Werden personenbezogene Daten nicht automatisiert erhoben, verarbeitet oder genutzt, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport oder der Vernichtung zu verhindern.

§ 7

Einrichtung automatisierter Abrufverfahren

(1) Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, darf nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Eine Vorabkontrolle nach § 14 Abs. 2 muss erfolgt sein. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 6 erforderliche technische und organisatorische Maßnahmen.

Die erforderlichen Festlegungen können auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Vor der Einrichtung von Abrufverfahren ist der Landesbeauftragte für den Datenschutz unter Mitteilung der vorgesehenen Festlegungen nach Absatz 2 zu unterrichten.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die übermittelnde Stelle prüft die Zulässigkeit der Abrufe, wenn dazu Anlass besteht. Die übermittelnde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt, so bezieht sich die Gewährleistung der Feststel-

lung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten.

(6) Absatz 1 Satz 1 und 3 sowie Absatz 4 gelten entsprechend, wenn innerhalb einer öffentlichen Stelle ein automatisiertes Abrufverfahren eingerichtet wird.

§ 7 a

Gemeinsame Verfahren

(1) Ein automatisiertes Verfahren, das mehreren verantwortlichen Stellen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ermöglicht (gemeinsames Verfahren), darf nur eingerichtet werden, soweit die beteiligten Stellen hinsichtlich aller im gemeinsamen Verfahren gespeicherten Daten zu deren Erhebung, Verarbeitung oder Nutzung dem Grunde nach befugt sind oder zur Teilnahme an einem Anrufverfahren nach § 7 berechtigt werden könnten. Das Verfahren muss unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen sein.

(2) Vor der Einrichtung eines gemeinsamen Verfahrens bestimmen die beteiligten Stellen eine Stelle, der die Planung, Einrichtung und Durchführung des Verfahrens obliegt, und legen die Bezeichnung und Aufgaben der beteiligten Stellen einschließlich der Verantwortung für die Freigabe nach § 14 Abs. 2 Satz 1 sowie den Bereich der Verantwortung, für deren Rechtmäßigkeit sie im Einzelfall verantwortlich sind, schriftlich fest.

(3) § 7 Abs. 2 bis 4 gilt entsprechend.

(4) Absatz 1 und § 7 Abs. 4 gelten entsprechend, wenn innerhalb einer öffentlichen Stelle für mehrere Organisationseinheiten mit unterschiedlichen Aufgaben ein Verfahren betrieben wird, das einem gemeinsamen Verfahren vergleichbar ist.

(5) Gemeinsame Verfahren sind auch unter Beteiligung von Stellen, die nicht Adressaten dieses Gesetzes sind, zulässig, soweit für diese Stellen dem Absatz 1 entsprechende und den Absätzen 2 und 3 gleichwertige Rechtsvorschriften bestehen.

§ 8

Erhebung, Verarbeitung oder Nutzung personenbezogener
Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 17 und 18 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art und der Kreis der Betroffenen,
3. die nach § 6 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftragsgebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags,
11. gegebenenfalls die nach Absatz 6 Satz 1 bestehenden Verpflichtungen des Arbeitnehmers.

Der Auftrag kann auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber, die Fachaufsichtsbehörde oder eine von der Fachaufsichtsbehörde bestimmte Stelle hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Hält der Auftraggeber trotz der Bedenken an der Weisung fest, so hat der Auftragnehmer den Landesbeauftragten für den Datenschutz zu informieren.

(4) Für den öffentlichen Auftragnehmer gelten nur die Absätze 1 bis 3 sowie die §§ 5, 6, 14 Abs. 1, §§ 14 a, 22 bis 24, 31 bis 32 .

(5) Ist der Auftragnehmer eine juristische Person, Gesellschaft oder andere Personenvereinigung des privaten Rechts, bei der dem Land, den Gemeinden, den Landkreisen oder den sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, gelten § 14 Abs. 1, §§ 19 sowie 22 bis 24 entsprechend, soweit diese Personen oder Personenvereinigungen personenbezogene Daten im Auftrag der in § 3 Abs. 1 genannten Stellen erheben, verarbeiten oder nutzen. Sofern kein Beauftragter für den Datenschutz nach den Bestimmungen des Bundesdatenschutzgesetzes bestellt ist, findet § 14 a entsprechend Anwendung.

(6) Sind auf den Auftragnehmer die Vorschriften dieses Gesetzes nicht anwendbar, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle durch den Landesbeauftragten für den Datenschutz entsprechend den §§ 22 bis 24 unterwirft. Der Auftraggeber hat den Landesbeauftragten für den Datenschutz über die Beauftragung zu unterrichten.

(7) Werden Datenverarbeitungsanlagen oder -verfahren durch Dritte gewartet, gelten, soweit bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht vermieden werden kann, die Absätze 1 und 2 sowie Absatz 3 Satz 1 entsprechend.

Zweiter Abschnitt
Rechtsgrundlagen der Datenerhebung, -verarbeitung
und -nutzung

§ 9
Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(2) Personenbezogene Daten sind beim Betroffenen mit seiner Kenntnis zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden und

a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht, insbesondere in den Fällen des § 10 Abs. 2 Nrn. 4, 6 bis 8, oder

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere in den Fällen des § 10 Abs. 2 Nrn. 3 und 5 .

(3) Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Er ist über die Rechtsvorschriften und über die Folgen der Verweigerung von Angaben aufzuklären. Ferner sind ihm gegenüber anzugeben:

1. die verantwortliche Stelle,
2. der Zweck der Erhebung, Verarbeitung und Nutzung sowie
3. die Dritten, an die Übermittlungen vorgesehen sind, soweit der Betroffene nicht aufgrund einer Rechtsvorschrift oder nach den Umständen des Einzelfalls mit der Übermittlung rechnen muss. Ist eine Übermittlung an eine der in § 15 Abs. 3 genannten Stellen vorgesehen und soll der Betroffene hierüber unterrichtet werden, ist die Unterrichtung nur mit Zustimmung der genannten Stellen zulässig.

(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(5) Werden personenbezogene Daten nicht beim Betroffenen erhoben, so ist dieser bei der Speicherung, im Falle einer vorgesehenen Übermittlung spätestens bei der ersten Übermittlung der Daten entsprechend Absatz 3 Satz 3 zu benachrichtigen. Wurden die Daten beim Betroffenen ohne seine Kenntnis erhoben, soll er nach Satz 1 benachrichtigt werden, sobald die Erfüllung der Aufgaben dadurch nicht mehr gefährdet wird. Satz 1 gilt nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt,
2. die Unterrichtung im Verhältnis zum Informationswert für den Betroffenen einen unverhältnismäßigen Aufwand erfordern würde,
3. die Verarbeitung oder Nutzung der Daten durch Gesetz ausdrücklich vorgesehen ist oder
4. eine Auskunft nach § 15 Abs. 2 nicht erfolgt oder nach § 15 Abs. 4 unterbleiben würde.

§ 10

Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke verändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,

4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,

6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonstigen gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

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

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 11

Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 7 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf die übermittelten Daten für den Zweck (§ 9 Abs. 1 und 2) verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 10 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden. Die Feststellung hierüber trifft, soweit sie nicht durch das für Datenschutz zuständige Ministerium generell erfolgt ist, die übermittelnde Stelle.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Verarbeitung oder Nutzung dieser Daten ist unzulässig. § 34 Abs. 3 bleibt unberührt.

(6) Absatz 5 Satz 1 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 12

Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden,

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat

oder

3. die Voraussetzungen des § 10 Abs. 2 Nr. 9 vorliegen.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen vorher von der Übermittlung seiner Daten, soweit nicht die Vereitelung von Rechtsansprüchen zu befürchten wäre. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 13

Datenübermittlung ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an öffentliche Stellen anderer Mitgliedsstaaten der Europäischen Union und der Vertragsstaaten des Abkommens

über den Europäischen Wirtschaftsraum sowie an Organe und Einrichtungen der Europäischen Gemeinschaften gilt § 11 Abs. 1 . Für die Übermittlung an nicht-öffentliche Stellen in Mitgliedsstaaten der Europäischen Union und in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum gilt § 12 Abs. 1 und 3 .

(2) Für die Übermittlung an andere als in Absatz 1 genannte ausländische oder über- oder zwischenstaatliche Stellen gilt § 12 Abs. 1 und 3 . Die Übermittlung ist nur zulässig, wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau gewährleistet ist. Fehlt es an einem angemessenen Datenschutzniveau ist die Übermittlung zulässig, wenn

1. der Betroffene eingewilligt hat,
2. sie für die Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen sind, erforderlich ist,
3. sie für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
4. sie für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
5. sie aus einem durch Rechtsvorschrift vorgeschriebenen Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

(2a) Übermittlungsbeschränkungen, die sich aus dem Fünften Abschnitt des Gesetzes ergeben, sind zu beachten.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(4) Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihr übermittelt werden.

§ 14

Durchführung des Datenschutzes

(1) Die obersten Landesbehörden, die Gemeinden, die Landkreise und die sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts haben jeweils für ihren Organisationsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Der Landesbeauftragte für den Datenschutz ist rechtzeitig über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten. Er ist vor dem Erlass von Rechts- und Verwaltungsvorschriften, die den Umgang mit personenbezogenen Daten betreffen, zu hören.

(2) Ein automatisiertes Verfahren ist, soweit

1. es sich um ein Abrufverfahren nach § 7 Abs. 1 Satz 1 oder ein gemeinsames Verfahren nach § 7a handelt,

2. personenbezogene Daten besonderer Art (§ 2 Abs. 1 Satz 2) erhoben, verarbeitet oder genutzt werden,

3. das Erheben, Verarbeiten oder Nutzen dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten, einschließlich seiner Kompetenz, seiner Leistung oder seines Verhaltens, oder

4. mobile personenbezogene Datenträger (§ 2 Abs. 11) eingesetzt werden, vor seiner Freigabe oder wesentlichen Änderung zu überprüfen, ob es datenschutzrechtlich zulässig ist und die nach § 6 Abs. 2 vorgesehenen technischen und organisatorischen Maßnahmen ausreichend sind. Die Vorabkontrolle ist bei der Stelle vorzunehmen, die über die Freigabe oder wesentliche Änderung des Verfahrens entscheidet.

(3) Die verantwortlichen Stellen haben für automatisierte Verfahren, mit deren Hilfe personenbezogene Daten erhoben, verarbeitet oder genutzt werden, in einem Verzeichnisse festzulegen

1. die Bezeichnung des Verfahrens,

2. die Zweckbestimmung und die Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung,

3. den Kreis der Betroffenen,
4. die Art der Daten,
5. die vorgesehenen Übermittlungen,
6. die vorgesehene Weitergabe personenbezogener Daten innerhalb der verantwortlichen Stelle zu Zwecken außerhalb des Speicherungszwecks sowie an Stellen, die personenbezogene Daten im Auftrag verarbeiten oder nutzen,
7. Regelfristen für die Löschung oder für die Prüfung, ob die weitere Speicherung der Daten noch erforderlich ist,
8. die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind, und
9. die technischen und organisatorischen Maßnahmen nach § 6, die Art der Geräte und die eingesetzte Software. Die Festlegungen können auch durch die in Absatz 1 genannten oder durch von diesen bestimmte Stellen getroffen werden.

(4) Absatz 3 gilt nicht für Verfahren,

1. deren einziger Zweck das Führen eines durch Rechtsvorschrift vorgeschriebenen Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, oder
2. die ausschließlich der Unterstützung der allgemeinen Bürotätigkeit dienen, insbesondere Verfahren der Textverarbeitung, Vorgangsverwaltung, Terminüberwachung und der Führung von Adress-, Telefon- und vergleichbaren Verzeichnissen, soweit sie keine Beeinträchtigung der Rechte Betroffener erwarten lassen.

(5) Das Verfahrensverzeichnis kann von jedermann eingesehen werden. Die Einsicht ist gebühren- und auslagenfrei. Ausgenommen von der Einsicht sind die Angaben nach Absatz 3 Satz 1 Nrn. 8 und 9. Satz 1 gilt nicht für Verfahren, die die in § 4 Abs. 4 Satz 2 genannten Stellen zu den dort angeführten Zwecken betreiben, soweit die verantwortliche Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für vereinbar erklärt.

§ 14 a
Beauftragter für den Datenschutz

(1) Öffentliche Stellen haben bei Einsatz automatisierter Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, soweit es sich nicht ausschließlich um Verfahren im Sinne des § 14 Abs. 4 Nr. 2 handelt, einen Beauftragten für den Datenschutz schriftlich einzusetzen. Soweit die öffentliche Stelle einer Dienstaufsicht unterliegt, kann die Einsetzung des Beauftragten auch durch die Dienstaufsichtsbehörde erfolgen. Notare und die in § 3 Abs. 1 Satz 2 genannten Stellen haben einen Beauftragten erst dann einzusetzen, wenn mindestens zehn Personen bei der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt werden. Für bis zu fünf Schulen mit jeweils zehn oder weniger Personen nach Satz 3 kann ein gemeinsamer Beauftragter für den Datenschutz eingesetzt werden. Die Einsetzung als Beauftragter für den Datenschutz kann in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches widerrufen werden. Vor der Entscheidung über den Widerruf sind der Betroffene und der Landesbeauftragte für den Datenschutz zu hören.

(2) Der Beauftragte für den Datenschutz muss die erforderliche Fachkunde und Zuverlässigkeit besitzen; er ist in seiner Funktion weisungsfrei. Zum Erwerb und zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde ist dem Beauftragten für den Datenschutz, wenn er Bediensteter einer öffentlichen Stelle ist, die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen; die Kosten hat die öffentliche Stelle zu übernehmen. Er kann sich unmittelbar an die Leitung der öffentlichen Stelle und bei der Erledigung seiner Aufgabe nach Absatz 4 Satz 2 Nr. 2 in Zweifelsfällen unmittelbar an den Landesbeauftragten für den Datenschutz wenden. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Er ist im erforderlichen Umfang von anderen Aufgaben freizustellen.

(3) Der Beauftragte für den Datenschutz darf zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen. Im Übrigen gelten § 22 Abs. 3 Satz 1 und § 23 Abs. 1 entsprechend. Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er davon nicht durch den Betroffenen befreit wird.

(4) Der Beauftragte für den Datenschutz führt das Verzeichnisse nach § 14 Abs. 3 Satz 1. Er hat die öffentliche Stelle, für die er eingesetzt ist, bei der Ausführung

dieses Gesetzes und anderer Vorschriften über den Datenschutz zu unterstützen, indem er insbesondere

1. auf die Beachtung dieser Vorschriften hinwirkt,
2. die Vorabkontrolle nach § 14 Abs. 2 vornimmt und
3. die bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigten Personen mit diesen Vorschriften vertraut macht.

§ 14 b

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

(1) Wird einer verantwortlichen Stelle bekannt, dass bei ihr gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen der Betroffenen, hat sie unverzüglich den Betroffenen und den Landesbeauftragten für den Datenschutz zu informieren.

(2) Die Information der Betroffenen muss erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Betroffenen sind über die Art der unrechtmäßigen Kenntniserlangung und über Maßnahmen zur Minderung möglicher nachteiliger Folgen zu unterrichten. Die Information unterbleibt, wenn

1. anzunehmen ist, dass die Betroffenen auf andere Weise die Informationen nach den Sätzen 1 und 2 erhalten haben,
2. eine Auskunft nach § 15 Abs. 4 zu verweigern wäre oder
3. sie einen unverhältnismäßigen Aufwand erfordern würde und an ihre Stelle eine angemessene Information der Öffentlichkeit tritt.

Dritter Abschnitt
Rechte des Betroffenen

§ 15
Auskunft

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten oder ihre erfolgte Übermittlung an Dritte beziehen,
2. den Zweck und die Rechtsgrundlage der Verarbeitung oder Nutzung,
3. die vorgesehenen Übermittlungen und
4. den strukturierten Ablauf der automatisierten Verarbeitung oder Nutzung der Daten und die dabei herangezogenen Entscheidungskriterien im Falle des § 4 a .

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(1a) Die Auskunft über Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, wird nur auf besonderen Antrag, den der Betroffene in Kenntnis der Kostenpflicht nach Absatz 7 Satz 2 gestellt hat, erteilt.

(2) Absatz 1 gilt nicht für personenbezogene Daten,

1. die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen oder
2. die für Zwecke der amtlichen Statistik verarbeitet oder genutzt werden.

(3) 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. Wird die Zustimmung nicht erteilt, ist hierüber der Landesbeauftragte für den Datenschutz zu unterrichten.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,

2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, sofern dieser der Auskunftserteilung nicht zustimmt, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Landesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist kostenfrei. Satz 1 gilt nicht, soweit die Auskunft über Daten im Sinne des Absatzes 1 a begehrt wird und mit der Auskunftserteilung besonderer Verwaltungsaufwand verbunden ist.

§ 16

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten in Akten unrichtig sind, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Personenbezogene Daten sind spätestens dann zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Satz 1 Nr. 2 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Soweit eine Löschung nach Satz 2 unterbleibt, sind die personenbezogenen Daten zu sperren.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder bei Akten nur mit unverhältnismäßig hohem Aufwand möglich ist.

Im Fall des Satzes 1 Nr. 2 sind die Gründe aufzuzeichnen.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(6) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen die Daten übermittelt wurden; dies gilt nicht, wenn die Verständigung zur Wahrung schutzwürdiger Interessen des Betroffenen nicht erforderlich ist, sich als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden wäre. Satz 1 gilt entsprechend, wenn personenbezogene Daten innerhalb der verantwortlichen Stelle weitergegeben werden.

(7) Vor der Löschung personenbezogener Daten nach Absatz 2 Satz 1 Nr. 2 Satz 2 sind Akten und Dateien, die solche personenbezogenen Daten enthalten, nach Maßgabe des Archivgesetzes Sachsen-Anhalt, dem zuständigen öffentlichen Archiv anzubieten und zu übergeben.

§ 17

Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§ 15) und auf Berichtigung, Löschung oder Sperrung (§ 16) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, die verantwortliche Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die verantwortliche Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die verantwortliche Stelle zu unterrichten. Die Verfassungsschutzbehörde, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Landesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 15 Abs. 6.

§ 18 Schadensersatz

(1) Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen zum Ersatz des daraus entstehenden Schadens verpflichtet. Die Ersatzpflicht tritt nicht ein, soweit die verantwortliche Stelle den Umstand, durch den der Schaden entstanden ist, nicht zu vertreten hat.

(2) Tritt ein Schaden nach Absatz 1 Satz 1 bei automatisierter Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ein, ist die verantwortliche Stelle dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet. Bei einer Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen. Der Anspruch ist insgesamt auf einen Betrag in Höhe von 125000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Betrag von 250000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zum Höchstbetrag steht. Sind für ein automatisiertes Verfahren mehrere Stellen verantwortlich und ist der Geschädigte nicht in der Lage, die schädigende Stelle festzustellen, so haften die Stellen als Gesamtschuldner. Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuches. Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuches entsprechende Anwendung.

§ 19 Anrufung des Landesbeauftragten für den Datenschutz

Jedermann kann sich an den Landesbeauftragten für den Datenschutz wenden, wenn er

1. der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen in seinen Rechten verletzt worden zu sein, oder

2. tatsächliche Anhaltspunkte für den Verstoß oder das unmittelbare Bestehen eines Verstoßes gegen Vorschriften dieses Gesetzes oder eine andere Rechtsvorschrift über den Datenschutz durch eine öffentliche Stelle hat.

Niemand darf wegen der Anrufung nach Satz 1 benachteiligt oder gemäßregelt werden.

Vierter Abschnitt **Landesbeauftragter für den Datenschutz**

§ 20

Berufung des Landesbeauftragten für den Datenschutz

(1) Der Landtag wählt gemäß Artikel 63 Abs. 2 der Verfassung des Landes Sachsen-Anhalt den Landesbeauftragten für den Datenschutz; die einmalige Wiederwahl ist zulässig. Der Landesbeauftragte muss, die Befähigung für den Zugang zu Laufbahnen der Laufbahngruppe 2 unter den Voraussetzungen des § 14 Abs. 4 des Landesbeamtengesetzes erworben haben und über die zur Erfüllung seiner Aufgaben und zur Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde, insbesondere im Bereich des Schutzes personenbezogener Daten, verfügen.

(2) Der Landesbeauftragte für den Datenschutz ist Beamter auf Zeit und wird vom Präsidenten des Landtages auf die Dauer von sechs Jahren berufen. Er ist verpflichtet, das Amt bis zur Bestellung eines Nachfolgers weiterzuführen; die Amtszeit gilt als entsprechend verlängert. Kommt er der Verpflichtung nach Satz 2 nicht nach, ist er zu entlassen.

§ 21

Rechtsstellung

(1) Der Landesbeauftragte für den Datenschutz ist Aufsichtsbehörde im Sinne von

1. Artikel 4 Nr. 21 in Verbindung mit Artikel 51 der Datenschutz-Grundverordnung vom 27. April 2016 (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72) und
2. Artikel 3 Nr. 15 in Verbindung mit 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).

Er ist in Ausübung seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Er gilt für den Bereich seiner Geschäftsstelle als oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung und als oberste Aufsichtsbehörde im Sinne des § 99 der Verwaltungsgerichtsordnung, des § 119 des Sozialgerichtsgesetzes sowie des § 86 der Finanzgerichtsordnung; er trifft die Entscheidungen nach § 51 des Landesbeamtengesetzes für sich, seine Vorgänger im Amt und seine Bediensteten in eigener Verantwortung. Er gilt in Wahrnehmung seiner Aufgabe nach § 22 Abs. 2 als oberste Landesbehörde im Sinne des § 68 Abs. 1 Satz 2 Nr. 1 der Verwaltungsgerichtsordnung. Im Übrigen untersteht er der Dienstaufsicht des Präsidenten des Landtages nur, soweit nicht seine Unabhängigkeit beeinträchtigt wird. Auf ihn sind die für Richter geltenden Vorschriften über Dienstaufsicht, Versetzung in ein anderes Richteramt, Eintritt und Versetzung in den Ruhestand, Entlassung, Amtsenthebung und Disziplinarmaßnahmen entsprechend anzuwenden. Für ein Disziplinarverfahren gegen den Landesbeauftragten für den Datenschutz ist der Dienstgerichtshof für Richter bei dem Obergericht des Landes Sachsen-Anhalt zuständig. Die nichtständigen Beisitzer müssen der Verwaltungsgerichtsbarkeit angehören.

(2) Für personenbezogene Daten, die dem Landesbeauftragten für den Datenschutz und seinen Bediensteten im Rahmen ihrer Aufgabenstellung nach diesem Gesetz bekannt werden, gilt § 10 Abs. 4 entsprechend.

(3) Beim Landesbeauftragten für den Datenschutz wird eine Geschäftsstelle eingerichtet. Dem Landesbeauftragten für den Datenschutz ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Haushalt des Landes in einem eigenen Einzelplan auszuweisen. Die Geschäftsstelle wird durch den Landesbeauftragten für den Datenschutz geleitet. Der Landesbeauftragte für den Datenschutz übt die Dienstaufsicht über alle Bediensteten der Geschäftsstelle aus; er ist Vorgesetzter, Dienstvorgesetzter, höherer Dienstvorgesetzter und oberste Dienstbehörde des Direktors der Geschäftsstelle und der Bediensteten der Geschäftsstelle. Der Direktor der Geschäftsstelle überwacht den ordnungsgemäßen Geschäftsablauf innerhalb der Geschäftsstelle; er muss die Befähigung nach § 5 des Deutschen Richtergesetzes besitzen. Der Landesbeauftragte für den Datenschutz kann Aufgaben der Personalverwaltung auf eine andere Stelle des Landes übertragen, wenn diese zustimmt; die Unabhängigkeit des Landes-

beauftragten für den Datenschutz darf hierdurch nicht beeinträchtigt werden. Der Stelle nach Satz 6 Halbsatz 1 dürfen personenbezogene Daten der Bediensteten übermittelt werden, soweit die Kenntnis der Daten zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(4) Der Landesbeauftragte für den Datenschutz wird durch den Direktor der Geschäftsstelle vertreten, wenn er an der Ausübung seines Amtes verhindert ist oder im Falle des § 20 Abs. 2 Satz 3 entlassen wurde. Für die Dauer der Vertretung hat der Direktor der Geschäftsstelle die Befugnisse des Landesbeauftragten für den Datenschutz.

§ 22

Aufgaben und Befugnisse

(1) Der Landesbeauftragte für den Datenschutz erfüllt gegenüber allen öffentlichen Stellen die Aufgaben aus Artikel 57 der Datenschutz-Grundverordnung. Dazu stehen ihm die Befugnisse aus Artikel 58 der Datenschutz-Grundverordnung zu. Geldbußen können durch den Landesbeauftragten für den Datenschutz gegenüber öffentlichen Stellen nicht verhängt werden; dies gilt nicht, soweit öffentliche Stellen als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Im Geltungsbereich der Richtlinie (EU) 2016/680 erfüllt er die Aufgaben aus Artikel 46 der Richtlinie (EU) 2016/680. Ihm stehen die Befugnisse aus Artikel 47 der Richtlinie (EU) 2016/680 zu. Die Gerichte unterliegen seiner Kontrolle nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(2) Der Landesbeauftragte für den Datenschutz ist Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes; in dieser Eigenschaft kommen nach diesem Gesetz nur die Absätze 2a, 2b und 4 bis 7 sowie § 21 Abs. 1, 3 und 4 zur Anwendung.

(2a) Der Landesbeauftragte für den Datenschutz ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten

1. nach § 43 des Bundesdatenschutzgesetzes,
2. nach § 16 Abs. 2 Nrn. 2 bis 5 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692), in der jeweils geltenden Fassung,
3. nach § 111 Abs. 1 Nr. 1 des Vierten Buches Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - in der Fassung der Bekanntmachung vom 12. November 2009 (BGBl. I S. 3710, 3973; 2011, 363), zuletzt geändert durch Artikel

3 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1202, 1204), in der jeweils geltenden Fassung,

4. nach § 85 des Zehnten Buches Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Artikel 13 des Gesetzes vom 23. Mai 2011 (BGBl. I S. 898, 917), in der jeweils geltenden Fassung,

5. nach § 31 a,

6. nach § 130 Abs. 1 des Gesetzes über Ordnungswidrigkeiten, soweit die unterlassene Aufsichtsmaßnahme datenschutzrechtliche Zuwiderhandlungen gegen die in den Nummern 1 bis 5 genannten Gesetze betrifft.

(2b) Der Landesbeauftragte für den Datenschutz ist hilfeleistende Behörde nach Artikel 13 Abs. 2 Buchst. a des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (BGBl. 1985 II S. 538, 539) in Verbindung mit Artikel 2 des Gesetzes zu dem Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 13. März 1985 (BGBl. II S. 538).

(3) Eine Kontrolle durch den Landesbeauftragten für den Datenschutz findet nicht statt, wenn sie sich auf personenbezogene Daten erstreckt, die sich in Akten über die Sicherheitsüberprüfung befinden und der Betroffene generell oder im Einzelfall der Kontrolle der auf ihn bezogenen Daten widersprochen hat. Der Widerspruch ist gegenüber dem Landesbeauftragten für den Datenschutz zu erklären. Unbeschadet des Kontrollrechts des Landesbeauftragten unterrichtet die öffentliche Stelle die Betroffenen über das Widerspruchsrecht in allgemeiner Form.

(4) Der Landesbeauftragte für den Datenschutz kann Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er den Landtag, die Landesregierung und die sonstigen öffentlichen Stellen in Fragen des Datenschutzes beraten.

(5) Auf Ersuchen des Landtages, seiner Ausschüsse oder der Landesregierung kann der Landesbeauftragte für den Datenschutz Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

(6) Der Landtag, seine Ausschüsse und die Landesregierung können den Landesbeauftragten für den Datenschutz um die Erstattung von Gutachten und Stellungnahmen ersuchen.

(7) Der Landesbeauftragte für den Datenschutz arbeitet mit den Behörden und sonstigen Stellen zusammen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in der Europäischen Union, im Bund und in den Ländern zuständig sind. Er leistet den anderen Kontrollstellen in den Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe).

(8) Stellt der Landesbeauftragte für den Datenschutz einen Verstoß gegen dieses Gesetz oder andere Rechtsvorschriften über den Datenschutz fest, so ist er befugt, diesen bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen.

§ 23

Durchführung der Aufgaben

(1) Die öffentlichen Stellen sind verpflichtet, den Landesbeauftragten für den Datenschutz und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

(2) Die in § 17 Abs. 2 genannten öffentlichen Stellen gewähren die Unterstützung nur dem Landesbeauftragten für den Datenschutz selbst und den von ihm schriftlich besonders Beauftragten. Absatz 1 Satz 2 gilt für die in Satz 1 genannten öffentlichen Stellen nicht, soweit die oberste Landesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(3) Der Landesbeauftragte für den Datenschutz teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung festgestellter Mängel bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 24 bleibt unberührt.

§ 24

Beanstandungen durch den Landesbeauftragten

(1) Stellt der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder son-

stige Mängel der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei den Gemeinden, Landkreisen und den sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen des Satzes 1 Nr. 2 unterrichtet der Landesbeauftragte für den Datenschutz gleichzeitig die zuständige Aufsichtsbehörde.

(2) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

(3) Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

Fünfter Abschnitt Sondervorschriften

§ 25

Automatisierte Verfahren mittels mobiler personenbezogener Datenträger

(1) Automatisierte Verfahren, soweit sie auf oder durch mobile personenbezogene Datenträger ablaufen, dürfen von öffentlichen Stellen nur eingesetzt werden, wenn

1. dies durch eine oder aufgrund einer Rechtsvorschrift vorgesehen ist,
2. der Betroffene eingewilligt hat,

3. dies zur Kontrolle von Zugangs- oder Zugriffsberechtigungen erfolgt, insbesondere in Durchführung technischer und organisatorischer Maßnahmen nach § 6 oder

4. dies zum Nachweis erforderlich ist

a) über An- und Abwesenheitszeiten,

b) über die Inanspruchnahme von Berechtigungen oder Leistungen oder

c) über die Eigenschaft der Zugehörigkeit zu einer bestimmten Personengruppe

und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen entgegenstehen.

(2) In solchen Verfahren dürfen nicht mehr personenbezogene Daten erhoben, verarbeitet oder genutzt werden, als für die nach Absatz 1 genannten Zwecke erforderlich sind.

(3) Die Stelle, die ein Verfahren nach Absatz 1 einsetzt oder ändert, muss den Betroffenen

1. über ihre Identität und Anschrift,

2. in allgemein verständlicher Form über die Funktionsweise des Datenträgers einschließlich der Art der zu verarbeitenden personenbezogenen Daten,

3. darüber, wie er seine Rechte nach den §§ 15 und 16 ausüben kann, und

4. über die bei Verlust oder Zerstörung des Datenträgers zu treffenden Maßnahmen unterrichten, soweit er nicht bereits Kenntnis erlangt hat.

(4) Der Vorgang des Erhebens, Verarbeitens oder Nutzens muss für den Betroffenen erkennbar sein.

§ 26

Erhebung, Verarbeitung oder Nutzung besonders geschützter personenbezogener Daten

(1) Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten besonderer Art ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. der Betroffene eingewilligt hat, wobei sich die Einwilligung ausdrücklich auf diese Daten beziehen muss,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonstigen gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies gemäß § 27 oder einer vergleichbaren gesetzlichen Regelung für Forschungszwecke erfolgt und die Voraussetzungen des § 10 Abs. 2 Nr. 9 vorliegen,
7. dies zum Zwecke öffentlicher Auszeichnungen erforderlich ist oder
8. es zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung des Betroffenen oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Satz 1 gilt nicht für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Wahrnehmung von Aufgaben der Gefahrenabwehr oder der Verfolgung von Straftaten oder Ordnungswidrigkeiten.

(2) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen. Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 27

Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten oder zu nutzen und die Vorschriften der Absätze 3 und 4 einzuhalten.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, 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.

(4) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur übermitteln, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 28

Erhebung, Verarbeitung oder Nutzung von Personal- und Bewerberdaten

(1) Für das Erheben, Verarbeiten oder Nutzen von Personaldaten über Angestellte, Arbeiter und Auszubildende, die in einem privatrechtlich ausgestalteten Ausbildungsverhältnis stehen, gelten die §§ 84 bis 91 des Landesbeamtengesetzes entsprechend, soweit nicht die Besonderheiten des Arbeits- und Tarifrechts hinsichtlich der Aufnahme und Entfernung bestimmter Unterlagen eine abweichende Behandlung erfordern.

(2) Die Einstellungsbehörde darf vom untersuchenden Arzt oder Psychologen in der Regel nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellte Risikofaktoren verlangen.

(3) Personenbezogene Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, dass der Betroffene in die weitere Speicherung eingewilligt hat.

(4) Soweit Daten der Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen des § 6 Abs. 2 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

§ 28 a

Gendiagnostik in öffentlich-rechtlichen Dienstverhältnissen

Es gelten entsprechend

1. für unmittelbare und mittelbare Beamte des Landes sowie für Richter des Landes die für Beschäftigte geltenden Vorschriften,

2. für Bewerber für ein öffentlich-rechtliches Dienstverhältnis oder Personen, deren öffentlich-rechtliches Dienstverhältnis beendet ist, die für Bewerber für ein Beschäftigungsverhältnis oder Personen, deren Beschäftigungsverhältnis beendet ist, geltenden Vorschriften und

3. für das Land, die Kommunen im Sinne von § 1 Abs. 1 des Kommunalverfassungsgesetzes und die der Aufsicht des Landes unterstehenden anderen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, die Dienstherrnenfähigkeit besitzen, die für Arbeitgeber geltenden Vorschriften

des Gendiagnostikgesetzes vom 31. Juli 2009 (BGBl. I S. 2529, 3672), geändert durch Artikel 2 Abs. 31 und Artikel 4 Abs. 18 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154, 3166, 3201).

§ 29

Fernmessen und Fernwirken

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen, wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen andere Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist; dies gilt nicht für Fernmess- und Fernwirkdienste der Versorgungsunternehmen. Der Betroffene kann seine Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass der Betroffene nach Absatz 1 Satz 1 oder 2 einwilligt. Verweigert oder widerruft er seine Einwilligung, so dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(3) Soweit im Rahmen von Fernmess- oder Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet oder genutzt werden. Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 30

Optisch-elektronische Beobachtung

(1) Öffentliche Stellen dürfen öffentlich zugängliche Bereiche durch optisch-elektronische Einrichtungen beobachten, soweit dies,

1. zur Wahrnehmung des Hausrechts,

2. zum Schutz des Eigentums oder Besitzes oder

3. zur Kontrolle von Zugangsberechtigungen, insbesondere in Durchführung technischer und organisatorischer Maßnahmen nach § 6, erforderlich ist und keine

Anhaltspunkte bestehen, dass schutzwürdige Interessen der Personen, die sich im Aufnahmebereich der Einrichtung befinden, überwiegen.

(2) Die Möglichkeit der Beobachtung muss für Betroffene, die sich im Aufnahmebereich der optisch-elektronischen Einrichtung befinden, erkennbar sein.

(3) Personenbezogene Daten dürfen nur erhoben oder gespeichert werden, wenn dies zur Erreichung der in Absatz 1 genannten Zwecke erforderlich oder unvermeidlich ist. Die Daten dürfen für einen anderen Zweck nur nach Maßgabe von § 10 Abs. 2 Nrn. 1 bis 3 und 6 bis 8 gespeichert, verändert, übermittelt oder genutzt werden.

(4) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

(5) Der Einsatz von Attrappen ist unter den Voraussetzungen der Absätze 1 und 2 zulässig.

§ 30 a

Öffentliche Auszeichnungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen dürfen personenbezogene Daten auch ohne Kenntnis des Betroffenen erhoben, verarbeitet oder genutzt werden. Eine Verarbeitung oder Nutzung dieser Daten für andere Zwecke ist nur mit Einwilligung des Betroffenen zulässig.

(2) Auf Ersuchen der zuständigen Stellen dürfen andere öffentliche Stellen die für die Vorbereitung der Auszeichnung erforderlichen Daten übermitteln.

(3) § 15 findet keine Anwendung.

Sechster Abschnitt
Schlussvorschriften

§ 31

Strafvorschriften

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, unbefugt von diesem Gesetz oder einer anderen Rechtsvorschrift über den Datenschutz geschützte personenbezogene Daten, die nicht allgemein zugänglich sind,

1. erhebt, verarbeitet oder nutzt,
2. zum Abruf durch Dritte mittels automatisierten Verfahrens bereithält oder
3. abrufen oder sich oder einem anderen aus Dateien verschafft,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen,

1. die Übermittlung von durch dieses Gesetz oder eine andere Rechtsvorschrift über den Datenschutz geschützten personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
2. entgegen § 12 Abs. 4 Satz 1, § 26 Abs. 2 Satz 1 oder § 27 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt,
3. entgegen § 27 Abs. 3 Satz 3 die in § 27 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt oder
4. entgegen § 18 Abs. 4 Satz 3 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt personenbezogene Daten zu einem Zweck verwendet, zu dem ihm die Daten nicht übermittelt worden sind.

(3) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 31 a Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich die Übermittlung von durch dieses Gesetz oder eine andere Rechtsvorschrift über den Datenschutz geschützten personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht.

(2) Ordnungswidrig handelt auch, wer vorsätzlich oder fahrlässig

1. entgegen § 12 Abs. 4 Satz 1, § 26 Abs. 2 Satz 1 oder § 27 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt,

2. entgegen § 27 Abs. 3 Satz 3 die in § 27 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt oder

3. entgegen § 18 Abs. 4 Satz 3 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt personenbezogene Daten zu einem Zweck verwendet, zu dem ihm die Daten nicht übermittelt worden sind.

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 2 Nr. 2 mit einer Geldbuße bis zu 25000 Euro und in den übrigen Fällen der Absätze 1 und 2 mit einer Geldbuße bis zu 250000 Euro geahndet werden.

§ 31 b Gerichtlicher Rechtsschutz

(1) Dem Verwaltungsgericht Magdeburg werden für die Bezirke aller Verwaltungsgerichte des Landes die Rechtsstreitigkeiten nach Artikel 78 Abs. 1 und 2 der Datenschutz-Grundverordnung und Artikel 53 Abs. 1 und 2 der Richtlinie (EU) 2016/680 zugewiesen. Satz 1 gilt nicht für Straf- und Bußgeldverfahren.

(2) Ein Vorverfahren findet nicht statt.

(3) Auch eine Landesbehörde kann gegen eine sie betreffende Anordnung des Landesbeauftragten für den Datenschutz Anfechtungsklage erheben.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn sich der Landesbeauftragte für den Datenschutz nicht mit einer Beschwerde nach § 19 befasst oder den Beschwerdeführer nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis setzt.

(5) Die Absätze 1 bis 4 gelten entsprechend für Anordnungen oder Unterlassungen des Landesbeauftragten für den Datenschutz, die ihre Grundlage außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung und der Richtlinie (EU) 2016/680 im nationalen Recht haben.

§ 32

Übergangsvorschriften

(1) Nach bisherigem Recht erstellte Dateifestlegungen nach § 14 Abs. 2 Satz 2, Errichtungsanordnungen nach § 33 Abs. 1 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt in der vor dem In-Kraft-Treten des Zweiten Gesetzes zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt vom 20. Juli 2000 (GVBl. LSA S. 444) geltenden Fassung und Dateianordnungen nach § 13 Abs. 1 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt gelten als Verfahrensverzeichnisse im Sinne des § 14 Abs. 3 Satz 1. Die Einsicht in diese Verzeichnisse ist nur in dem nach § 14 Abs. 5 vorgesehenen Umfang möglich. Fehlen in den Verzeichnissen nach Satz 1 einzelne Festlegungen nach § 14 Abs. 3 Satz 1 Nrn. 1 bis 9, sind diese gelegentlich der nächsten Fortschreibung oder im Fall der ersten Einsichtnahme nach § 14 Abs. 5 nachzuholen.

(2) Bestehende gemeinsame Verfahren und Verfahren im Sinne des § 7a Abs. 4 sind bis zum Ablauf des 31. Dezember 2016 an die Anforderungen des § 7a in Verbindung mit § 7 Abs. 2 und 4 anzupassen und dem Landesbeauftragten für den Datenschutz entsprechend § 7 Abs. 3 anzuzeigen.

§ 33

Personalrechtliche Überleitungsvorschriften zum Gesetz zur Organisationsfortentwicklung des Landes- beauftragten für den Datenschutz und zur Änderung des Informationszugangsgesetzes Sachsen-Anhalt

(1) Beamte, die bis zum 5. Mai 2018 in der beim Präsidenten des Landtages eingerichteten Geschäftsstelle des Landesbeauftragten für den Datenschutz tätig waren, gehen zum 6. Mai 2018 zur Geschäftsstelle des Landesbeauftragten für den Datenschutz über. Einer Versetzung bedarf es nicht.

(2) Der Landesbeauftragte für den Datenschutz tritt am 6. Mai 2018 kraft Gesetzes in die Rechte und Pflichten des Arbeitgebers der Tarifbeschäftigten, die mit Aufgaben der beim Präsidenten des Landtages eingerichteten Geschäftsstelle des Landesbeauftragten für den Datenschutz betraut waren, ein.

(3) Der leitende Beamte der beim Präsidenten des Landtages eingerichteten Geschäftsstelle des Landesbeauftragten für den Datenschutz ist ab dem 6. Mai 2018 leitender Beamter der Geschäftsstelle des Landesbeauftragten für den Datenschutz und führt ab dem 6. Mai 2018 die Amtsbezeichnung "Direktor der Geschäftsstelle des Landesbeauftragten für den Datenschutz".

(4) Bis zur Wahl eines neuen Personalrats der Geschäftsstelle des Landesbeauftragten für den Datenschutz nimmt der Personalrat im Geschäftsbereich des Präsidenten des Landtages die Aufgaben wahr, längstens jedoch bis zum 31. Dezember 2018. Die in der beim Präsidenten des Landtages eingerichteten Geschäftsstelle des Landesbeauftragten für den Datenschutz geltenden Dienstvereinbarungen nach dem Landespersonalvertretungsgesetz Sachsen-Anhalt gelten in der Geschäftsstelle des Landesbeauftragten für den Datenschutz längstens bis zum 30. Juni 2019 fort, wenn sie nicht durch Zeitablauf, Kündigung oder Aufhebungsvereinbarung außer Kraft treten. Für die ehrenamtliche Gleichstellungsbeauftragte und den ehrenamtlichen Schwerbehindertenbeauftragten gilt Satz 1 entsprechend.

§ 34 Evaluierung

Das Verfahren zur Aufstellung des Einzelplans des Landesbeauftragten für den Datenschutz wird spätestens im Jahr 2020 einer Evaluierung unterzogen. Die Landesregierung berichtet dem Landtag schriftlich über das Ergebnis der Evaluierung.

§ 35 (aufgehoben)

§ 36 Sprachliche Gleichstellung

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

§ 36 a
Einschränkung von Grundrechten

Durch dieses Gesetz wird das Recht auf Schutz personenbezogener Daten im Sinne des Artikels 6 Abs. 1 Satz 1 der Verfassung des Landes Sachsen-Anhalt eingeschränkt.

§ 37
(In-Kraft-Treten)