Amtliche Abkürzung:	LDSG
Ausfertigungsdatum:	12.06.2018
Gültig ab:	21.06.2018
Dokumenttyp:	Gesetz
Quelle:	Land Baden-Württemberg
Fundstelle:	GBl. 2018, 173
Gliederungs-Nr:	2040

Landesdatenschutzgesetz
(LDSG)
Vom 12. Juni 2018*

Zum 02.04.2026 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: letzte berücksichtigte Änderung: mehrfach geändert sowie §§ 2a, 3a, 7a, 9a, 11a, 12a, 17a, 17b, 18a, 18b und 27a neu eingefügt und § 6 neu gefasst durch Artikel 1 des Gesetzes vom 10. Februar 2026 (GBl. 2026 Nr. 19)

Fußnoten

*) Verkündet als Artikel 1 des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 vom 12. Juni 2018 (GBl. S. 173)

Nichtamtliches Inhaltsverzeichnis

Titel	Gültig ab
Landesdatenschutzgesetz (LDSG) vom 12. Juni 2018	21.06.2018
Inhaltsverzeichnis	28.02.2026
ABSCHNITT 1 - Allgemeine Bestimmungen	21.06.2018
§ 1 - Zweck des Gesetzes	21.06.2018
§ 2 - Anwendungsbereich	28.02.2026
§ 2a - Begriffsbestimmungen	28.02.2026
§ 3 - Sicherstellung des Datenschutzes	28.02.2026
§ 3a - Nutzung von KI-Systemen	28.02.2026
ABSCHNITT 2 - Rechtsgrundlagen der Verarbeitung personenbezogener Daten	21.06.2018
§ 4 - Zulässigkeit der Verarbeitung personenbezogener Daten	28.02.2026
§ 5 - Datenverarbeitung zu anderen Zwecken	28.02.2026
§ 6 - Übermittlung personenbezogener Daten	28.02.2026
§ 7 - Datenverarbeitung in der gemeinsamen Dienststelle	21.06.2018
§ 7a - Auftragsverarbeitung; Verordnungsermächtigung	28.02.2026
ABSCHNITT 3 - Rechte der betroffenen Person	21.06.2018

Titel	Gültig ab
§ 8 - Beschränkung der Informationspflicht	28.02.2026
§ 9 - Beschränkung des Auskunftsrechts	21.06.2018
§ 9a - Beschränkung des Rechts auf Berichtigung	28.02.2026
§ 10 - Beschränkung des Rechts auf Löschung	28.02.2026
§ 11 - Beschränkung der Benachrichtigungspflicht	21.06.2018
ABSCHNITT 4 - Besondere Verarbeitungssituationen	21.06.2018
§ 11a - Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen	28.02.2026
§ 12 - Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen	21.06.2018
§ 12a - Verarbeitung zu Zwecken der parlamentarischen Kontrolle	28.02.2026
§ 13 - Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken	28.02.2026
§ 14 - Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken	21.06.2018
§ 15 - Datenverarbeitung bei Dienst- und Arbeitsverhältnissen	28.02.2026
§ 16 - Öffentliche Auszeichnungen und Ehrungen	28.02.2026
§ 17 - Verarbeitung personenbezogener Daten im öffentlichen Interesse	28.02.2026
§ 17a - Absicherung des Zugangs zu personenbezogenen Daten	28.02.2026
§ 17b - Öffentlichkeitsarbeit	28.02.2026
§ 18 - Videoschutz öffentlich zugänglicher Räume	28.02.2026
§ 18a - Videoüberwachung nicht öffentlich zugänglicher Räume	28.02.2026
§ 18b - Sonstige technische Überwachung	28.02.2026
§ 19 - Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken	21.06.2018
ABSCHNITT 5 - Datenverarbeitung im Landtag	06.08.2025
§ 19a - Verarbeitung personenbezogener Daten im Landtag	06.08.2025
§ 19b - Zulässigkeit der Datenverarbeitung	06.08.2025
§ 19c - Verantwortlicher	06.08.2025
§ 19d - Rechte betroffener Personen	06.08.2025
§ 19e - Datenschutzaufsicht	06.08.2025
ABSCHNITT 6 - Unabhängige Aufsichtsbehörden	06.08.2025
§ 20 - Errichtung	21.06.2018

Titel	Gültig ab
§ 21 - Unabhängigkeit	21.06.2018
§ 22 - Ernennung und Amtszeit	21.06.2018
§ 23 - Amtsverhältnis	01.01.2019
§ 24 - Rechte und Pflichten	21.06.2018
§ 25 - Aufgaben und Befugnisse	21.06.2018
§ 26 - Pflicht zur Unterstützung	21.06.2018
§ 27 - Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz	01.12.2025
§ 27a - Datenschutzaufsicht für digitale Dienste	28.02.2026
ABSCHNITT 7 - Sanktionen	06.08.2025
§ 28 - Ordnungswidrigkeiten	21.06.2018
§ 29 - Strafvorschrift	21.06.2018
ABSCHNITT 8 - Übergangsbestimmungen	06.08.2025
§ 30 - Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes	21.06.2018
§ 31 - Überleitungsvorschriften	21.06.2018

INHALTSÜBERSICHT

Abschnitt 1: Allgemeine Bestimmungen

§ 1 Zweck des Gesetzes

§ 2 Anwendungsbereich

§ 2a Begriffsbestimmungen

§ 3 Sicherstellung des Datenschutzes

§ 3a Nutzung von KI-Systemen

Abschnitt 2: Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 4 Zulässigkeit der Verarbeitung personenbezogener Daten

§ 5 Datenverarbeitung zu anderen Zwecken (Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679)

§ 6 Übermittlung personenbezogener Daten

§ 7 Datenverarbeitung in der gemeinsamen Dienststelle

§ 7a Auftragsverarbeitung; Verordnungsermächtigung

Abschnitt 3: Rechte der betroffenen Person

§ 8 Beschränkung der Informationspflicht (Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679)

§ 9 Beschränkung des Auskunftsrechts (Ergänzung zu Artikel 15 der Verordnung [EU] 2016/679)

§ 9a Beschränkung des Rechts auf Berichtigung

§ 10 Beschränkung des Rechts auf Löschung (Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679)

§ 11 Beschränkung der Benachrichtigungspflicht (Ergänzung zu Artikel 34 der Verordnung [EU] 2016/679)
Abschnitt 4: Besondere Verarbeitungssituationen
§ 11a Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen
§ 12 Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen
§ 12a Verarbeitung zu Zwecken der parlamentarischen Kontrolle
§ 13 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
§ 14 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken
§ 15 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
§ 16 Öffentliche Auszeichnungen und Ehrungen
§ 17 Verarbeitung personenbezogener Daten im öffentlichen Interesse
§ 17a Absicherung des Zugangs zu personenbezogenen Daten
§ 17b Öffentlichkeitsarbeit
§ 18 Videoschutz öffentlich zugänglicher Räume
§ 18a Videoüberwachung nicht öffentlich zugänglicher Räum
§ 18b Sonstige technische Überwachung
§ 19 Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken
Abschnitt 5: Datenverarbeitung im Landtag
§ 19a Verarbeitung personenbezogener Daten im Landtag
§ 19b Zulässigkeit der Datenverarbeitung
§ 19c Verantwortlicher
§ 19d Rechte betroffener Personen
§ 19e Datenschutzaufsicht
Abschnitt 6: Unabhängige Aufsichtsbehörden
§ 20 Errichtung
§ 21 Unabhängigkeit
§ 22 Ernennung und Amtszeit
§ 23 Amtsverhältnis
§ 24 Rechte und Pflichten
§ 25 Aufgaben und Befugnisse
§ 26 Pflicht zur Unterstützung
§ 27 Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz
§ 27a Datenschutzaufsicht für digitale Dienste
Abschnitt 7: Sanktionen
§ 28 Ordnungswidrigkeiten (Ergänzung zu Artikel 83 Absatz 7 der Verordnung [EU] 2016/679)
§ 29 Strafvorschrift (Ergänzung zu Artikel 84 der Verordnung [EU] 2016/679)
Abschnitt 8: Übergangsbestimmungen
§ 30 Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes
§ 31 Überleitungsvorschriften

ABSCHNITT 1
Allgemeine Bestimmungen

§ 1
Zweck des Gesetzes

Dieses Gesetz trifft ergänzende Regelungen zur Durchführung 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung sowie Regelungen für die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt nach Maßgabe von Absatz 2 bis 7 für die Verarbeitung personenbezogener Daten durch Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses oder ein anderes Gesetz nichts anderes bestimmt. Dieses Gesetz gilt nicht für die Verarbeitung personenbezogener Daten

1. durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes,

2. beim Vollzug des Landessicherheitsüberprüfungsgesetzes,

3. durch die Polizei sowie die Gerichte, Staatsanwaltschaften, das Justizministerium und die Justizvollzugsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit und

4. durch andere für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständige Stellen,

soweit besondere Rechtsvorschriften keine abweichenden Regelungen treffen. § 30 gilt auch für die Verarbeitung personenbezogener Daten nach Satz 3.

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts nach Satz 1 an einer weiteren Vereinigung des privaten Rechts, findet Satz 1 entsprechende Anwendung. Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Vorschriften dieses Gesetzes gehen denen des Landesverwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Soweit die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit stattfindet, die nicht in den sachlichen Anwendungsbereich der Verordnung (EU) 2016/679 oder 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. Mai 2016, S. 89) fällt, gelten die Regelungen der Verordnung (EU) 2016/679 und dieses Gesetz entsprechend, sofern die Verarbeitung nicht in besonderen Rechtsvorschriften geregelt ist. Die Artikel 30, 35 und 36 der Verordnung (EU) 2016/679 gelten nur, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Auf die Prüfungstätigkeit des Rechnungshofs und der Gemeindeprüfungsanstalt Baden-Württemberg finden Artikel 30 und Kapitel VI der Verordnung (EU) 2016/679 sowie §§ 25 und 26 dieses Gesetzes keine Anwendung.

(5) Dieses Gesetz gilt für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Abweichend hiervon gelten die §§ 2a, 3a, 4 Absatz 2, §§ 9a, 10 Absatz 4 und § 11a für Gerichte auch außerhalb von Verwaltungsangelegenheiten bei der Datenverarbeitung mittels künstlicher Intelligenz (KI) in Bezug auf KI-Systeme und KI-Modelle, soweit nicht besondere Rechtsvorschriften über Verfahren der Rechtspflege auf die Datenverarbeitung anzuwenden sind, die den Vorschriften dieses Gesetzes vorgehen; Abschnitt 5 gilt nicht. Absatz 1 Satz 3 Nummer 3 bleibt unberührt.

(6) Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nichtöffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden. Satz 1 gilt nicht für Zweckverbände.

(7) Die Vorschriften dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten zur Ausübung des Begnadigungsrechts.

§ 2a
Begriffsbestimmungen

(1) Für die in diesem Gesetz verwendeten Begriffe sind, soweit nichts anderes bestimmt ist, die Begriffsbestimmungen der Verordnung (EU) 2016/679 in der jeweils geltenden Fassung maßgeblich.

(2) Ein System künstlicher Intelligenz (KI-System) ist ein KI-System im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L vom 12.7.2024) in der jeweils geltenden Fassung.

(3) Ein Modell künstlicher Intelligenz (KI-Modell) ist ein KI-Modell mit allgemeinem Verwendungszweck im Sinne des Artikels 3 Nummer 63 der Verordnung über künstliche Intelligenz oder ein vergleichbares Modell, welches lediglich einen oder mehrere spezielle Verwendungszwecke aufweist, einschließlich KI-Modelle für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen.

§ 3
Sicherstellung des Datenschutzes

(1) Bei der Datenverarbeitung sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Dabei sind der Stand der Technik, die Implementierungs-

kosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Technische und organisatorische Maßnahmen müssen sicherstellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt; zu den erforderlichen Maßnahmen können insbesondere gehören:

1. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,

2. die Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten,

3. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,

4. die Pseudonymisierung personenbezogener Daten,

5. die Verschlüsselung personenbezogener Daten,

6. die Abschottung von internen Systemen vor unbefugten Zugriffen aus öffentlichen Telekommunikationsnetzen,

7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und

9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung [EU] 2016/679 sicherstellen.

(2) Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das Datengeheimnis besteht nach Beendigung ihrer Tätigkeit fort.

§ 3a
Nutzung von KI-Systemen

Die Nutzung von KI-Systemen zur Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn die Voraussetzungen für die Verarbeitung der personenbezogenen Daten als solche gegeben sind.

ABSCHNITT 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 4
Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.

(2) Öffentliche Stellen dürfen, soweit zur Aufgabenerfüllung oder zur Ausübung öffentlicher Gewalt erforderlich, aus den rechtmäßig gespeicherten Daten synthetische Daten herstellen sowie rechtmäßig gespeicherte Daten auf sonstige Weise anonymisieren. Besondere Kategorien personenbezogener Daten dürfen entsprechend Satz 1 verarbeitet werden, wenn zusätzlich die Voraussetzungen des Artikels 9 Absatz 2 der Verordnung (EU) 2016/679 oder einer speziellen Rechtsgrundlage vorliegen.

§ 5
Datenverarbeitung zu anderen Zwecken

(Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679)

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist unbeschadet der Bestimmungen der Verordnung [EU] 2016/679 zulässig, wenn

1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist; das Gemeinwohl ist gleichzusetzen mit den gesetzlich anerkannten allgemeinen öffentlichen Interessen,

2. sie zum Schutz der betroffenen Person oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist,

3. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,

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

5. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zwecks ihre Einwilligung nicht erteilen würde,

soweit die Verarbeitung notwendig und verhältnismäßig ist.

(2) Eine Verarbeitung gilt als mit den ursprünglichen Zwecken vereinbar, wenn sie

1. für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen benötigt wird oder

2. der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen oder der Prüfung und Wartung von automatisierten Verfahren dient.

Dies gilt auch für die Verarbeitung zu eigenen Aus- und Fortbildungszwecken, soweit schutzwürdige Belange der betroffenen Person nicht entgegenstehen.

(3) Abweichend von Artikel 13 der Verordnung [EU] 2016/679 erfolgt eine Information der betroffenen Person über die Datenverarbeitung nach Absatz 1 Nummern 1 bis 4 nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde und die Interessen der öffentlichen Stelle an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

(4) Personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verarbeitet werden, dürfen nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Beschäftigten verarbeitet werden oder soweit dies zur Verhütung oder Verfolgung von Straftaten gegen Leib, Leben oder Freiheit einer Person erforderlich ist.

§ 6
Übermittlung personenbezogener Daten

(1) Die Übermittlung personenbezogener Daten zu anderen als ihren Erhebungszwecken an Stellen innerhalb des öffentlichen Bereichs ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden öffentlichen Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 5 zulassen würden.

(2) Die Übermittlung personenbezogener Daten zu anderen als ihren Erhebungszwecken an nichtöffentliche 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 Verarbeitung nach § 5 zulassen würden,

2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder

3. es zur Geltendmachung, Ausübung von Rechtsansprüchen oder Verteidigung gegen Rechtsansprüche Dritter erforderlich ist.

(3) Für die Übermittlung an Stellen in anderen Mitgliedstaaten der Europäischen Union, in Vertragsstaaten des Europäischen Wirtschaftsraums oder an Organe und Einrichtungen der Europäischen Union gelten Absatz 1 und 4 sowie die §§ 4 und 5 entsprechend, soweit nichts anderes bestimmt ist.

(4) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde öffentliche Stelle. Erfolgt die Übermittlung aufgrund eines automatisierten Verfahrens, welches die Übermittlung personenbezogener Daten durch Abruf ermöglicht oder aufgrund eines Ersuchens einer öffentlichen Stelle im Geltungsbereich des Grundgesetzes, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs oder des Ersuchens die abrufende oder ersuchende Stelle; die übermittelnde Stelle prüft die Zulässigkeit des Abrufs oder die Rechtmäßigkeit des Ersuchens nur, wenn dazu Anlass besteht.

(5) Automatisierte Abrufverfahren oder eine gemeinsame automatisierte Datei, in oder aus der mehrere öffentliche Stellen personenbezogene Daten verarbeiten, dürfen eingerichtet werden, soweit die rechtlichen Voraussetzungen zur Übermittlung vorliegen und die Einrichtung 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. Automatisierte Abrufverfahren für Abrufe aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung offenstehen, dürfen ungeachtet der Bestimmungen in Satz 1 eingerichtet werden.

§ 7
Datenverarbeitung in der gemeinsamen Dienststelle

(1) Die örtlich zuständige öffentliche Stelle darf personenbezogene Daten nur den in einer gemeinsamen Dienststelle nach § 16 Absatz 1 des Landesverwaltungsgesetzes beschäftigten eigenen Bediensteten zur Verarbeitung für eigene Aufgaben überlassen. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass ein Zugriff auf die Daten nach Satz 1 durch Bedienstete anderer Behörden nicht möglich ist. Soweit dies zur Sicherstellung einer sachgerechten Erledigung der eigenen Aufgaben erforderlich ist, darf die örtlich zuständige öffentliche Stelle auch Bediensteten anderer Behörden, die in der gemeinsamen Dienststelle beschäftigt sind, personenbezogene Daten zur Verarbeitung überlassen. Im Rahmen einer solchen Datenverarbeitung unterliegen die Bediensteten anderer Behörden den Weisungen der örtlich zuständigen öffentlichen Stelle. Hinsichtlich der Daten, die sie im Rahmen ihrer Tätigkeit für die fremde Behörde zur Kenntnis nehmen, haben sie das Datengeheimnis gegenüber ihrer eigenen Dienststelle zu wahren. Das Nähere ist durch gemeinsame interne Dienstanweisungen zu regeln. Verantwortlicher bleibt die örtlich zuständige öffentliche Stelle.

(2) Für gemeinsame Dienststellen nach § 27 des Gesetzes über kommunale Zusammenarbeit gilt Absatz 1 entsprechend.

§ 7a
Auftragsverarbeitung; Verordnungsermächtigung

(1) Soweit eine staatliche Behörde oder eine Anstalt in alleiniger Trägerschaft des Landes im Auftrag einer anderen öffentlichen Stelle, welche verpflichtet oder berechtigt ist, das Dienstleistungsangebot der staatlichen Behörde oder der Anstalt für die Erbringung von Dienstleistungen zu nutzen, personenbezogene Daten nach Artikel 28 der Verordnung (EU) 2016/679 verarbeitet, erfolgt dies auf der Grundlage eines Auftragsverarbeitungsvertrags nach Artikel 28 Absatz 3 Satz 1 Alternative 1 der Verordnung (EU) 2016/679 nach Maßgabe der folgenden Bestimmungen. Zur Begründung des Auftragsverarbeitungsverhältnisses durch Vertrag teilt die verantwortliche öffentliche Stelle der staatlichen Behörde oder der Anstalt als Auftragsverarbeiter in Textform mit:

1. Gegenstand und Dauer der Verarbeitung,

2. Art und Zweck der Verarbeitung,

3. die Art der personenbezogenen Daten und

4. die Kategorien betroffener Personen.

Die Sätze 1 und 2 gelten nicht für die staatlichen Hochschulen.

(2) Die Landesregierung wird ermächtigt, durch Rechtsverordnung

1. die Pflichten und Rechte der verantwortlichen öffentlichen Stelle sowie des Auftragsverarbeiters festzulegen,

2. die Maßgaben nach Artikel 28 Absatz 3 Satz 2 der Verordnung (EU) 2016/679 für eine Auftragsverarbeitung durch den Auftragsverarbeiter zu bestimmen,

3. die Verpflichtung weiterer Auftragsverarbeiter, deren Dienste die staatliche Behörde oder die Anstalt in Anspruch nimmt, auf dieselben Datenschutzpflichten zu regeln sowie

4. weitere Nutzungsbedingungen festzulegen,

die Bestandteile der Auftragsverarbeitungsverträge nach Absatz 1 werden. Bestehende einzelvertragliche Regelungen zur Auftragsverarbeitung werden entsprechend der Rechtsverordnung ersetzt. Abweichende einzelvertragliche Vereinbarungen sind im Rahmen des nach Artikel 28 der Verordnung (EU) 2016/679 zulässigen Regelungsinhalts möglich.

(3) Der Auftrag zur Verarbeitung personenbezogener Daten kann auch durch die Fachaufsichtsbehörde mit Wirkung für die ihrer Aufsicht unterliegenden Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten.

ABSCHNITT 3
Rechte der betroffenen Person

§ 8
Beschränkung der Informationspflicht

(Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679)

(1) Eine Pflicht zur Information der betroffenen Person besteht nicht, soweit und solange

1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

2. die Information die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung gefährden würde,

3. die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde,

4. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen oder

5. die Information voraussichtlich die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks unmöglich macht oder ernsthaft beeinträchtigt

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1 Nummern 1 oder 2, ergreift die öffentliche Stelle geeignete Maßnahmen zum Schutz der berechtigten Interessen

der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 oder Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten an Staatsanwaltschaften, Polizeibehörden oder den Polizeivollzugsdienst, Verfassungsschutzbehörden und, soweit sie in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung personenbezogene Daten speichern, an Behörden der Finanzverwaltung, ist diesen Behörden vorab Gelegenheit zur Stellungnahme zu geben. Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, an andere Behörden des Bundesministers der Verteidigung. Satz 1 und 2 gelten entsprechend für die Information über die Herkunft der Daten von den genannten Behörden.

(4) Die Gründe für das Absehen von der Information sind zu dokumentieren.

§ 9
Beschränkung des Auskunftsrechts

(Ergänzung zu Artikel 15 der Verordnung [EU] 2016/679)

(1) Die Auskunftserteilung kann aus den in § 8 Absatz 1 Nummern 1 bis 4 genannten Gründen abgelehnt werden. Die betroffene Person kann ferner keine Auskunft verlangen, soweit und solange die personenbezogenen Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

(2) Sofern die öffentliche Stelle eine große Menge von Informationen über die betroffene Person verarbeitet, kann sie sich auf die Benennung der Verarbeitungsvorgänge und der Art der verarbeiteten Daten beschränken, wenn sie im Übrigen von der betroffenen Person eine Präzisierung verlangt, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht. Kommt die betroffene Person dem Verlangen nicht nach, kann die Auskunft verweigert werden, soweit die Auskunftserteilung einen unzumutbaren Aufwand auslösen würde.

(3) § 8 Absatz 2 gilt entsprechend.

(4) Die Ablehnung der Auskunftserteilung ist zu begründen, es sei denn, durch die Mitteilung der Gründe würde der mit der Auskunftsverweigerung verfolgte Zweck gefährdet. In diesem Fall sind die Gründe der Auskunftsverweigerung zu dokumentieren. Die betroffene Person ist auf die Möglichkeit der Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz hinzuweisen.

(5) Wird der betroffenen Person keine Auskunft erteilt, ist sie auf ihr Verlangen der oder 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 der oder des Landesbeauftragten für den Datenschutz an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand der öffentlichen Stelle zulassen, sofern diese nicht einer weiter gehenden Auskunft zustimmt.

§ 9a
Beschränkung des Rechts auf Berichtigung

(Ergänzung zu Artikel 16 der Verordnung [EU] 2016/679)

Die Berichtigung von mit KI-Systemen und KI-Modellen verarbeiteten personenbezogenen Daten kann nicht verlangt werden, solange dies nur mit einem unverhältnismäßig hohen Aufwand an technischen oder wirtschaftlichen Mitteln oder erheblichen ökologischen Folgen möglich wäre oder solange der rechtmäßige Zweck der Verarbeitung erheblich erschwert würde. An die Stelle einer Berichtigung treten ein Filter oder sonstige geeignete Maßnahmen, soweit der Aufwand verhältnismäßig ist. Zur Umsetzung der Maßnahmen nach Satz 2 dürfen personenbezogene Daten gespeichert werden, soweit dies zwingend erforderlich ist. Diese personenbezogenen Daten dürfen nur für diesen Zweck verarbeitet werden.

§ 10
Beschränkung des Rechts auf Löschung

(Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679)

(1) Die Bestimmungen des Landesarchivgesetzes zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten bleiben unberührt.

(2) Die Pflicht zur Löschung personenbezogener Daten nach Artikel 17 der Verordnung [EU] 2016/679 besteht nicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. Die öffentliche Stelle unterrichtet die betroffene Person über das Absehen von der Löschung und die Einschränkung der Verarbeitung. Widerspricht die betroffene Person dem Absehen von der Löschung, sind die Daten zu löschen.

(3) Ist eine Löschung im Falle nichtautomatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht der öffentlichen Stelle zur Löschung personenbezogener Daten nicht. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(4) Für die Löschung gilt § 9a entsprechend.

§ 11
Beschränkung der Benachrichtigungspflicht

(Ergänzung zu Artikel 34 der Verordnung [EU] 2016/679)

Die öffentliche Stelle kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person absehen, soweit und solange

1. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

2. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte anderer Personen geheim gehalten werden müssen oder

3. die Benachrichtigung die Sicherheit von Systemen der Informationstechnologie gefährden würde

und deswegen das Interesse der betroffenen Person an der Benachrichtigung zurücktreten muss.

ABSCHNITT 4
Besondere Verarbeitungssituationen

§ 11a
Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen

Für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen dürfen zum Zweck der Erfüllung von in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben oder zur Ausübung öffentlicher Gewalt personenbezogene Daten weiterverarbeitet werden, wenn der Zweck des KI-Systems oder KI-Modells auf andere Weise nicht effektiv erreicht werden kann. Besondere Kategorien personenbezogener Daten dürfen weiterverarbeitet werden, wenn zusätzlich ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder einer speziellen Rechtsgrundlage vorliegt.

§ 12
Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die der öffentlichen Stelle in Ausübung einer Berufs- oder Amtspflicht übermittelt worden sind, dürfen von der öffentlichen Stelle nur für den Zweck verarbeitet werden, für den sie die Daten erhalten hat. Artikel 9 der Verordnung (EU) 2016/679 bleibt unberührt.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet werden, wenn

1. die Änderung des Zwecks durch besonderes Gesetz zugelassen ist oder

2. die Voraussetzungen des § 5 Absatz 1 Nummern 1 bis 3, § 13 Absatz 1 oder § 14 Absatz 1 vorliegen und die zur Verschwiegenheit verpflichtete Stelle zugestimmt hat.

§ 12a
Verarbeitung zu Zwecken der parlamentarischen Kontrolle

Die Landesregierung darf personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten zur Beantwortung parlamentarischer Anfragen und Anträge sowie zur Vorlage von Unterlagen und Berichten an den Landtag in dem dafür erforderlichen Umfang verarbeiten. Eine Übermittlung der personenbezogenen Daten zu einem der in Satz 1 genannten Zwecke ist nicht zulässig, wenn dies wegen des streng persönlichen Charakters der Daten für die betroffene Person unzumutbar ist oder wenn der Eingriff in ihr informationelles Selbstbestimmungsrecht unverhältnismäßig ist. Satz 2 gilt nicht, wenn durch Regelungen des Landtags oder sonstige geeignete Maßnahmen sichergestellt ist, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden.

§ 13
Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten und vorhandene Daten der genannten Art weiterverarbeiten, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen.

(2) Für wissenschaftliche Forschungszwecke ist die Verarbeitung allgemein zugänglicher personenbezogener Daten zulässig, es sei denn, dass schutzwürdige Interessen der betroffenen Person der Datenverarbeitung entgegenstehen.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis zur Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert. Zur Wahrung der Interessen der betroffenen Person sind weitere angemessene und spezifische Maßnahmen nach § 3 Absatz 1 zu treffen.

(4) Die wissenschaftliche oder historische Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(5) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten an nichtöffentliche Stellen zu deren gemeinwohlbezogenen Forschungszwecken übermitteln, wenn dies zur Erfüllung des Forschungszwecks erforderlich ist und die Interessen der forschenden Dritten die Interessen der betroffenen Personen überwiegen. Absatz 3 gilt entsprechend. Die Übermittlung darf nur erfolgen, wenn die Empfänger sich gegenüber der übermittelnden Stelle verpflichten und die Gewähr dafür bieten, Maßnahmen entsprechend § 3 einschließlich der Geheimhaltung zu treffen, die Daten zu anonymisieren, sobald der Personenbezug für das Forschungsvorhaben nicht mehr erforderlich ist, die Daten nicht an Dritte weiterzugeben und der übermittelnden Stelle jederzeit auf Verlangen die Einhaltung dieser Verpflichtungen nachzuweisen.

(6) Die in Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der jeweiligen Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

§ 14
Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist.

(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Anga-

ben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Artikel 18, 19, 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

(5) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten und von diesem nicht als archivwürdig übernommen worden sind oder über die Übernahme nicht innerhalb der gesetzlichen Frist entschieden worden ist.

§ 15
Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Personenbezogene Daten von Bewerberinnen und Bewerbern sowie Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist. Die Verarbeitung ist auch zulässig, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

(2) Besondere Kategorien personenbezogener Daten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit die Verarbeitung erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen oder der betroffenen Person, auch aufgrund von Kollektivvereinbarungen, auf dem Gebiet des Dienst- und Arbeitsrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes zu genügen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Besondere Kategorien personenbezogener Daten dürfen entsprechend Satz 1 auch verarbeitet werden, soweit die Verarbeitung für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin oder der Beurteilung der Arbeitsfähigkeit der Beschäftigten erforderlich ist und wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

(3) Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbezogener Daten einer Bewerberin oder eines Bewerbers bei dem bisherigen Dienstherrn oder Arbeitgeber nur zulässig, wenn die betroffene Person eingewilligt hat. Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherren oder Arbeitgeber.

(4) Auf die Verarbeitung von Personalaktendaten von Arbeitnehmerinnen und Arbeitnehmern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamtinnen und Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbe-

amtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(5) Zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat oder schwerwiegende Pflichtverletzung begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(6) Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, die Verarbeitung ist durch Dienst- oder Betriebsvereinbarung geregelt oder die betroffene Person hat ausdrücklich eingewilligt und für die Erreichung der Zwecke steht in beiden Fällen kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung. Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.

(7) Eine Überwachung von Beschäftigten mit Hilfe optisch-elektronischer Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig. Absatz 5 bleibt unberührt. Für sonstige technische Einrichtungen gilt Absatz 1 entsprechend; die öffentliche Stelle muss geeignete Maßnahmen treffen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(8) Beschäftigte sind alle bei öffentlichen Stellen beschäftigten Personen unabhängig von der Rechtsform des Beschäftigungsverhältnisses. Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

(9) Die Beschäftigten sowie die Bewerberinnen und Bewerber sind über den Einsatz von KI-Systemen, die Dauer von deren Einsatz und deren Zwecke zu unterrichten.

§ 16
Öffentliche Auszeichnungen und Ehrungen

(1) Zur Entscheidung über öffentliche Auszeichnungen und Ehrungen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten verarbeitet werden; die öffentlichen Stellen sind insofern nicht zur Informations- und Auskunftserteilung gemäß Artikel 13 bis 15 der Verordnung (EU) 2016/679 verpflichtet. Satz 1 findet keine Anwendung, wenn der datenverarbeitenden Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der mit ihr verbundenen Datenverarbeitung widersprochen hat.

(2) Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden, es sei denn, sie werden für protokollarische Zwecke benötigt.

§ 17
Verarbeitung personenbezogener Daten im öffentlichen Interesse

Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses oder zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist und die Interessen der öffentlichen Stelle an der Datenverarbeitung die Interessen der betroffenen Person überwiegen. Die öffentliche Stelle trifft angemessene und spezifische Maßnahmen

zur Wahrung der Grundrechte und Interessen der betroffenen Person; hierfür sind mindestens die Maßnahmen nach § 3 Absatz 1 Nummern 1 bis 3 zu treffen.

§ 17a
Absicherung des Zugangs zu personenbezogenen Daten

(1) Für die Überprüfung der Zuverlässigkeit von Besuchern, Mitarbeitern von Unternehmen und anderen Organisationen sowie sonstigen Personen, die in sicherheits- oder sicherheitstechnisch relevante Bereiche gelangen sollen, für die öffentliche Stellen Verantwortung tragen, gilt § 15 Absatz 1 Satz 1 entsprechend mit der Maßgabe, dass zusätzlich die Einwilligung der betroffenen Person erforderlich ist. Besondere Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln dürfen nur aufgrund einer ausdrücklichen Einwilligung verarbeitet werden.

(2) Öffentliche Stellen dürfen personenbezogene Daten von Dritten oder Auftragsverarbeitern, die Zugang zu sicherheits- oder sicherheitstechnisch relevanten Datenverarbeitungsanlagen oder -geräten haben, verarbeiten, sofern dies für die Durchführung von Maßnahmen, einschließlich Schulungs- und Sensibilisierungsmaßnahmen, zur Gewährleistung der Informationssicherheit, der Cybersicherheit oder des Funktionierens kritischer Infrastruktur erforderlich ist. Die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, dass die betroffene Person ausdrücklich einwilligt und kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung steht; zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.

§ 17b
Öffentlichkeitsarbeit

(1) Soweit der öffentlichen Stelle ein Auftrag zur politischen Bildung oder zur Bürgerinformation obliegt, dürfen öffentliche Stellen unbeschadet sonstiger Bestimmungen personenbezogene Daten verarbeiten, um die Bürgerinnen und Bürger in angemessener Weise über ihre Arbeit zu informieren einschließlich werblicher Zwecke, sofern die schutzwürdigen Interessen betroffener Personen dem nicht entgegenstehen. In der Regel sind hiernach im erforderlichen Umfang insbesondere die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen und deren Verbreitung, die Verwendung von Kontakt- und Adressdaten für Kontaktpflege und Einladungen zu Veranstaltungen einschließlich deren Organisation zulässig. Die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen und deren Verbreitung unterliegt den Schranken der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266, 280) geändert worden ist, in der jeweils geltenden Fassung.

(2) Den betroffenen Personen ist Gelegenheit zum Widerspruch ohne Angabe von Gründen zu geben.

§ 18
Videoschutz öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Der Schutz von Leben, Gesundheit und Freiheit von Personen ist ein besonders wichtiges öffentliches Interesse. Sofern die Videoüberwachung zum Schutz von sicherheitsrelevanten Einrichtungen, Dienstgebäuden, Dienstfahrzeugen, Kulturgütern oder öffentlichen

Verkehrsmitteln und den dort oder in unmittelbarer Nähe jeweils befindlichen Personen und Sachen erforderlich ist, gilt Videoüberwachung als angemessen und verhältnismäßig.

(2) Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen; dabei sind mindestens der Verantwortliche mitsamt seinen Kontaktdaten sowie die Kontaktdaten des behördlichen Datenschutzbeauftragten mitzuteilen. Zudem ist darauf hinzuweisen, wo die weiteren Informationen des Verantwortlichen nach Artikel 13 der Verordnung (EU) 2016/679 verfügbar sind.

(3) Für einen anderen Zweck dürfen die Daten nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen erforderlich ist.

(4) Die Videoaufzeichnungen und daraus gefertigte oder sich auf die Videoüberwachung beziehende Unterlagen sind unverzüglich, spätestens jedoch zwei Monate nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.

(5) Öffentliche Stellen haben ihren jeweiligen Datenschutzbeauftragten unbeschadet des Artikels 35 Absatz 2 der Verordnung (EU) 2016/679 rechtzeitig vor dem erstmaligen Einsatz einer Videoüberwachungseinrichtung den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen und ihm Gelegenheit zur Stellungnahme zu geben.

(6) Videoüberwachung öffentlich zugänglicher Räume unter Nutzung von KI-Systemen ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, um

1. Leib oder Leben von Personen zu schützen, oder

2. den Erhaltungszustand und die Funktionsfähigkeit des Eigentums öffentlicher Stellen und zu öffentlichen Zwecken gewidmeter Gegenstände zu überwachen

und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Absätze 2 bis 5 gelten entsprechend.

§ 18a
Videoüberwachung nicht öffentlich zugänglicher Räume

Die Videoüberwachung nicht öffentlich zugänglicher Räume einschließlich der Nutzung von KI-Systemen zur Überwachung des Erhaltungszustands und der Funktionsfähigkeit des Eigentums öffentlicher Stellen und zu öffentlichen Zwecken gewidmeter Gegenstände ist entsprechend § 18 Absatz 6 zulässig. Der Schutz beschäftigter oder sich im Überwachungsbereich aufhaltender Personen ist durch technische und organisatorische Maßnahmen so weit wie möglich zu gewährleisten; § 15 Absätze 5, 7 und 9 gelten entsprechend.

§ 18b
Sonstige technische Überwachung

Der Einsatz sonstiger technischer Mittel einschließlich der Nutzung von KI-Systemen zur Überwachung des Erhaltungszustands und der Funktionsfähigkeit des Eigentums öffentlicher Stellen und zu öffentli-

chen Zwecken gewidmeter Gegenstände ist in öffentlich zugänglichen Räumen entsprechend § 18 Absatz 6 und in nicht öffentlich zugänglichen Räumen entsprechend § 18a zulässig. Tonaufnahmen mit personenbezogenen Daten sind so weit wie möglich zu vermeiden; ist dies nicht oder nur mit unzumutbarem Aufwand möglich, sind sie innerhalb von 180 Sekunden automatisch zu löschen.

§ 19
Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken

(1) Werden personenbezogene Daten zu künstlerischen und literarischen Zwecken verarbeitet, gelten neben Absatz 2 und 3 nur Artikel 5 Absatz 1 Buchstabe f in Verbindung mit Absatz 2, Artikel 24 und 32, sowie Kapitel I, VI, VIII, X und XI der Verordnung (EU) 2016/679. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass nur für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Den betroffenen Personen stehen nur die in Absatz 2 und 3 genannten Rechte zu.

(2) Führt die künstlerische oder literarische Offenlegung oder Verbreitung personenbezogener Daten zu hierauf bezogenen Maßnahmen wie Gegendarstellungen, Verpflichtungserklärungen, Gerichtsentscheidungen oder Widerrufen sind diese Maßnahmen zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst und bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch die künstlerische oder literarische Offenlegung oder Verbreitung personenbezogener Daten in seinem Persönlichkeitsrecht beeinträchtigt, kann er Auskunft über die zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen.

ABSCHNITT 5
Datenverarbeitung im Landtag

§ 19a
Verarbeitung personenbezogener Daten im Landtag

(1) Für die Verarbeitung personenbezogener Daten durch den Landtag, seine Gremien, seine Mitglieder und deren Beschäftigte, die Fraktionen und deren Beschäftigte sowie durch die Landtagsverwaltung gelten dieses Gesetz und die Verordnung (EU) 2016/679 nach Maßgabe dieses Abschnitts.

(2) Die Richtlinien für die Behandlung geheimhaltungsbedürftiger Angelegenheiten im Bereich des Landtags bleiben unberührt.

§ 19b
Zulässigkeit der Datenverarbeitung

(1) Erlaubt ist die Verarbeitung personenbezogener Daten, soweit sie zur Wahrnehmung der Aufgaben nach § 19a Absatz 1 erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten im Sinne von Artikel 9 und Artikel 10 der Verordnung (EU) 2016/679 ist für die Wahrnehmung der Aufgaben nach § 19a Absatz 1 ohne ausdrückliche Einwilligung der betroffenen Personen nur zulässig, soweit dies zur Aufgabenerfüllung erforderlich und verhältnismäßig ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen bestehen.

§ 19c
Verantwortlicher

Verantwortlicher gemäß der Artikel 4 Nummer 7 Verordnung (EU) 2016/679 für Datenverarbeitungen zur Erfüllung der Aufgaben nach § 19a Absatz 1 ist

1. bei der Wahrnehmung der Aufgaben des Landtags der Landtag,

2. für die Tätigkeit der Fraktionen stets die jeweilige Fraktion, auch wenn sie Aufgaben des Landtags wahrnimmt,

3. bei der Mandatsausübung der Mitglieder des Landtags die oder der jeweilige Abgeordnete, soweit sie oder er keine Aufgaben des Landtags wahrnimmt.

§ 19d
Rechte betroffener Personen

(1) Für Datenverarbeitungen im Rahmen der Aufgabenerfüllung nach § 19a Absatz 1 gelten die Rechte der betroffenen Personen gemäß den Artikeln 13 bis 19 und 21 der Verordnung (EU) 2016/679 im Hinblick auf Artikel 23 Absatz 1 Buchstabe e und h der Verordnung (EU) 2016/679 nach Maßgabe der Absätze 2 bis 8.

(2) Die nach Artikel 13 und 14 der Verordnung (EU) 2016/679 vorgeschriebenen Informationen sind in Form einer Erklärung auf elektronischem Weg zur Verfügung zu stellen (Datenschutzerklärung). Die Informationspflichten gemäß Artikel 13 Absatz 1 Buchstabe e sowie Artikel 14 Absatz 1 Buchstabe d und e und Absatz 2 Buchstabe f der Verordnung (EU) 2016/679 finden keine Anwendung.

(3) Das Auskunftsrecht gemäß Artikel 15 der Verordnung (EU) 2016/679 findet keine Anwendung

1. bei nicht öffentlichen Informationen, Verschlusssachen oder Gegenständen und Inhalten nicht öffentlicher, vertraulicher oder geheimer Beratungen, Verhandlungen, Sitzungen und Beschlüsse,

2. hinsichtlich der Rechte gemäß Artikel 15 Absatz 1 Buchstabe c und g sowie Absatz 3 der Verordnung (EU) 2016/679.

(4) Das Recht auf Löschung gemäß Artikel 17 der Verordnung (EU) 2016/679 umfasst nur das Recht auf Entfernung veröffentlichter personenbezogener Daten von der Website des Parlaments.

(5) Das Recht auf Berichtigung gemäß Artikel 16 der Verordnung (EU) 2016/679 ist auf Schreibfehler und andere offensichtliche Unrichtigkeiten beschränkt. Zu darüber hinausgehenden unrichtigen oder unvollständigen personenbezogenen Daten kann die betroffene Person eine ergänzende Erklärung abgeben, die ohne Kosten für die betroffene Person gemeinsam mit den als unrichtig oder unvollständig gerügten personenbezogenen Daten zu veröffentlichen ist.

(6) Das Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679 und die Mitteilungspflicht gemäß Artikel 19 der Verordnung (EU) 2016/679 kommen nicht zur Anwendung.

(7) Das Widerspruchsrecht gemäß Artikel 21 der Verordnung (EU) 2016/679 ist auf die Veröffentlichung beschränkt. Anstelle eines Nachweises überwiegender schutzwürdiger Gründe für die Verarbei-

tung durch den Verantwortlichen gemäß Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 genügt die Glaubhaftmachung solcher Gründe.

(8) Sämtliche in den Absätzen 4 bis 7 genannten Beschränkungen gelangen nur insoweit zur Anwendung, als die Beschränkung jeweils zur Erfüllung der Aufgaben nach § 19a Absatz 1 geeignet und erforderlich ist.

§ 19e
Datenschutzaufsicht

(1) Der Landtag kann sich für die Aufsicht über die Verarbeitung von personenbezogenen Daten im Landtag eine Datenschutzaufsichtsordnung geben, mit der ein eigenes Aufsichtsgremium gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichtet wird und die insbesondere Bestimmungen enthält über

1. die Einrichtung, die Zusammensetzung und die Anzahl der Mitglieder,

2. Beginn und Ende der Amtszeit der Mitglieder,

3. die Beschlussfassung.

(2) Hinsichtlich der Aufgaben des Gremiums gilt Artikel 57 der Verordnung (EU) 2016/679.

(3) Für die Unabhängigkeit des Aufsichtsgremiums gilt Artikel 52 Absatz 1 bis 3 der Verordnung (EU) 2016/679.

(4) Zur Gewährleistung der Sachkunde nach Artikel 53 Absatz 2 der Verordnung (EU) 2016/679 muss mindestens ein Mitglied des Aufsichtsgremiums die Befähigung zum Richteramt besitzen.

(5) Für Untersuchungs- und Abhilfebefugnisse sowie für Genehmigungs- und Beratungsbefugnisse gilt Artikel 58 der Verordnung (EU) 2016/679 mit der Beschränkung in § 28.

ABSCHNITT 6
Unabhängige Aufsichtsbehörden

§ 20
Errichtung

(1) Die oder der Landesbeauftragte für den Datenschutz ist eine unabhängige, nur dem Gesetz unterworfene oberste Landesbehörde. Der Dienstsitz ist Stuttgart.

(2) Die oder der Landesbeauftragte für den Datenschutz ist Dienstvorgesetzte oder Dienstvorgesetzter der Beamtinnen und Beamten der Behörde. Die Beschäftigten der oder des Landesbeauftragten für den Datenschutz sind ausschließlich an ihre oder seine Weisungen gebunden.

(3) Die oder der Landesbeauftragte für den Datenschutz kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Landes übertragen, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist. Die Aufgabenübertragung nach Satz 1 kann nur im Einvernehmen mit der anderen Stelle erfolgen.

§ 21
Unabhängigkeit

(1) Die oder der Landesbeauftragte für den Datenschutz handelt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig.

(2) Die oder der Landesbeauftragte für den Datenschutz unterliegt der Rechnungsprüfung durch den Rechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(3) Die Abgeordneten des Landtags sind berechtigt, Anfragen an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz zu richten, zu deren Beantwortung diese oder dieser nur verpflichtet ist, soweit hierdurch nicht ihre oder seine Unabhängigkeit beeinträchtigt wird.

§ 22
Ernennung und Amtszeit

(1) Der Landtag wählt ohne Aussprache auf Vorschlag der Landesregierung mit der Mehrheit seiner Mitglieder die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz. Diese oder dieser soll neben der erforderlichen Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst haben oder für eine andere Laufbahn des höheren Dienstes befähigt sein.

(2) Die oder der Gewählte wird von der Landtagspräsidentin oder dem Landtagspräsidenten ernannt. Sie oder er wird vor dem Landtag auf das Amt verpflichtet.

(3) Die Amtszeit der oder des Landesbeauftragten für den Datenschutz beträgt sechs Jahre. Die zweimalige Wiederwahl ist zulässig.

§ 23
Amtsverhältnis

(1) Die oder der Landesbeauftragte für den Datenschutz steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis zum Land.

(2) Die Landtagspräsidentin oder der Landtagspräsident kann die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz ihres oder seines Amtes entheben, wenn diese oder dieser eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Die Amtsenthebung bedarf der Zustimmung von zwei Dritteln der Mitglieder des Landtags. Die Amtsenthebung wird mit der Zustellung der Urkunde durch die Landtagspräsidentin oder den Landtagspräsidenten wirksam.

(3) Die Leitende Beamtin oder der Leitende Beamte der Dienststelle der oder des Landesbeauftragten für den Datenschutz nimmt die Rechte und Pflichten der oder des Landesbeauftragten für den Datenschutz wahr, wenn die oder der Landesbeauftragte für den Datenschutz an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis geendet hat. § 21 Absatz 1 gilt in den genannten Fällen entsprechend.

(4) Die oder der Landesbeauftragte für den Datenschutz erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, Bezüge in Höhe des Grundgehalts der Besoldungsgruppe B 6. Daneben werden der Familienzuschlag sowie sonstige Besoldungsbestandteile, Trennungsgeld, Reisekostenvergütung, Umzugskostenvergütung und Beihilfen in Krankheits-, Geburts- oder Todesfällen in sinngemäßer Anwendung der für Beamtinnen und Beamte geltenden Vorschriften gewährt.

(5) Die oder der Landesbeauftragte für den Datenschutz erhält nach dem Ausscheiden aus dem Amt Versorgungsbezüge in sinngemäßer Anwendung der für Beamtinnen und Beamte geltenden Vorschriften.

§ 24
Rechte und Pflichten

(1) Die oder der Landesbeauftragte für den Datenschutz hat von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen abzusehen und während ihrer oder seiner Amtszeit keine andere mit ihrem oder seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit auszuüben. Insbesondere darf die oder der Landesbeauftragte für den Datenschutz neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung, dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(2) Die oder der Landesbeauftragte für den Datenschutz hat der Landtagspräsidentin oder dem Landtagspräsidenten Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. Die Landtagspräsidentin oder der Landtagspräsident entscheidet über die Verwendung der Geschenke; sie oder er kann Verfahrensvorschriften erlassen.

(3) Die oder der Landesbeauftragte für den Datenschutz ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Landesbeauftragte für den Datenschutz entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er oder ihre oder seine Beschäftigten über solche Angelegenheiten vor Gericht oder außergerichtlich aussagen oder Erklärungen abgeben. Wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Landesbeauftragten für den Datenschutz erforderlich. Satz 1, 2 und 4 gelten entsprechend für die Beschäftigten der oder des Landesbeauftragten für den Datenschutz nach Beendigung ihrer Tätigkeit bei ihrer oder seiner Dienststelle.

(4) Die oder der Landesbeauftragte für den Datenschutz hat für die Dauer von zwei Jahren nach der Beendigung ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres oder seines früheren Amtes nicht zu vereinbarenden Handlungen und entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(5) Die oder der Landesbeauftragte für den Datenschutz darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde dem Wohle des Bundes oder eines Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder ihre Beziehungen zu anderen Staaten, oder Grundrechte verletzen. Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Landesregierung zuzurechnen sind oder sein könnten, darf die oder der Landesbeauftragte für den Datenschutz nur im Benehmen mit der Landesregierung aussagen.

§ 25
Aufgaben und Befugnisse

(1) Die oder der Landesbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde im Sinne des Artikels 51 Absatz 1 der Verordnung (EU) 2016/679 im Geltungsbereich dieses Gesetzes, es sei denn,

besondere Vorschriften regeln eine andere Zuständigkeit. Sie oder er ist zugleich Aufsichtsbehörde für den Datenschutz für nichtöffentliche Stellen nach § 40 des Bundesdatenschutzgesetzes.

(2) Die oder der Landesbeauftragte für den Datenschutz nimmt auch im Anwendungsbereich des § 2 Absatz 4 die Aufgaben gemäß Artikel 57 der Verordnung (EU) 2016/679 wahr und übt die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 aus. Bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie bei den in § 2 Absatz 2 genannten Stellen ist das vertretungsberechtigte Organ der Verantwortliche.

(3) Jede oder jeder kann sich an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch eine öffentliche Stelle in ihren oder seinen Rechten verletzt worden zu sein. Wer von seinem Recht nach Satz 1 Gebrauch gemacht hat, darf aus diesem Grund nicht benachteiligt oder gemaßregelt werden.

(4) Stellt die oder der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, teilt sie oder er dies bei den öffentlichen Stellen des Landes der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstaben b bis g und j der Verordnung (EU) 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie den in § 2 Absatz 2 genannten Stellen tritt an die Stelle der Rechts- und Fachaufsichtsbehörde das vertretungsberechtigte Organ; zugleich unterrichtet die oder der Landesbeauftragte für den Datenschutz die zuständige Aufsichtsbehörde. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Landesbeauftragten für den Datenschutz getroffen worden oder beabsichtigt sind.

(5) § 29 Absatz 3 des Bundesdatenschutzgesetzes bleibt unberührt und gilt entsprechend für die Notarinnen und Notare des Landes. Im Übrigen erstreckt sich die Kontrolle der oder des Landesbeauftragten für den Datenschutz auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Erlangt die oder der Landesbeauftragte für den Datenschutz im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz.

§ 26
Pflicht zur Unterstützung

(1) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz und ihre oder seine Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihnen ist im Rahmen ihrer gesetzlichen Befugnisse insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen und

2. jederzeit Zutritt zu den Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte zu gewähren.

(2) Die Ministerien beteiligen die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz rechtzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen.

§ 27
Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz

Für alle Tätigkeiten des Südwestrundfunks und seiner Beteiligungsunternehmen nach § 42 Absatz 3 Satz 1 des Medienstaatsvertrags vom 14. bis 28. April 2020 (Gesetz vom 30. Juni 2020; GBl. S. 429, 430), der zuletzt durch Artikel 1 des Staatsvertrags vom 27. Februar bis 7. März 2024 (Gesetz vom 25. Juli 2024; GBl. 2024, Nr. 67, S. 3) geändert worden ist, in der jeweils geltenden Fassung ist anstelle der oder des Landesbeauftragten für den Datenschutz die oder der gemeinsame Rundfunkdatenschutzbeauftragte der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des ZDF und des Deutschlandradios nach den Vorschriften des Medienstaatsvertrags zuständige Aufsichtsbehörde nach Artikel 51 Absatz 1 der Verordnung (EU) 2016/679.

§ 27a
Datenschutzaufsicht für digitale Dienste

Die oder der Landesbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde für digitale Dienste im Sinne des § 1 Nummer 8 zweiter Halbsatz des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; ber. 2022 I S. 1045), das zuletzt durch Artikel 44 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234, S. 19) geändert worden ist, in der jeweils geltenden Fassung. Im Hinblick auf die Befugnisse der oder des Landesbeauftragten für den Datenschutz im Rahmen ihrer oder seiner Aufsichtstätigkeit über die Einhaltung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung.

ABSCHNITT 7
Sanktionen

§ 28
Ordnungswidrigkeiten

(Ergänzung zu Artikel 83 Absatz 7 der Verordnung [EU] 2016/679)

Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 dürfen keine Geldbußen verhängt werden, es sei denn, die öffentlichen Stellen nehmen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teil.

§ 29
Strafvorschrift

(Ergänzung zu Artikel 84 der Verordnung [EU] 2016/679)

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. unbefugt von diesem Gesetz oder der Verordnung (EU) 2016/679 geschützte personenbezogene Daten, die nicht allgemein zugänglich sind,

a) speichert, nutzt, verändert, übermittelt oder löscht,

b) zum Abruf mittels automatisierten Verfahrens bereithält oder

c) abruft oder sich oder einem anderen aus Dateien verschafft oder

2. durch unrichtige Angaben personenbezogene Daten, die durch dieses Gesetz oder die Verordnung (EU) 2016/679 geschützt werden und nicht allgemein zugänglich sind, erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, die öffentliche Stelle, der Auftragsverarbeiter, die oder der Landesbeauftragte für den Datenschutz, die oder der Rundfunkbeauftragte für den Datenschutz und die Aufsichtsbehörden.

ABSCHNITT 8
Übergangsbestimmungen

§ 30
Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes

(1) Für die Verarbeitung personenbezogener Daten durch die Polizeibehörden und den Polizeivollzugsdienst gilt, soweit sie nicht die Verordnung (EU) 2016/679 anzuwenden haben, das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis die Regelungen des Landes Baden-Württemberg zur Umsetzung der Richtlinie (EU) 2016/680 für den Bereich der Polizei in Kraft treten.

(2) Für die Verarbeitung personenbezogener Daten zu den in Artikel 2 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679 genannten Zwecken durch das Justizministerium und die Justizvollzugsbehörden sowie durch die ordentlichen Gerichte und die Staatsanwaltschaften des Landes, soweit sie zu diesen Zwecken in Verwaltungsangelegenheiten tätig werden, sowie für die Behörden des Landes, die personenbezogene Daten zur Verfolgung und Ahndung von Ordnungswidrigkeiten verarbeiten, gilt das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis das Gesetz des Landes Baden-Württemberg zur Anpassung des besonderen Datenschutzrechts an die Verordnung und zur Umsetzung der Richtlinie (EU) 2016/680 für den Geschäftsbereich des Justizministeriums sowie für die zur Ahndung von Ordnungswidrigkeiten zuständigen Behörden des Landes in Kraft tritt.

(3) Für die Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes und beim Vollzug des Landessicherheitsüberprüfungsgesetzes gilt das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis das Gesetz des Landes Baden-Württemberg zur Änderung des Landesverfassungsschutzgesetzes und anderer Gesetze in Kraft tritt.

§ 31
Überleitungsvorschriften

(1) Der zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Landesbeauftragte für den Datenschutz gilt ab dem Tag des Inkrafttretens dieses Gesetzes als in ein Amt nach § 23 Absatz 1

berufen. Mit der Berufung in dieses Amt endet sein Beamtenverhältnis auf Zeit. Seine Amtszeit endet am 31. Dezember 2022.

(2) Mit Inkrafttreten dieses Gesetzes sind die Angehörigen des öffentlichen Dienstes bei dem Landesbeauftragten für den Datenschutz vom Landtag zu dem Landesbeauftragten für den Datenschutz versetzt.

(3) Der Personalrat bei der Dienststelle des Landesbeauftragten für den Datenschutz besteht ab Inkrafttreten dieses Gesetzes bis zu seiner Neuwahl als Personalrat bei dem Landesbeauftragten für den Datenschutz fort.