**Gesetz zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze**

Vorblatt

A. Zielsetzung

Mit dem Gesetz zur Änderung des Landesdatenschutzgesetzes werden im Evaluierungsbericht zum Landesdatenschutzgesetz vom 8. Oktober 2024 (Landtagsdrucksache 17/7596) festgestellte Änderungsbedarfe umgesetzt. Ziel ist, den öffentlichen Stellen den für die moderne Verwaltung erforderlichen Spielraum zur Verarbeitung personenbezogener Daten in dem Rahmen zur Verfügung zu stellen, den die schutzwürdigen Interessen der betroffenen Personen zulassen.

Des Weiteren wird zur Erprobung und Einführung des automatisierten Erlasses von Verwaltungsakten eine Vorschrift in das E-Government-Gesetz Baden-Württemberg eingefügt. Im Gesetz zur Ausführung des Personenstandsgesetzes wird für die Fachaufsicht über die Standesämter der automatisierte Abruf der in den elektronischen Sammelakten gespeicherten personenbezogenen Daten ermöglicht. Im Landesinformationsfreiheitsgesetz werden aus Anlass aktueller Rechtsprechung des Verwaltungsgerichtshofs Baden-Württemberg die Bereichsausnahmen entsprechend verfassungsrechtlicher Anforderungen geändert.

B. Wesentlicher Inhalt

Entsprechend dem Ziel, die Bedarfe der Verwaltung besser zu berücksichtigen, finden sich in der Novellierung des Landesdatenschutzgesetzes Vorschriften für den Einsatz künstlicher Intelligenz (KI), zur Verarbeitung personenbezogener Daten für die Öffentlichkeitsarbeit sowie erweiterte Befugnisse für die Forschung öffentlicher Stellen. Die Auftragsverarbeitung für öffentliche Stellen durch staatliche Behörden wird ebenso wie die Einrichtung automatisierter Abrufverfahren auf eine gesetzliche Grundlage gestellt. Die Videoüberwachung wird für sicherheitsrelevante Einrichtungen und Gegenstände, Dienstgebäude, Kulturgüter und Verkehrsmittel abstrakt-generell als verhältnismäßiges Mittel zugelassen. Daneben erfolgen Klarstellungen und redaktionelle Anpassungen. Die Verarbeitungsbefugnisse werden um spezifische Maßnahmen zugunsten der Betroffenen ergänzt.

In Fällen, in denen weder ein Ermessen noch ein Beurteilungsspielraum besteht, können in Zukunft automatisiert Verwaltungsakte einschließlich der Nutzung von KI erlassen werden. Das E-Government-Gesetz Baden-Württemberg regelt die verfahrensrechtlichen Voraussetzungen hierfür.

Die Fachaufsicht über die Standesämter benötigt zur Aufgabenerfüllung den automatisierten Zugriff auf die elektronischen Sammelakten der Standesämter; hierzu wird eine entsprechende Vorschrift im Gesetz zur Ausführung des Personenstandsgesetzes eingefügt.

In die Vorschrift zu den Bereichsausnahmen des Landesinformationsfreiheitsgesetzes werden Regelungen zum Schutz der Kunst- und Wissenschaftsfreiheit sowie des religionsgemeinschaftlichen Selbstbestimmungsrechts aufgenommen.

Digitale Dienste betreffende Vorschriften in der Verordnung der Landeregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten und im Landesmediengesetz werden an bundesgesetzliche Vorschriften, das Landesmediengesetz darüber hinaus an den Fünften Medienstaatsvertrag angepasst.

C. Alternativen

Keine. Die öffentlichen Stellen benötigen für die Verarbeitung personenbezogener Daten hinreichend bestimmte Rechtsgrundlagen. Digitale Verwaltung muss außerdem über geeignete Instrumente zur Ausübung ihrer Befugnisse verfügen. Die Änderungen der Bereichsausnahmen im Landesinformationsfreiheitsgesetz sind verfassungsrechtlich geboten.

D. Kosten für die öffentlichen Haushalte

Kosten für die öffentlichen Haushalte entstehen durch die Änderung des Landesdatenschutzgesetzes, des E-Government-Gesetzes Baden-Württemberg und des Landesinformationsfreiheitsgesetzes nicht. Den Kommunen entstehen durch die Änderung des Gesetzes zur Ausführung des Personenstandsgesetzes geringfügige Kosten, indem sie den automatisierten Abruf für die elektronischen Sammelakten einrichten müssen.

E. Bürokratievermeidung, Prüfung Vollzugstauglichkeit

Transparente Regelungen erleichtern den öffentlichen Stellen die Einhaltung des Datenschutzes. Automatisierte Entscheidungen und Abrufverfahren sind geeignet, die Verwaltungsarbeit zu erleichtern. Die neu gefassten Bereichsausnahmen im Landesinformationsfreiheitsgesetz sollen der Rechtssicherheit dienen und damit die Verwaltung entlasten.

F. Nachhaltigkeits-Check

Die Anpassung des Landesdatenschutzgesetzes an die Anforderungen der Praxis unterstützt die Verwaltung nachhaltig und trägt zur Ressourcenschonung bei. Insbesondere die Regulierung des KI-Einsatzes ist in der Lage, die Grundlage für die Einführung von datenschutzgerechter KI in der Verwaltung zugunsten einer effizienten Aufgabenerledigung zu sein, von der die Bürgerinnen und Bürger ebenso profitieren.

In gleicher Weise fördern die Einführung einer Experimentierklausel für den automatisierten Erlass von Verwaltungsakten, automatisierte Abrufverfahren sowie die Ausweitung des elektronischen Abrufverfahrens bei den Standesämtern auf die elektronischen Sammelakten die Digitalisierung und Zukunftsfähigkeit der öffentlichen Verwaltung.

G. Digitaltauglichkeits-Check

Die neuen Regelungen im Landesdatenschutzgesetz betreffen überwiegend die Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten. Darüber hinaus unterstützen sie ebenso wie die weiteren Regelungen die Digitalisierung der Verwaltung.

H. Sonstige Kosten für Private

Kosten für Private entstehen nicht.

**Gesetz zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze**

Vom

Artikel 1

Änderung des Landesdatenschutzgesetzes

Das Landesdatenschutzgesetz vom 12. Juni 2018 (GBl. S. 173), das zuletzt durch Artikel 1 des Gesetzes vom 29. Juli 2025 (GBl. 2025 Nr. 80) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) In Absatz 1 Satz 2 werden nach dem Wort „dieses“ die Wörter „oder ein anderes“ eingefügt.

   b) In Absatz 4 Satz 3 werden die Wörter „und der staatlichen Rechnungsprüfungsämter“ gestrichen und das Wort „finden“ durch das Wort „findet“ ersetzt.

   c) Absatz 5 wird wie folgt gefasst:

      „(5) Dieses Gesetz gilt für den Landtag und die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Abweichend hiervon gelten die Vorschriften der §§ 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 Nummer 3 bleibt unberührt.“

2. Nach § 2 wird folgender § 2a eingefügt:

§ 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 (EU) 2024/1689 in der jeweils geltenden Fassung 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. § 3 Absatz 1 Satz 3 wird wie folgt geändert:

   a) Die Wörter „Zu den Maßnahmen können insbesondere gehören“ werden durch die Wörter „Technische und organisatorische Maßnahmen müssen sicherstellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt; zu den erforderlichen Maßnahmen können insbesondere gehören“ ersetzt.

   b) Nummer 1 wird aufgehoben und die bisherigen Nummern 2 bis 6 werden die Nummern 1 bis 5.

   c) Der Nummer 5 wird als Nummer 6 angefügt:

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

4. Nach § 3 wird folgender § 3a eingefügt:

„§ 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.“

5. § 4 wird wie folgt geändert:

a) Der bisherige Wortlaut wird Absatz 1.

b) Es wird folgender Absatz 2 angefügt:

„(2) Öffentliche Stellen dürfen zum Zweck der Datenminimierung aus den rechtmäßig gespeicherten Daten synthetische Daten herstellen sowie rechtmäßig gespeicherte Daten auf sonstige Weise anonymisieren.“

6. § 5 Absatz 1 wird wie folgt geändert:

a) In Nummer 1 werden nach dem Wort „ist“ die Wörter „das Gemeinwohl ist gleichzusetzen mit den gesetzlich anerkannten allgemeinen öffentlichen Interessen“ eingefügt.

b) Nummer 3 wird wie folgt gefasst:

„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,“.

c) In Nummer 4 wird das Wort „bestehen,“ durch die Wörter „bestehen oder“ ersetzt.

d) Es wird folgende Nummer 5 eingefügt:

„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,“.

7. § 6 wird wie folgt gefasst:

„§ 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 oder Verteidigung von Rechtsansprüchen der übermittelnden Stelle erforderlich ist.

(3) Für die Übermittlung in andere 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.

8. Nach § 7 wird folgender § 7a eingefügt:

„§ 7a

Auftragsverarbeitung

(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 werden.

Bestehende einzelvertragliche Regelungen zur Auftragsverarbeitung werden entsprechend der Verordnung 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.“

9. § 8 wird wie folgt geändert:

a) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1 Nummern 1, 2 oder 5, 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.“

b) Die bisherigen Absätze 2 und 3 werden die Absätze 3 und 4.

10. Nach § 9 wird folgender § 9a eingefügt:

„§ 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.“

11. § 10 wird folgender Absatz 4 angefügt:

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

12. § 12 wird folgender § 11a vorangestellt:

„§ 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.“

13. Nach § 12 wird folgender § 12a eingefügt:

„§ 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.“

14. § 13 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) Nach dem Wort „verarbeiten“ werden die Wörter „und vorhandene Daten der genannten Art weiterverarbeiten“ eingefügt.

bbb) Die Wörter „wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können“ werden durch die Wörter „wenn die Verarbeitung zu diesen Zwecken erforderlich ist“ ersetzt.

bb) Satz 2 wird aufgehoben.

b) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

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

c) Der bisherige Absatz 2 wird Absatz 3.

d) Absatz 3 wird folgender Satz angefügt:

„Zur Wahrung der Interessen der betroffenen Person sind weitere angemessene und spezifische Maßnahmen entsprechend § 3 Absatz 1 zu treffen.“

e) Der bisherige Absatz 3 wird Absatz 4.

f) Nach Absatz 4 wird folgender Absatz 5 eingefügt:

„(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 Auskunft über den Umgang mit den übermittelten personenbezogenen Daten zu erteilen.

g) Der bisherige Absatz 4 wird Absatz 6.

15. § 15 wird wie folgt geändert:

a) Absatz 2 wird folgender Satz 2 angefügt:

„Besondere Kategorien personenbezogener Daten dürfen 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.“

b) Absatz 6 wird wie folgt gefasst:

„(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 zugestimmt 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.“

c) Es wird folgender Absatz 9 angefügt:

„(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. § 16 Absatz 1 wird folgender Satz angefügt:

„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.“

17. § 17 wird wie folgt geändert:

Absatz 1 wird aufgehoben. Dem verbleibenden Wortlaut wird folgender Satz angefügt:

„Die öffentliche Stelle trifft angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person; hierfür sind mindestens die Maßnahmen nach § 3 Nummern 1 bis 3 zu treffen.“

18. Nach § 17 werden folgende §§ 17a und 17b eingefügt:

„§ 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 zustimmt und kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung steht.

§ 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.

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

19. § 18 wird wie folgt geändert:

a) In der Überschrift wird das Wort „Videoüberwachung“ durch das Wort „Videoschutz“ ersetzt.

b) Absatz 1 werden folgende Sätze angefügt:

„Der Schutz von Leben, Gesundheit und Freiheit der in Nummer 1 genannten Personen ist ein besonders wichtiges öffentliches Interesse. Sofern die Videoüberwachung zum Schutz von sicherheitsrelevanten Einrichtungen, Dienstgebäuden, Dienstfahrzeugen, Kulturgütern oder öffentlichen Verkehrsmitteln und den dort jeweils befindlichen Personen und Sachen erforderlich ist, gilt Videoüberwachung als angemessen und verhältnismäßig.“

c) Absatz 2 wird wie folgt gefasst:

„(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 auf die Möglichkeit hinzuweisen, die weiteren Informationen nach Artikel 13 der Verordnung (EU) 2016/679 vom Verantwortlichen zu erhalten.“

d) In Absatz 3 werden die Wörter „Sicherheit oder“ durch das Wort „Sicherheit“ ersetzt und nach dem Wort „Straftaten“ werden die Wörter „oder zur Geltendmachung von Rechtsansprüchen“ eingefügt.

e) Absatz 4 wird aufgehoben.

f) Die bisherigen Absätze 5 und 6 werden Absätze 4 und 5.

g) Im neuen Absatz 4 werden die Wörter „vier Wochen“ ersetzt durch die Wörter „zwei Monate“.

h) Es wird folgender Absatz 6 angefügt:

„(6) Videoüberwachung einschließlich der Nutzung von KI-Systemen ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, um 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. Absatz 2 bis 5 gelten entsprechend.“

20. Nach § 18 werden folgende §§ 18a und 18b eingefügt:

„§ 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 Absatz 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 öffentlichen 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.“

21. Nach § 27 wird folgender § 27a eingefügt:

„§ 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 der Bestimmungen nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung.“

22. Die Inhaltsübersicht ist entsprechend anzupassen.

Artikel 2

Änderung des E-Government-Gesetzes Baden-Württemberg

Das E-Government-Gesetz Baden-Württemberg vom 17. Dezember 2015 (GBl. S. 1191), das zuletzt durch Artikel 3 des Gesetzes vom 4. Februar 2021 (GBl. S. 182, 190) geändert worden ist, wird wie folgt geändert:

1. Nach § 17 wird folgender § 17 a eingefügt:

„§ 17a

Automatisierter Erlass von Verwaltungsakten

(1) Dieser Paragraf dient der Erprobung des vollständig automatisierten Erlasses von Verwaltungsakten einschließlich der Nutzung künstlicher Intelligenz (KI) durch KI-Systeme in verschiedenen Anwendungsbereichen und

der daran anknüpfenden, durch die Landesregierung erfolgenden dauerhaften Zulassung des automatisierten Erlasses von Verwaltungsakten in einzelnen Anwendungsbereichen. KI-Systeme nach Satz 1 sind solche 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).

(2) Die für die Durchführung eines Verwaltungsverfahrens zuständige Behörde kann im Rahmen des § 35a des Landesverwaltungsverfahrensgesetzes Verwaltungsakte vollständig automatisiert erlassen, soweit nicht überwiegende Interessen derjenigen entgegenstehen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden. Deren Interessen überwiegen in der Regel nicht, soweit

1. sie ausdrücklich und freiwillig ihre Einwilligung zum vollständig automatisierten Erlass des Verwaltungsakts geben,

2. gegen die Entscheidungen Widerspruchsverfahren eröffnet sind und die Widerspruchsbescheide nicht ihrerseits vollständig automatisiert erlassen werden,

3. die Behörde den Anträgen entspricht oder Erklärungen folgt und die Verwaltungsakte nicht in die Rechte anderer eingreifen oder

4. denjenigen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden, die Auffassung der Behörde über die Sach- und Rechtslage bekannt oder auch ohne Begründung für sie ohne weiteres erkennbar ist.

(3) Mindestens einen Monat vor Aufnahme des Verfahrens zum vollständig automatisierten Erlass von Verwaltungsakten ist der obersten Fachaufsichtsbehörde und dem Innenministerium die neue Verfahrensweise anzuzeigen.

(4) Die Erprobung ist für eine angemessene Zeit zu befristen. Der Erprobungszeitraum beträgt mindestens ein Jahr und darf höchstens zwei Jahre betragen und wird durch die für die Durchführung des Verwaltungsverfahrens zuständige Behörde festgelegt. Innerhalb eines Jahres nach Ende des nach Satz 2 festgelegten Erprobungszeitraums ist ein Evaluierungsbericht der obersten Fachaufsichtsbehörde und dem Innenministerium vorzulegen, wenn eine Fortführung der Erprobung oder der Dauerbetrieb beabsichtigt ist. Innerhalb dieses Jahres kann die Erprobung fortgesetzt werden, sowie für zwei weitere Jahre nach dem Ablauf dieses Jahres, wenn ein Evaluierungsbericht vorgelegt wird. Wird innerhalb der Jahresfrist nach Satz 3 kein Evaluierungsbericht vorgelegt, darf der vollständig automatisierte Erlass von Verwaltungsakten danach nur mit Einverständnis der obersten Fachaufsichtsbehörde im Einvernehmen mit dem Innenministerium, allerdings nicht länger als ein Jahr, fortgesetzt werden.

(5) Nach Auswertung des Evaluierungsberichts oder der Evaluierungsberichte kann die Landesregierung durch Rechtsverordnung den vollständig automatisierten Erlass von Verwaltungsakten im Rahmen des § 35 a des Landesverwaltungsverfahrensgesetzes zulassen, wenn davon auszugehen ist, dass die überwiegenden Interessen derjenigen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden, nicht entgegenstehen. Absatz 2 Satz 2 gilt entsprechend. In der Rechtsverordnung nach Satz 1 können insbesondere Vorgaben für ein Risikomanagementsystem aufgenommen werden.“

2. Die Inhaltsübersicht ist entsprechend anzupassen.

## Artikel 3

## Änderung des Gesetzes zur Ausführung des Personenstandsgesetzes

In § 4a des Gesetzes zur Ausführung des Personenstandsgesetzes vom 3. Dezember 2008 (GBl. S. 434), das zuletzt durch Artikel 12 des Gesetzes vom 15. Dezember 2015 (GBl. S. 1147, 1154) geändert worden ist, werden nach dem Wort „Personenstandsregister“ die Wörter „sowie der in ihren elektronischen Sammelakten“ eingefügt.

## Artikel 4

Änderung des Landesinformationsfreiheitsgesetzes

§ 2 Absatz 3 des Landesinformationsfreiheitsgesetzes vom 17. Dezember 2015 (GBl. S. 1201), das zuletzt durch Artikel 4 des Gesetzes vom 17. Dezember 2024 (GBl. 2024 Nr. 114, S. 4) geändert worden ist, wird wie folgt gefasst:

„Keine Informationspflicht nach diesem Gesetz besteht für

1. das Landesamt für Verfassungsschutz und die sonstigen öffentlichen Stellen des Landes, soweit sie nach Feststellung der Landesregierung gemäß § 35 des Landessicherheitsüberprüfungsgesetzes Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wahrnehmen,

2. Schulen nach § 2 des Schulgesetzes für Baden-Württemberg sowie Ausbildungs- und Prüfungsbehörden, soweit Leistungsbeurteilungen und Prüfungen betroffen sind,

3. die Landesbank Baden-Württemberg, die Landeskreditbank Baden-Württemberg - Förderbank, die Sparkassen sowie ihre Verbände und Verbundunternehmen, die Selbstverwaltungsorganisationen der Wirtschaft, der Freien Berufe und der Krankenversicherung,

4. die Landesfinanzbehörden im Sinne des § 2 des Finanzverwaltungsgesetzes, soweit sie in Verfahren in Steuersachen tätig werden,

5. Informationen, die die Freiheit der Kunst, Wissenschaft, Forschung oder Lehre betreffen, sowie

6. Angelegenheiten der Kirchen, der Religions- und Weltanschauungsgemeinschaften sowie ihrer Untergliederungen und Einrichtungen, soweit diese dem religiösen Selbstbestimmungsrecht unterfallen.“

Artikel 5

Änderung des Landesmediengesetzes

Das Landesmediengesetz vom 19. Juli 1999 (GBl. S. 273, ber. S. 387), das zuletzt durch Artikel 2 des Gesetzes vom 20. November 2023 (GBl. S. 417) geändert worden ist, wird wie folgt geändert:

1. § 12 Absatz 2 wird wie folgt geändert:

   a) In Satz 1 werden nach dem Wort „Vollprogramm“ die Wörter „oder Spartenprogramm“ ersetzt durch die Wörter „, Spartenprogramm, Fensterprogramm oder Regionalfensterprogramm“.

   b) In Satz 2 werden nach den Wörtern „Sie wird“ die Wörter „mit Ausnahme der Zulassung nach § 23 Absatz 2 Satz 2“ eingefügt.

2. § 23 Absatz 3 wird wie folgt gefasst:

   „In den beiden, jeweils unterschiedlichen Unternehmen nach § 62 des Medienstaatsvertragsvertrages zuzurechnenden, bundesweit verbreiteten, nach Zuschaueranteilen reichweitenstärksten Fernsehvollprogrammen sind im zeitlichen und regional differenzierten Umfang der Programmaktivitäten zum 1. Juli 2002 Fensterprogramme zur aktuellen und authentischen Darstellung der Ereignisse des politischen, wirtschaftlichen, sozialen und kulturellen Lebens in Baden-Württemberg aufzunehmen. Dem Fensterprogrammveranstalter wird für die Dauer von zehn Jahren eine gesonderte Zulassung erteilt. Fensterprogrammveranstalter und Hauptprogrammveranstalter sollen zueinander nicht im Verhältnis eines verbundenen Unternehmens nach § 62 des Medienstaatsvertrages stehen. Zum 31. Dezember 2009 bestehende Zulassungen bleiben unberührt. Mit der Organisation der Fensterprogramme ist zugleich deren Finanzierung durch den Hauptprogrammveranstalter sicherzustellen.“

3. In § 30 Absatz 2 Satz 2 wird das Wort „Telemediengesetzes“ durch die Wörter „Digitale-Dienste-Gesetzes, sofern nicht aus § 12 des Digitale-Dienste-Gesetzes eine andere Zuständigkeit folgt,“ ersetzt.

4. In § 51 Absatz 4 werden die Wörter „§ 11 Absatz 2 Nummer 1 bis 3 des Telemediengesetzes“ ersetzt durch die Wörter „§ 33 Absatz 1 und Absatz 2 Nummer 1 und 2 des Digitale-Dienste-Gesetzes“.

## Artikel 6

## Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten

Die Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten in der Fassung vom 2. Februar 1990 (GBl. S. 73, ber. S. 268), die zuletzt durch Artikel 2 der Verordnung vom 30. Oktober 2024 (GBl. 2024 Nr. 9, S. 2) geändert worden ist, wird wie folgt geändert:

1. In § 3a werden die Wörter „des Telekommunikation-Telemedien-Datenschutz-Gesetzes“ durch die Wörter „des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ ersetzt.

2. § 4 Absatz 2 Satz 1 Nummer 4 wird wie folgt gefasst:

   „§ 28 Absatz 1 Nummer 12 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes,“.

## Artikel 7

## Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Stuttgart, den

Die Regierung des Landes Baden-Württemberg:

**Begründung**

A. Allgemeiner Teil

I. Zielsetzung

1. Änderung des Landesdatenschutzgesetzes (LDSG)

Die Landesregierung hat entsprechend dem Auftrag des Gesetzgebers in Artikel 20 des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO) vom 12. Juni 2018 die Auswirkungen des LDSG unter Mitwirkung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) und der kommunalen Landesverbände überprüft. Der Landtag wurde über das Ergebnis der Evaluierung unterrichtet (Drucksache 17/7596).

Ziel der Evaluierung war es, festzustellen, ob die Regelungen des LDSG normenklar sind und den Bedürfnissen der öffentlichen Stellen entsprechen sowie gegebenenfalls, inwiefern das LDSG nachgebessert oder ergänzt werden sollte. Entsprechend dem in der Evaluierung festgestellten Änderungsbedarf wird das LDSG geändert.

Die Evaluierung des LDSG hat ergeben, dass das Landesdatenschutzrecht sich im Wesentlichen bewährt hat, an einigen Stellen aber einer Nachbesserung bedarf, um praktischen Bedarfen der Verwaltung oder berechtigten Interessen der betroffenen Person zu genügen.

Zugleich soll neuen Rechtsentwicklungen entsprochen werden. Die Anforderungen der Datenökonomie sowie Aspekte des „gestaltenden Datenschutzes“ werden hierbei einbezogen. Datennutzung und Datenschutz sollen in Ausgleich gebracht werden. Hierzu gehört, der Datennutzung zu Forschungszwecken mehr Spielraum zu geben, um die gemeinwohlorientierte Forschung zu stärken.

Im Zuge der fortschreitenden Digitalisierung und zur Entlastung der menschlichen Arbeit wird der Bedarf des Einsatzes von künstlicher Intelligenz (KI) in der Landesverwaltung immer bedeutsamer. Sie ist daher ein unverzichtbarer Querschnittsbereich der Digitalisierungsstrategie digital.LÄND. Der Einsatz von KI in der Verwaltung eröffnet vielfältige Möglichkeiten zur Optimierung von Prozessen, Steigerung der Effizienz und Verbesserung der Servicequalität. Für Baden-

Württemberg können sich so vielfältige Chancen für die Stärkung des Wirtschaftsstandorts und die Leistungsfähigkeit der öffentlichen Verwaltung ergeben. Der Einsatz von KI soll in dem von der EU, dem Bund und dem landesrechtlich gesetzten Rahmen gefördert werden. Dabei soll stets die Gemeinwohlorientierung im Vordergrund stehen. Auch die Justiz kann entscheidend von der Unterstützung durch KI profitieren und wird dementsprechend berücksichtigt.

Gleichzeitig sind Anpassungen des Landesrechts erforderlich zur Durchführung der Verordnung (EU) 2024/1689 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) (KI-VO). Von wenigen Ausnahmen abgesehen (insbesondere Artikel 10 Absatz 5 der KI-VO) enthält die KI-VO keine Vorgaben zur Verarbeitung von personenbezogenen Daten, aber sie macht allgemeine Vorgaben für die relevanten Vorgänge. Dementsprechend sollen die dort verwendeten Begriffe als Orientierung für die Regelung des Einsatzes von KI-Systemen (Artikel 3 Nummer 1 der KI-VO) und KI-Modellen (vgl. Artikel 3 Nummer 63 der KI-VO und Erwägungsgrund 97) in den neuen Regelungen dienen.

2. Änderung des E-Government-Gesetzes Baden-Württemberg (EGovG BW)

Ebenfalls angepasst an die KI-VO und zur Arbeitsentlastung der für die Verwaltungsverfahren zuständigen Behörden soll eine Erprobungsregelung für den automatisierten Erlass von Verwaltungsakten im EGovG BW eingeführt werden.

3. Änderung des Gesetzes zur Ausführung des Personenstandsgesetzes (AGPStG)

Die Standesämter haben den Personen, die in der zuständigen unteren Fachaufsichtsbehörde mit der Standesamtsaufsicht betraut sind, zur Erfüllung dieser Aufgaben den Abruf der in ihrem elektronischen Personenstandsregister gespeicherten personenbezogenen Daten mit Ausnahme der mit einem Sperrvermerk nach § 64 des Personenstandsgesetzes (PStG) versehenen Daten zu ermöglichen. Künftig soll sich das Abrufverfahren auch auf die elektronischen Sammelakten der Standesämter erstrecken. Die dafür erforderliche datenschutzrechtliche Rechtsgrundlage soll durch diese Änderung geschaffen werden.

4. Änderung des Landesinformationsfreiheitsgesetzes (LIFG)

Aufgrund aktueller Rechtsprechung des Verwaltungsgerichtshofs Baden-Württemberg (VGH BW, Urteil vom 25.10.2023 – 10 S 125/22 sowie Urteil vom 08.11.2023 – 10 S 916/22) sind in der Vorschrift des § 2 Absatz 3 LIFG Änderungen zu den Bereichsausnahmen veranlasst. Die Änderungen sollen die Verfassungsmäßigkeit der Regelungen in § 2 Absatz 3 LIFG sicherstellen und Rechtssicherheit in der Anwendung schaffen.

5. Änderung des Landesmediengesetzes (LMedienG)

Die Neufassung dient der Anpassung des Landesmediengesetzes an die Änderungen im Medienstaatsvertrag durch den Fünften Staatsvertrag zur Änderung medienrechtlicher Staatsverträge, der am 1. Oktober 2024 in Kraft trat. Wegen der Überführung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) in das Telekommunikation-Digitale Dienste-Datenschutz-Gesetz (TDDDG) sowie des Telemediengesetzes (TMG) in das Digitale-Dienste-Gesetz (DDG) sind des Weiteren die jeweiligen Verweisungen anzupassen.

6. Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten (OWiZuVO)

In der OWiZuVO ist ebenfalls die Verweisung auf das TTDSG in eine solche auf das TDDDG anzupassen. Die Zuständigkeit für die Ordnungswidrigkeit nach § 33 Absatz 1 DDG übernimmt die Landesanstalt für Kommunikation.

II. Inhalt

1. Änderung des LDSG

Die Änderungen berücksichtigen die Vorgaben der unmittelbar geltenden DSGVO.

Die Regelungen erfolgen in dem durch die Spezifizierungsklauseln der DSGVO eröffneten Rahmen.

Neben redaktionellen Änderungen werden im Wesentlichen folgende Änderungen vorgenommen:

- Im Anwendungsbereich (§ 2) werden Klarstellungen aufgenommen, um den Vorrang der DSGVO zu unterstreichen.

- Begriffsbestimmungen werden eingeführt (§ 2a).

- Die Regelung zu technischen und organisatorischen Maßnahmen (§ 3 LDSG) wird spezifiziert, insbesondere in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Für letztere werden im jeweiligen Kontext spezifische Maßnahmen zur Wahrung der Grundrechte und der Interessen der betroffenen Personen verlangt.

- Für den Einsatz von KI, der neben der Nutzung auch das Training von KI-Systemen und damit zusammenhängende Datenverarbeitungen umfasst, wird der erforderliche Rechtsrahmen geschaffen, damit diese innovative Technologie datenschutzkonform eingesetzt werden kann. Insbesondere das Training von KI erfordert die Verarbeitung personenbezogener Daten und damit eine entsprechende Rechtsgrundlage.

- Mit der Einbeziehung der Aufgabenerledigung durch KI in der justiziellen Tätigkeit der Gerichte in den Anwendungsbereich des LDSG wird der Einsatz von KI legitimiert.

- Für die Anonymisierung von personenbezogenen Daten und für die Herstellung synthetischer Daten wird eine Rechtsgrundlage geschaffen.

- Die Zweckänderungstatbestände des § 5 LDSG werden präzisiert und maßvoll erweitert.

- In § 6 LDSG erfolgen redaktionelle Anpassungen zum besseren Verständnis. Eine Regelung zu den Voraussetzungen für Abrufverfahren und regelmäßige Datenübermittlungen stellt die Einführung solcher Verfahren auf eine sichere Grundlage.

- Um Auftragsverarbeitung zu vereinheitlichen, wird eine gesetzliche Grundlage mit Rechtsverordnungsermächtigung eingeführt. Der Auftragsverarbeitungsvertrag soll auch durch die Fachaufsichtsbehörde geschlossen werden können (§ 7a).

- Die Beschränkungen der Betroffenenrechte (§§ 8 ff. LDSG) bedürfen der Ergänzung durch spezifische Vorschriften nach Artikel 23 Absatz 2 DSGVO.

- Die Verarbeitung zu Zwecken der parlamentarischen Kontrolle wird rechtlich gesondert legitimiert (§ 12a).

- In Bezug auf die Forschungsregelung (§ 13 LDSG) werden mehrere Änderungen vorgenommen, um die Bedingungen für die Forschung zu verbessern. Neben der Anpassung an die Bundesregelung wird die Sekundärnutzung von personenbezogenen Daten für Forschungszwecke, soweit im Rahmen des allgemeinen Datenschutzrechts möglich, unterstützt. Die Kooperation mit der Privatwirtschaft und deren gemeinwohlorientierte Forschung wird ermöglicht.

- Für die Verarbeitung bei Dienst- und Arbeitsverhältnissen (§ 15) werden die Vorschriften zur Verarbeitung besonderer Kategorien personenbezogener Daten um weitere Tatbestände aus der DSGVO und eine Transparenzpflicht bei der Nutzung von KI-Systemen ergänzt.

- Die Vorschrift zu öffentlichen Auszeichnungen und Ehrungen wird in Bezug auf das Widerspruchsrecht klarstellend ergänzt (§ 16).

- Die Verarbeitung besonderer Kategorien personenbezogener Daten im öffentlichen Interesse (§ 17 LDSG) wird im Hinblick auf die Zwecke konkretisiert einschließlich Garantien für die Freiheiten der betroffenen Personen.

- Besondere Verarbeitungssituationen zur Absicherung des Zugangs zu personenbezogenen Daten werden aus § 17 herausgelöst und in § 17a gesondert geregelt.

- Die Öffentlichkeitsarbeit der Behörden wird ebenso wie die Arbeit mit Kontakt- und Adressdaten explizit geregelt. Regelbeispiele sollen zu mehr Rechtssicherheit führen (§ 17a).

- Die Videoüberwachung (§ 18 LDSG) wird als generell geeignetes Mittel zum Schutz besonders sicherheitsrelevanter Objekte zugelassen; dies ist dadurch gerechtfertigt, dass andere Mittel einen unverhältnismäßigen Aufwand erfordern würden oder für die Aufgabenerfüllung nicht geeignet sind. Damit wird die Vorrangprüfung anderer Mittel erleichtert. Des Weiteren wird die Abwägung mit den schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen gesetzlich insoweit determiniert, als der Schutz von

Leben, Gesundheit und Freiheit von Personen an den geschützten Objekten als besonders wichtiges öffentliches Interesse bestimmt wird. Flankierend wird die maximale Speicherfrist auf zwei Monate erhöht. Die Informationspflichten der öffentlichen Stellen werden zugunsten der betroffenen Personen erweitert.

- Ebenso besteht ein Bedarf, KI bei optisch-elektronischer Überwachung in öffentlich zugänglichen Räumen zu nutzen, insbesondere, um Bauwerke und Infrastruktur der öffentlichen Hand technisch zu überwachen. Zwar wird die Verarbeitung personenbezogener Daten hierbei nicht bezweckt; sie kann aber nicht ausgeschlossen werden und bedarf daher einer Legitimation.

- Es wird eine Regelung zur Videoüberwachung einschließlich der KI-Nutzung nicht öffentlich zugänglicher Räume eingefügt und mit Regelungen zum Schutz der betroffenen Personen versehen (§ 18a).

- In engen Grenzen können auch sonstige technische Mittel mit KI-Unterstützung zur Überwachung von Bauwerken und Infrastruktur eingesetzt werden (§ 18b).

- Eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten für die Durchführung sicherheitstechnischer Maßnahmen fehlt bisher im Landesrecht und wird ergänzt. Dabei geht es vor allem um Maßnahmen zur Gewährleistung der Informationssicherheit, die auch die Sensibilisierung der Beschäftigten erfordern.

- Die Aufsichtszuständigkeit der oder des LfDI in Bezug auf die Überwachung der datenschutzrechtlichen Pflichten nach dem TDDDG wird klarstellend geregelt.

2. Änderung des EGovG BW

Um daten- und informationsgeschützte Entscheidungsfindungsprozesse zu verbessern und dabei auch den Einsatz von KI (z. B. für Assistenzsysteme) zu nutzen, sieht der Koalitionsvertrag 2021–2026 von BÜNDNIS 90/DIE GRÜNEN Baden-Württemberg und der CDU Baden-Württemberg sowie die Digitalisierungsstrategie digital.LÄND der Landesregierung vor, dass ergänzend zu § 35a Landesverwaltungsverfahrensgesetz (LVwVfG) eine Regelung zur Erprobung des vollständig automatisierten Erlasses von Verwaltungsakten eingeführt wird. Vorteile eines automatisierten Erlasses sind neben der Effizienz auch die

Vermeidung von menschlichen Flüchtigkeitsfehlern und Fehleinschätzungen. Durch die Beachtung der Vorgaben der KI-VO soll die Neutralität und Objektivität gegenüber menschlichen Entscheidungen erhöht werden.

Die probeweise verfahrensrechtliche Zulassung des vollständig automatisierten Erlasses von Verwaltungsakten erfolgt deshalb zunächst im EGovG BW, während die Voraussetzungen für die Verarbeitung der personenbezogenen Daten zu diesem Zweck durch Artikel 1 im LDSG neu geregelt werden.

3. Änderung des AGPStG

Die Änderung im AGPStG betrifft den elektronischen Zugriff der unteren Fachaufsichtsbehörden auf die Daten der Standesämter. Nach § 4 Absatz 2 AGPStG unterliegen die Standesämter und damit auch deren Registerführung der Fachaufsicht der unteren Verwaltungsbehörden. Die Fachaufsicht über die Standesämter in den Gemeinden der Stadtkreise führt der Stadtkreis als untere Verwaltungsbehörde, über die Standesämter in den übrigen Gemeinden das Landratsamt als untere Verwaltungsbehörde. Nach § 4 a AGPStG können die unteren Fachaufsichtsbehörden zur Erfüllung ihrer Aufgaben schon bisher die in den elektronischen Personenstandsregistern gespeicherten Daten abrufen.

Zur Erfüllung ihrer Aufsichtsaufgaben sollen sie in Zukunft auch auf die in den elektronischen Sammelakten gespeicherten Daten zugreifen können. Die Personenstandsregister werden seit dem 1. Januar 2014 nur noch elektronisch geführt. Die Sammelakten der Standesämter werden zum Teil noch als gesonderte Akte in Papier geführt. Die Standesämter haben nach § 22 Satz 1 Personenstandsverordnung (PStV) allerdings auch die Möglichkeit, die Sammelakten elektronisch zu führen. Die Standesämter im Land haben eine elektronische Nacherfassung ihrer Sammelakten entweder schon durchgeführt oder sind dabei diese nach und nach elektronisch zu erfassen.

4. Änderung des LIFG

Es erfolgen Änderungen in der Vorschrift zu den Bereichsausnahmen in § 2 Absatz 3 LIFG.

Die stellenbezogenen Bereichsausnahmeregelungen in den Nummern 1 bis 4 werden um zwei informationsbezogene Bereichsausnahmeregelungen in den neuen Nummern 5 und 6 ergänzt:

- Die stellenbezogene Bereichsausnahme in Nummer 2 wird im Hinblick auf den Schutz der verfassungsrechtlich gewährleisteten Kunst- und Wissenschaftsfreiheit in eine informationsbezogene Bereichsausnahme umgewandelt (Nummer 5).

- Die stellenbezogene Bereichsausnahme in Nummer 2 wird für die Schulen nach § 2 des Schulgesetzes für Baden-Württemberg und die Ausbildungs- und Prüfungsbehörden in Bezug auf Leistungsbeurteilungen und Prüfungen beibehalten.

- In Nummer 6 wird eine informationsbezogene Bereichsausnahme zum Schutz des religiösen Selbstbestimmungsrechts der Kirchen, Religions- und Weltanschauungsgemeinschaften sowie ihrer Untergliederungen und Einrichtungen aufgenommen.

Im Übrigen erfolgen sprachliche Anpassungen sowie redaktionelle Änderungen.

5. Änderung des LMedienG

Die Verpflichtung zur Sicherung der Regionalfensterprogramme in Baden-Württemberg wird gesetzlich klargestellt. Die Zulassung für Fensterprogrammveranstalter wird auf zehn Jahre begrenzt. Des Weiteren erfolgt die notwendige Anpassung an die bundesgesetzliche Überführung des Telemediengesetzes in das Digitale-Dienste-Gesetz. Die Landesanstalt für Kommunikation übernimmt zusätzlich die Zuständigkeit der Verwaltungsbehörde für die Verfolgung und Ahndung der Ordnungswidrigkeit nach § 33 Absatz 1 DDG.

6. Änderung der OWiZuVO

Nach Ablösung des TTDSG durch das TDDDG ist die Gesetzesbezeichnung in § 3a OWiZuVO zu ändern. Die Zuständigkeit für die Ordnungswidrigkeit nach § 33 Absatz 1 DDG, vormals 11 Absatz 1 TMG wird auf die Landesanstalt für Kommunikation übertragen. Die Vorschrift des § 4 Absatz 2 Nummer 4 OWiZuVO ist daher anzupassen.

III. Alternativen

1. Änderung des LDSG

Keine. Mit den neu aufgenommenen Vorschriften werden der Verwaltung die datenschutzrechtlich erforderlichen Rechtsgrundlagen für moderne Verwaltungsarbeit zur Verfügung gestellt. Um Rechtssicherheit zu erlangen und dem Grundrecht auf Datenschutz zu genügen, sind gesetzliche Regelungen erforderlich.

Der Einsatz innovativer Technologien wie KI und automatisierter Verfahren ist unverzichtbar für die Leistungsfähigkeit der Verwaltung. Der Schutz der Bürgerinnen und Bürger erfordert hierfür einen gesetzlichen Rahmen.

2. Änderung des EGovG BW

Keine. Für die Erprobung des automatisierten Erlasses von Verwaltungsakten ist die Ergänzung des EGovG BW notwendig.

3. Änderung des AGPStG

Keine. Für den elektronischen Zugriff auf die Sammelakten bedarf es aus datenschutzrechtlichen Gründen einer gesetzlichen Zulassung der Einrichtung durch die Standesämter im AGPStG.

4. Änderung des LIFG

Keine. Um verfassungsrechtliche Bedenken und Zweifelsfragen auszuräumen, sind gesetzliche Änderungen der Vorschriften zu den Bereichsausnahmen erforderlich.

5. Änderung des LMedienG

Keine. Es handelt sich im Wesentlichen um notwendige Anpassungen an geänderte Regelungen.

6. Änderung der OWiZuVO

Keine. Der Zuständigkeitswechsel für die Bußgeldvorschrift des § 33 Absatz 1 DDG erfolgt aufgrund der größeren Sachnähe der Landesanstalt für Kommunikation.

IV. Änderungen

Geändert werden die §§ 2, 3, 4, 5, 6, 8, 9, 10, 13, 15, 16, 17, 18 LDSG, sowie § 4a AGPStG, § 2 LIFG, §§ 12, 23, 30, 51 LMedienG, §§ 3a, 4 OWiZuVO.

Neu eingefügt werden in das LDSG §§ 2a, 3a, 7a, 9a, 11a, 12a, 17a, 17b, 18a, 18b, 27a sowie in das EGovG BW § 17a.

V. Finanzielle Auswirkungen

1. Änderung des LDSG

Finanzielle Auswirkungen sind nicht zu erwarten, da die Pflichten öffentlicher Stellen nur geringfügig erweitert werden.

2. Änderung des EGovG BW

Die Erprobung automatisierter Verfahren steht im Ermessen der Behörde. Ggf. können durch die Nutzung automatisierter Verfahren Kosten eingespart werden.

3. Änderung des AGPStG

**Finanzielle Auswirkungen:**

| | | Laufendes Haushaltsjahr | Folgendes Haushaltsjahr<br><br>In Tsd. Euro | Restliche Jahre der Finanzplanung<br><br>In Tsd. Euro | | |
|---|---|---|---|---|---|---|
| 1 | **Land**<br>Ausgaben insgesamt | 0 | 0 | | | |
| | davon<br>Personalausgaben | | | | | |
| | Anzahl der erforderlichen Neustellen | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | **Kommunen** | 0 | 300 | 200 | 200 | 200 |
| 3 | **Andere öffentlich-rechtliche Körperschaften, Anstalten und Stiftungen** | | | | | |
| 4 | **Ausgaben insgesamt** | | 300 | 200 | 200 | 200 |
| 5 | **Finanzierung oder Gegenfinanzierung, soweit vorhanden** | | | | | |
| 6 | **strukturelle Mehrbelastung / Entlastung** (Saldo Ziffer 3 - Ziffer 4) | | | | | |

Die technischen Voraussetzungen für das automatisierte Abrufverfahren der Daten aus den Personenstandsregistern durch die unteren Fachaufsichtsbehörden nach § 4a AGPStG wurden bei Komm.ONE, dem kommunalen IT-Dienstleister, der in Baden-Württemberg die elektronischen Personenstandsregister im Auftrag der angeschlossenen Gemeinden führt, durch einen sog. „Aufsichtsclient“ bereits geschaffen.

Für die Erweiterung des „Aufsichtsclients“ auf die elektronischen Sammelakten entstehen den unteren Fachaufsichtsbehörden ausschließlich Sachaufwendungen, die wie folgt beziffert werden:

Für Entwicklung, Implementierung und Einbindung in das Fachverfahren werden von dem IT-Dienstleister Komm.ONE einmalige Kosten in Höhe von ca. 300.000 EUR veranschlagt. Rund 175.000 - 200.000 EUR jährliche Kosten fallen voraussichtlich für die Pflege, Betreuung und Lizenzierung an.

Durch die elektronische Einsichtnahme werden Vor-Ort-Termine in den meisten Fällen obsolet und führen zu entsprechenden Entlastungen.

Bei der Verpflichtung der unteren Fachaufsichtsbehörden, den o.g. „Aufsichtsclient“ auf die elektronischen Sammelakten zu erweitern, handelt es sich um keine Sach- oder Zweckaufgabe mit Außenwirkung, sondern um eine reine Organisationsaufgabe. Organisationsaufgaben sind nicht vom Konnexitätsprinzip des Artikels 71 Absatz 3 der Verfassung des Landes Baden-Württemberg umfasst.

4. Änderung des LIFG

Es entstehen keine Kosten.

5. Änderung des LMedienG

Durch Anpassungen an bereits getroffene Regelungen werden keine Kostenfolgen ausgelöst.

6. Änderung der OWiZuVO

Die Übertragung der Zuständigkeit vom Regierungspräsidium Karlsruhe auf die Landesanstalt für Kommunikation löst keine direkten Kostenfolgen aus.

VI. Bürokratievermeidung

Die getroffenen Vorschriften, insbesondere diejenigen zum Einsatz von KI und zur Erprobung automatisierter Verfahren sowie die Anpassungen der Bereichsausnahmen im LIFG regeln die Voraussetzungen für rechtssichere und datenschutzgerechte Verfahren in der Verwaltung. Damit tragen sie zur Entlastung und Effizienzsteigerung der Verwaltung bei. Die Evaluierungspflicht für die Erprobung automatisierter Verfahren wird nur für den Fall der geplanten Fortsetzung des automatisierten Verfahrens eingeführt und ist daher bürokratiearm ausgestaltet.

VII. Wesentliche Ergebnisse des Nachhaltigkeitschecks

1. Änderung des LDSG

Die Anpassung des LDSG an die Anforderungen der Praxis unterstützt die Verwaltung nachhaltig und trägt zur Ressourcenschonung bei. Insbesondere die Regulierung des KI-Einsatzes ist in der Lage, die Grundlage für die Einführung von datenschutzgerechter KI in der Verwaltung zugunsten einer effizienten Aufgabenerledigung zu sein, von der die Bürgerinnen und Bürger ebenso profitieren.

2. Änderung des EGovG BW

Dort, wo sich der automatisierte Erlass von Verwaltungsakten eignet, kann sowohl die Effizienz der Verwaltung gesteigert wie die Richtigkeit und Objektivität der Entscheidungen erhöht werden. Automatisierte Entscheidungen sollten aber nur ergehen, wenn sie zuvor erprobt wurden, damit die Ziele erreicht und Risiken ausgeschlossen werden.

3. Änderung des AGPStG

Der Gesetzentwurf fördert die Digitalisierung und Zukunftsfähigkeit der öffentlichen Verwaltung. Aufwändige Vor-Ort-Termine werden künftig weitgehend obsolet.

4. Änderung des LIFG

Die Änderungen sind verfassungsrechtlich angezeigt und tragen so zur Rechtssicherheit bei.

5. Änderung des LMedienG

Materiell werden Regionalfensterprogramme zugunsten der Information und Partizipation der Bürgerinnen und Bürger gesichert und die Meinungsvielfalt gestärkt.

6. Änderung der OWiZuVO

Es ist zu erwarten, dass in Bezug auf die Überwachung der Pflichten nach dem DDG die Landesanstalt für Kommunikation ihre Expertise für digitale Dienste einbringen kann.

VIII. Wesentliche Ergebnisse des Digitaltauglichkeitschecks

Die Zielrichtung aller Gesetzesänderungen geht unter anderem dahin, verwaltungsinterne Geschäftsprozesse verstärkt medienbruchfrei elektronisch abzuwickeln. In dieser Beziehung sind erhebliche Verbesserungen zu erwarten. Die Änderung des LDSG adressiert insbesondere den datenschutzgerechten Einsatz von KI und findet angemessene Regelungen zum Schutz der betroffenen Personen.

IX. Sonstige Kosten für Private

Die Änderungsgesetze adressieren ausschließlich öffentliche Stellen. Den Bürgerinnen und Bürgern sowie der Wirtschaft entstehen keine Kosten.

B. Einzelbegründung

1. Zu Artikel 1 – Änderung des LDSG

Zu Nummer 1 (§ 2 – Anwendungsbereich)

Zu Buchstabe a (Absatz 1)

Die Einfügung dient der Klarstellung, dass abweichende Definitionen des Verantwortlichen in einem anderen Gesetz erfasst werden. Hingewiesen wird auf § 67 Absatz 4 SGB X, der für Gebietskörperschaften als Leistungsträger die funktional zuständige Organisationseinheit als Verantwortlichen festlegt.

Zu Buchstabe b (Absatz 4)

Durch das Haushaltsbegleitgesetz 2025/2026 vom 17. Dezember 2024 (GBl. 2024 Nr. 114) wurden die staatlichen Rechnungsprüfungsämter aufgelöst und in den Rechnungshof eingegliedert. Diese Änderung wird im LDSG durch die Streichung der staatlichen Rechnungsprüfungsämter in Satz 3 nachvollzogen.

Zu Buchstabe c (Absatz 5)

Das LDSG findet bisher gemäß § 2 Absatz 5 lediglich auf die Verwaltungsangelegenheiten der Gerichte Anwendung. Für die justizielle Tätigkeit ist bisher die Anwendung des LDSG ausgeschlossen. Dabei meint der Begriff „justizielle Tätigkeit“ in Übereinstimmung mit der Rechtsprechung des Europäischen Gerichtshofs (EuGH, Urteil vom 24. März 2022 – C-245/20) sämtliche Tätigkeiten, die mit der gerichtlichen Entscheidungsfindung in Zusammenhang stehen.

Der Anwendungsbereich des LDSG wird mit der Gesetzesänderung auf die justizielle Tätigkeit der Gerichte erstreckt, soweit die Datenverarbeitung nicht in den Anwendungsbereich 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, zuletzt ber. ABl. L 74 vom 4.3.2021, S. 36) fällt und soweit KI-Systeme und KI-Modelle zum Einsatz kommen. Dabei orientieren sich die Begriffe KI-System und KI-Modell an dem in der KI-VO zum Ausdruck kommenden Verständnis. KI-Systeme und KI-Modelle werden in § 2a Absatz 2 und Absatz 3 definiert.

Die mit Hilfe von KI-Systemen und KI-Modellen insbesondere im Rahmen von elektronischen Aktenführungssystemen, Datenbanken und digitalen Kommunikationssystemen verarbeiteten personenbezogenen Daten sollen besser geschützt werden.

Gemäß Erwägungsgrund 20 der DSGVO kann im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden auszusehen haben. Bestimmte Aspekte des Datenschutzes werden im Bereich der justiziellen Tätigkeit bereits in den Prozessordnungen geregelt (z. B. in § 299 ZPO für die Auskunft aus den Akten) . Zum Einsatz von Verfahren der KI fehlt es in den Prozessordnungen bisher aber an Regelungen.

Die Gesetzgebungskompetenz des Landes für die vorliegende Gesetzesänderung ergibt sich aus Artikel 70, 72 Absatz 1 GG:

Allgemein leitet sich die Gesetzgebungskompetenz für das Datenschutzrecht als Querschnittsmaterie von dem jeweiligen im Übrigen betroffenen Rechtsgebiet kraft Sachzusammenhangs ab. Im Bereich der dem Bund nach Art. 74 Absatz 1 Nummer 1 GG (gerichtliches Verfahren) zustehenden konkurrierenden Gesetzgebungsbefugnis hat er von dieser keinen abschließenden Gebrauch gemacht. Vielmehr hat der Bund in § 1 Absatz 1 Satz 1 Nummer 2 BDSG den Anwendungsbereich für öffentliche Stellen der Länder auf den Fall beschränkt, dass die Länder keine datenschutzrechtlichen Regelungen durch Landesgesetz getroffen haben. Folglich hat der Bundesgesetzgeber einer landesdatenschutzrechtlichen Regelung im Grundsatz – und damit auch im Bereich der justiziellen Tätigkeit – ausdrücklich den Vorrang eingeräumt.

Die teilweise Erweiterung des LDSG auf den justiziellen Bereich ist eine notwendige Maßnahme, um den Schutz personenbezogener Daten in der Justiz effektiv zu gewährleisten. Dabei wird den spezifischen Anforderungen der richterlichen Unabhängigkeit in vollem Umfang Rechnung getragen. Die vorgeschlagene Gesetzesänderung greift nicht in die verfahrensrechtlichen Grundsätze ein. Sie

ergänzt sie um datenschutzrechtliche Bestimmungen, die unionsrechtlich bereits vorgegeben sind. Durch die Einführung klarer datenschutzrechtlicher Regelungen werden sowohl der Schutz der betroffenen Personen als auch die Rechtssicherheit der Datenverarbeitung in der Justiz verbessert.

Es wird ein Gleichlauf zu der Entwicklung und Anwendung von KI in der Verwaltung hergestellt, damit der Schutz personenbezogener Daten auch in Bezug auf justizielle KI-Tätigkeiten vollständig gewährleistet werden kann.

Absatz 5 Satz 2 Halbsatz 2 dient der Klarstellung. Er bezieht sich lediglich auf Absatz 5 Satz 2. Die Datenschutzaufsichtsbehörden sind nach Artikel 55 Absatz 3 DSGVO nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen. Folglich gilt Abschnitt 5 nicht, soweit die Gerichte im Rahmen ihrer justiziellen Tätigkeit personenbezogene Daten in Bezug auf KI-Systeme und KI-Modelle verarbeiten.

Ebenfalls der Klarstellung dient Absatz 5 Satz 3, wonach Absatz 5 Satz 1 und 2 die Regelung in Absatz 1 Nummer 3 unberührt lässt.

Zu Nummer 2 (§ 2a neu – Begriffsbestimmungen)

Zur Unterstützung der Anwendung, insbesondere in Bezug auf den neu geregelten Einsatz von KI, werden Begriffsbestimmungen aufgenommen.

Zu Absatz 1

Es wird klargestellt, dass die Begriffsbestimmungen der DSGVO maßgeblich sind. Die Begriffsbestimmungen der DSGVO finden sich im Wesentlichen in deren Artikel 4. Dessen Nummer 1 definiert die personenbezogenen Daten; zu diesen gehören auch die besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 DSGVO.

Zu Absatz 2

Um Kohärenz mit der KI-Verordnung herzustellen, wird für den verwendeten Begriff der KI-Systeme auf die in Artikel 3 Nummer 1 der KI-Verordnung aufgenommene Begriffsbestimmung verwiesen.

Zu Absatz 3

Das KI-Modell wird in der KI-Verordnung nicht im umfassenden Sinn definiert. In Artikel 3 Nummer 63 findet sich lediglich die Begriffsbestimmung des „KI-Modells mit allgemeinem Verwendungszweck“. Diese ist zu erweitern um KI-Modelle für spezielle Verwendungszwecke. Ein Beispiel wäre ein KI-Modell, das spezifisch dazu dient, Baugenehmigungsanträge oder Gerichtsakten zu strukturieren. Wie in den Sätzen 6 bis 8 von Erwägungsgrund 97 der KI-VO zum Ausdruck kommt, sind KI-Modelle wesentliche Komponenten von KI-Systemen, aber sie stellen für sich genommen keine KI-Systeme dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon.

Einbezogen werden in Bezug auf die Verarbeitung personenbezogener Daten KI-Modelle für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen; die KI-VO gilt für diese, ebenso wie für KI-Systeme mit demselben Zweck, gemäß Artikel 2 Absatz 6 der KI-VO nicht.

Zu Nummer 3 (§ 3 – Sicherstellung des Datenschutzes)

Zu Buchstabe a

Die Sicherstellung des Datenschutzes durch technische und organisatorische Maßnahmen gehört nach Artikel 25, 32 der DSGVO zu den zentralen Anforderungen des Datenschutzes. Um Missverständnisse zu vermeiden, wird dies durch die Neuformulierung des § 3 Absatz 1 LDSG nunmehr klargestellt. Es sind zumindest die aufgezählten Maßnahmen auf ihre Erforderlichkeit zu prüfen.

Zu Buchstabe b

Infolge der Änderung in Satz 3 kann Nummer 1 entfallen: Die bisherigen Nummern 2 bis 6 werden Nummern 1 bis 5.

Zu Buchstabe c

Eine häufige Ursache für Datenschutzvorfälle ist die unnötige direkte Anbindung von rein internen Systemen an das Internet. Es wird daher als zusätzliche zu prüfende Maßnahme die Abschottung der internen Systeme vor unbefugten Zugriffen aus öffentlichen Telekommunikationsnetzen eingefügt. Die Abschottung ist nicht alleine durch die physische Trennung erreichbar, sondern auch durch logische Trennung, wie dem Einsatz von Segmentierung oder Firewallsystemen.

Bei der physischen Trennung wird z.B. ein System komplett ohne Netzwerkschnittstelle betrieben oder vom bestehenden Netzwerk abgekoppelt. Bei der logischen Trennung kann z.B. eine Firewall oder ein virtuelles, logisch getrenntes Netzwerk (VLAN) eingesetzt werden, um den Zugang zum Internet softwareseitig zu steuern oder zu unterbinden.

Eine gänzliche Abschottung von rein internen Systemen wird häufig nicht umsetzbar sein, da auch rein interne Systeme oftmals eine Anbindung an das Internet benötigen, etwa zur Fernwartung oder zur Durchführung von Herstellerupdates. Daher wird die Abschottung auf unbefugte Zugriffe beschränkt.

Zu Nummer 4 (§ 3a neu – Nutzung von KI-Systemen)

Für die Nutzung von KI-Systemen kann die Eingabe von personenbezogenen Daten erforderlich sein und die Ausgabe eines KI-Systems kann Angaben über natürliche Personen enthalten. § 3a knüpft an bestehende Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten an und erklärt die Verarbeitung– soweit die Voraussetzungen zur Verfügung stehen – für zulässig.

KI soll nämlich der Verwaltung als weiteres Betriebsmittel zur Aufgabenerledigung zur Verfügung stehen. KI ist in besonderer Weise geeignet, die Verwaltung dabei zu unterstützen, die gesetzlichen Aufgaben effizient, in der gebotenen Qualität und ressourcenschonend zu erfüllen. Die KI-VO erkennt dieses Ziel ausdrücklich als in erheblichem öffentlichen Interesse liegend an (vgl. Artikel 59 Absatz 1 Buchst. a Ziffer v KI-VO). Auch weitere Gemeinwohlziele wie die öffentliche Sicherheit und die öffentliche Gesundheit, die Sicherung von Mobilität und kritischer Infrastruktur u. v. m. können durch die Nutzung von KI befördert werden. KI kommt den Bürgerinnen und Bürgern und der Wirtschaft zugute und ist für die Zukunft der Verwaltung und den Wirtschaftsstandort Baden-Württemberg unverzichtbar.

Die Vorschrift soll zum Ausdruck bringen, dass KI-Tools für die Verwaltung Betriebsmittel zur Erledigung von Aufgaben darstellen und als solche für ihre Nutzung den Zulässigkeitsvoraussetzungen für die Aufgabenerfüllung unterliegen. Zugleich wird vorausgesetzt, dass die eingesetzte KI entsprechend den rechtlichen Vorschriften entwickelt wurde und daher einsetzbar ist. Insbesondere sind die Vorschriften der KI-VO zu beachten. Für die Verarbeitung besonderer Kategorien personenbezogener Daten bedarf es zusätzlich des Vorliegens der Voraussetzungen einer Ermächtigungsnorm aus Artikel 9 Absatz 2 DSGVO.

Die Verarbeitung von personenbezogenen Daten durch Nutzung von KI-Systemen nach § 3a dient allein dem ursprünglichen Verarbeitungszweck und verändert das KI-System nicht. In Abgrenzung dazu wird in § 11a die Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen geregelt. Wenn bei der Nutzung von KI-Systemen gleichzeitig auch ein Training etc. des KI-Systems erfolgen soll, dann müssen die Voraussetzungen von § 3a und § 11a nebeneinander erfüllt sein.

Zu Nummer 5 (§ 4 Absatz 2 neu)

Zu Buchstabe a

Redaktionelle Folgeänderung zu Buchstabe b.

Zu Buchstabe b

Ergänzend zur datenschutzrechtlichen Generalklausel wird eine Erlaubnisnorm zur Anonymisierung sowie zur Herstellung synthetischer Daten eingefügt. Anonymisieren ist das Verändern von Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Synthetische Daten sind »künstliche« Daten, die in Eigenschaften und Struktur (idealerweise) den Originaldaten stark ähnlich sind, selbst aber keine »echten« Datenpunkte enthalten. Synthetische Daten werden aus Originaldaten generiert, indem ein mathematisches Modell trainiert wird, das die Struktur der ursprünglichen Daten lernt und reproduzieren kann. Synthetische Daten und Originaldaten sollten daher bei einer statistischen Analyse sehr ähnliche Ergebnisse liefern (vgl. Kompetenzzentrum öffentliche IT, abrufbar unter: https://www.oeffentliche-it.de/blog/synthetische-daten/). Bei der Herstellung synthetischer Daten sind also im Verhältnis zu einer bloßen Entfernung von personenbezogenen Daten beim Regelfall der Anonymisierung mehr Datenverarbeitungsschritte erforderlich, damit die „synthetischen Daten“ nach der Anonymisierung in Eigenschaften und Struktur den Originaldaten stark ähneln, aber keine personenbezogenen Originaldaten enthalten.

Vor allem für die Forschung (§ 13) (andernfalls müssten die Voraussetzungen des § 13 für die Verarbeitung personenbezogener Daten vorliegen) sowie für die Entwicklung und das Training von KI (ansonsten § 11a) werden anonyme – und möglichst synthetische – Daten benötigt. Unabhängig von der strittigen Frage, ob die Anonymisierung eine Verarbeitung im Sinne der DSGVO ist, wird zur Klarstellung

eine Rechtsgrundlage gemäß Artikel 6 DSGVO geschaffen, um dem Grundsatz der Datenminimierung – Daten dürfen nur in dem für die Zwecke der Verarbeitung notwendigen Maß verarbeitet werden – nach Artikel 5 Absatz 1 Buchstabe c DSGVO Rechnung zu tragen. Da Echtdaten als Muster oder Vorlage für die Erstellung synthetischer Daten herangezogen werden, bedarf es diesbezüglich einer datenschutzrechtlichen Regelung. Die Erlaubnisnorm des § 4 Absatz 2 schafft eine rechtssichere Grundlage hierfür.

Zu Nummer 6 (§ 5 Absatz 1 – Ergänzung)

Zu Buchstabe a

Die in § 5 Absatz 1 Nummer 1 geregelte Erlaubnis zur Zweckänderung aus Gründen des Gemeinwohls beruht auf Artikel 6 Absatz 4 in Verbindung mit Artikel 23 Absatz 1 Buchst. e DSGVO. Dort wird der Begriff Gemeinwohl nicht verwendet. Dieser soll daher gemäß Artikel 23 Absatz 2 Buchst. a DSGVO konkretisiert werden. Er ist von der Intention gleichzusetzen mit den in Artikel 23 Absatz 1 Buchst. e DSGVO geschützten Zielen des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats. Alle Gemeinwohlziele müssen die gleiche Relevanz aufweisen wie die genannten Ziele im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit. Die gesetzliche Konkretisierung stellt daher klar, dass die gesetzlich anerkannten allgemeinen öffentlichen Interessen maßgeblich sind. Diese können sich auch aus Rechtsakten der Europäischen Union, wie z. B. dem Daten-Governance-Rechtsakt (vgl. Erwägungsgründe 24 und 45) ergeben.

Zu Buchstabe b

Die geltende Fassung ist in § 5 Nummer 3 zu eng gefasst. Die Neufassung orientiert sich an § 23 Absatz 1 Nummer 4 BDSG. Entsprechend der Bundesregelung wird die Beschränkung auf die Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung aufgegeben. Als Korrektiv ist vielmehr darauf zu achten, dass die zweckändernde Verarbeitung verhältnismäßig ist.

Zu Buchstabe c

Redaktionelle Folgeänderung zu Buchstabe d.

Zu Buchstabe d (Nummer 5 neu)

Dieser zusätzliche Zweckänderungstatbestand, der auf der Grundlage von Artikel 6 Absatz 4 in Verbindung mit Artikel 23 Absatz 1 Buchst. i DSGVO eingefügt wird, stellt klar, dass Zweckänderungen zugunsten der betroffenen Person zulässig sind, sofern dies objektiv im Interesse der betroffenen Person ist. Diese soll keine Nachteile durch unnötige Einbeziehung erleiden, wenn es sich um eine erkennbar begünstigende Maßnahme handelt und notwendige Angaben bereits bekannt sind. Die Zweckänderung ist jedoch unzulässig, wenn (z. B. aufgrund vorliegender Äußerungen) anzunehmen ist, dass die betroffene Person mit der Zweckänderung nicht einverstanden wäre.

Im Zusammenspiel mit § 6 erlaubt die Regelung insbesondere eine Weiterleitung an die zuständige Behörde, wenn die betroffene Person ihr Anliegen an die unzuständige Behörde adressiert; denn die Weiterleitung an die zuständige Behörde entspricht in der Regel dem Interesse der betroffenen Person. Ob eine Ausnahme von dieser Regel vorliegt, ist jeweils zu prüfen.

Zu Nummer 7 (§ 6 – Übermittlung personenbezogener Daten)

Die Übermittlungsvorschrift wird zum besseren Verständnis neu gefasst. Insbesondere wird in der Überschrift klargestellt, dass nur die Übermittlung personenbezogener Daten zu anderen Zwecken geregelt wird. Im Übrigen orientiert sich die Struktur der Vorschrift nunmehr in Absatz 1 und Absatz 2 an § 25 BDSG. Inhaltlich wurde keine Veränderung zu § 6 Absatz 1 LDSG vorgenommen, lediglich nunmehr die Alternative der Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen der übermittelnden Stelle eingefügt (vgl. Absatz 2 Nummer 3) sowie klargestellt, dass die Norm für die Übermittlung an alle Stellen innerhalb des öffentlichen Bereichs, also auch an die öffentlichen Stellen des Bundes und der Länder, gilt.

Absatz 3 fügt eine klarstellende Regelung zur Übermittlung in andere Mitgliedstaaten der Europäischen Union, des Europäischen Wirtschaftsraums oder an Organe und Einrichtungen der Europäischen Union ein. Durch die DSGVO wurde ein einheitlicher Rechtsraum in Europa für die Verarbeitung personenbezogener Daten geschaffen, sodass die Vorschriften des LDSG auch für die Übermittlung an die aufgeführten Stellen gelten. Eine Ausnahme ist in Absatz 4 für Datenübermittlungen auf Ersuchen aufgenommen.

In Absatz 4 wird der Grundsatz festgelegt, dass die übermittelnde öffentliche Stelle die Verantwortung für die Übermittlung trägt. Dies gilt auch im Fall von

Datenübermittlungen auf Ersuchen. Die Verantwortung für die Rechtmäßigkeit des Ersuchens oder des Abrufs im Fall von automatisierten Abrufen trägt die ersuchende bzw. die abrufende Stelle. Im Ergebnis ist die übermittelnde Stelle dafür verantwortlich, dass für die Durchführung der Übermittlung eine Rechtsgrundlage besteht, ausgehend davon, dass das Ersuchen oder der Abruf rechtmäßig sind.

In Absatz 5 werden die Voraussetzungen für die Einrichtung eines automatisierten Abrufverfahrens normiert, sofern die Einrichtung nicht durch das Registermodernisierungsgesetz oder andere Gesetze (z. B. das AGPStG) geregelt ist. Eine solche Regelung fehlt bisher. Wegen der erhöhten Gefahren für den Schutz personenbezogener Daten durch automatisierte Abrufe bedarf die Einrichtung einer Abwägung des Nutzens mit der Beeinträchtigung des informationellen Selbstbestimmungsrechts der betroffenen Personen sowie technischer und organisatorischer Maßnahmen zur Vermeidung von Beeinträchtigungen. Abrufverfahren, die für jedermann zugängliche Daten eingerichtet werden, sind von der Regelung in Satz 1 nicht betroffen. Dies gilt unabhängig davon, ob es einer Zulassung der Person zum Abruf bedarf.

Zu Nummer 8 (§ 7a neu – Auftragsverarbeitung durch staatliche Behörden)

Zu Absatz 1

Zur Entlastung der Verwaltung wird in Absatz 1 die Auftragsverarbeitung, sofern eine öffentliche Stelle gesetzlich verpflichtet oder berechtigt ist, eine staatliche Behörde zu beauftragen, gesetzlich geregelt. Dies ist gemäß Artikel 28 Absatz 3 Satz 1 DSGVO zulässig. Staatliche Behörden sind gemäß § 1 des Landesverwaltungsgesetzes Baden-Württemberg Behörden, die staatliche Verwaltungsaufgaben zu erfüllen haben, also Behörden des Landes (unmittelbare Landesverwaltung). Als Beispiel und Hauptanwendungsfall ist die BITBW anzuführen, die als Landesoberbehörde fungiert. Des Weiteren werden Anstalten des öffentlichen Rechts in alleiniger Trägerschaft des Landes erfasst. Damit fallen alle Anstalten heraus, die dem kommunalen Bereich zugeordnet sind. Insbesondere soll damit die Einbeziehung der L-Bank gewährleistet werden, sofern sie als Auftragsverarbeiter für das Land (z. B. bei Förderanträgen) tätig wird. Öffentliche Stellen können sowohl dem Land als auch einer kommunalen Gebietskörperschaft zugehören; auch andere öffentlich-rechtliche Träger wie Anstalten des öffentlichen Rechts oder kommunale Zweckverbände werden unter die öffentlichen Stellen gefasst.

Die staatlichen Hochschulen im Sinne des § 1 Absatz 2 des Landeshochschulgesetzes werden von der Regelung ausgenommen. Für sie gilt auch Absatz 2 nicht. Die Spielräume, die die DSGVO für die Auftragsverarbeitung bietet, sollen für die Hochschulen erhalten bleiben.

Die Mitteilung der in Absatz 2 Satz 1 unter den Nummern 1 bis 4 genannten Parameter begründet den Auftragsverarbeitungsvertrag.

Entscheidend für die Begründung eines Auftragsverarbeitungsvertrags ist gemäß Artikel 28 Absatz 3 Buchst. a DSGVO die Verarbeitung nach den Weisungen der verantwortlichen öffentlichen Stelle. Mit der einheitlichen Festlegung der Nutzungsbedingungen kann die individuelle Vertragsaushandlung entfallen und die Verantwortlichen und Auftragsverarbeiter werden an einheitliche Vorgaben gebunden. Die Rechtmäßigkeit wird dadurch in verstärktem Maße sichergestellt.

Bestehende einzelvertragliche Regelungen zur Auftragsverarbeitung werden entsprechend der Verordnung ersetzt, einzelvertragliche Regelungen bleiben aber zulässig. Dies schließt es ein, dass auch die bestehenden Regelungen bestehen bleiben können, sofern sie den Vorgaben der DSGVO entsprechen.

Zu Absatz 2

Die Nutzungsbedingungen bedürfen einer Regelung durch Rechtsverordnung. Eine entsprechende Ermächtigung wird aufgenommen. Die Ermächtigung wird der Landesregierung zugewiesen, um einheitliche Vertragsbedingungen zu gewährleisten. Der für den Vertragsschluss zu leistende Aufwand wird sowohl für die öffentlichen Stellen als Verantwortliche wie für die staatlichen Behörden als Auftragsverarbeiter erheblich reduziert.

Zu Absatz 3

Neu eingefügt wird in Absatz 3 eine Regelung zur Beauftragung der Auftragsverarbeitung durch die Fachaufsichtsbehörde mit Wirkung für die nachgeordneten Behörden. Hierfür wurde in der Evaluierung ein Bedarf festgestellt, insbesondere, um ein Instrument für eilige und einheitliche Auftragsverarbeitungen zur Verfügung zu stellen. Dies kann bei Beschaffungsmaßnahmen, OZG-Leistungen oder IT-Vereinheitlichungsmaßnahmen oder in Fällen besonderer Eilbedürftigkeit sinnvoll sein. Das Auftragsverarbeitungsverhältnis wird jeweils nur zwischen der nutzenden Stelle und dem Auftragsverarbeiter konstituiert.

Zu Nummer 9 (§ 8 – Beschränkung der Informationspflicht)

Zu Buchstabe a (Absatz 2)

Die Beschränkungen der Informationspflicht beruhen auf Artikel 23 Absatz 1 DSGVO. Wie Artikel 23 Absatz 2 DSGVO regelt, müssen spezifische Vorschriften in Bezug auf die Transparenz und die Rechte der betroffenen Personen getroffen werden. Solche Regelungen fehlen bisher in § 8. In Anlehnung an die Regelungen in §§ 32, 33 BDSG werden entsprechende Maßnahmen vorgeschrieben. Die Pflicht zur Nachholung der Information, sobald der vorübergehende Hinderungsgrund entfallen ist, ergibt sich bereits aus dem Wort „solange“ in § 8 Absatz 1.

Zu Absatz 2

Mit der Vorschrift wird die öffentliche Stelle angehalten, soweit wie möglich Transparenz über die Verarbeitung personenbezogener Daten der betroffenen Personen herzustellen. Die Information kann beispielsweise durch die Bereitstellung der Information auf einer allgemein zugänglichen Webseite der verantwortlichen öffentlichen Stelle erfolgen (vgl. Erwägungsgrund 58 Satz 2 der DSGVO).

Zu Buchstabe b

Redaktionelle Folgeänderung zu Buchstabe a.

Zu Nummer 10 (§ 9a neu – Beschränkungen des Rechts auf Berichtigung)

Nach dem derzeit bestehenden Entwicklungsstand kann bei dem Einsatz von KI-Systemen und KI-Modellen nicht ausgeschlossen werden, dass unrichtige Daten über natürliche Personen ausgegeben werden (sog. Halluzinationen). Ebenso besteht die Möglichkeit, dass personenbezogene Daten (versehentlich) unrichtig eingegeben werden oder unrichtig werden.

Grundsätzlich sieht die DSGVO, die bei der Datenverarbeitung mittels KI-Systemen oder -Modellen uneingeschränkt Anwendung findet, in Fällen der Verarbeitung von unrichtigen personenbezogenen Daten einen Berichtigungsanspruch nach Artikel 16 DSGVO vor.

Nach dem Stand der Technik können Wahrscheinlichkeitsparameter, die als personenbezogene Daten gedeutet werden könnten, ob unrichtig oder rechtmäßig

gespeichert, sehr schwierig oder gar nicht aus den KI-Modellen entfernt oder berichtigt werden.

In dieser Lage könnten die KI-Modelle, um dem Berichtigungs- oder Löschungsanspruch zu entsprechen, nur verworfen werden. Dies würde letztlich dazu führen, dass die öffentliche Verwaltung derzeit und auf unbestimmte Zeit dieses KI-Modell nicht einsetzen kann. Auf der anderen Seite ist die Anwendung von KI in der öffentlichen Verwaltung unverzichtbar, um effizient, in der gebotenen Qualität und ressourcenschonend die gesetzlichen Aufgaben zu erfüllen. Gemäß Artikel 23 Absatz 1 Buchst. e DSGVO erlaubt die Abwägung des Interesses des Einzelnen an der Wahrnehmung seiner Betroffenenrechte mit dem erheblichen öffentlichen Interesse am Einsatz von KI, die Betroffenenrechte – hier das Recht auf Berichtigung und Löschung – zu beschränken.

Die Beschränkung darf nur in verhältnismäßigem Umfang erfolgen, also nur, soweit die Erfüllung des Anspruchs auf Berichtigung oder Löschung unverhältnismäßigen Aufwand erfordern würde. Desgleichen müssen alle zur Verfügung stehenden technischen Maßnahmen genutzt werden, um die Betroffenenrechte zu erfüllen. Nach derzeitigem Stand kommen hierfür insbesondere Filter in Betracht.

Unbeeinträchtigt bleibt das Recht nach Artikel 16 Satz 2 DSGVO, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. Ebenso wenig kann eine Entscheidung gegenüber der betroffenen Person auf eine unrichtige Eingabe oder Ausgabe gestützt werden.

Zu Nummer 11 (§ 10 Absatz 4 neu)

Ein Löschungsanspruch entsteht in den in Artikel 17 DSGVO genannten Fällen, insbesondere, wenn die Speicherung zur Aufgabenerfüllung nicht mehr erforderlich ist oder die betroffene Person ihre Einwilligung widerrufen oder Widerspruch eingelegt hat. Auch hier soll die Speicherbegrenzung nicht regelmäßig dazu führen, dass KI-Systeme nicht mehr einsetzbar sind. Denn ein KI-Modell von Grund auf neu zu trainieren, ist extrem teuer und zeitaufwändig Da die praktische Umsetzung des Löschungsanspruchs auf vergleichbare Schwierigkeiten wie beim Berichtigungsanspruch stößt, wird der Löschungsanspruch entsprechend der Beschränkung beim Berichtigungsanspruch behandelt, nämlich auf Maßnahmen reduziert, die mit verhältnismäßigem Aufwand machbar sind. Hierzu kann ein Filter

dienen, der die Antwort des KI-Modells in Bezug auf bestimmte personenbezogene Daten filtert, so dass diese nicht ausgegeben werden

Zu Nummer 12 (§ 11a neu – 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 sind in der KI-VO sehr detaillierte Rahmenbedingungen enthalten. Öffentliche Stellen sind „Akteure“ im Sinne des Artikels 3 Nummer 8 der KI-VO. Sie dürfen also KI-Systeme insbesondere in eigener Verantwortung im Rahmen ihrer Tätigkeit verwenden (Betreiber im Sinne des Artikels 3 Nummer 4 der KI-VO) und KI-Systeme oder ein KI-Modell mit allgemeinem Verwendungszweck entwickeln oder entwickeln lassen und in den Verkehr bringen oder in Betrieb nehmen (Anbieter im Sinne des Artikel 3 Nummer 3 der KI-VO). Der Einsatz ist auf die Wahrnehmung der öffentlich-rechtlichen Verwaltungstätigkeit begrenzt und setzt die Einhaltung der maßgeblichen Rechtsvorschriften voraus.

Bei dem Einsatz von KI-Systemen ist folgendes zu beachten:

- Der Einsatz von KI-Systemen muss in einer transparenten und nachvollziehbaren Weise erfolgen.

- Der Einsatz hat stets den rechtlichen Anforderungen an Datenschutz und Diskriminierungsfreiheit zu genügen.

- KI-gestützte Verwaltungsverfahren müssen den Anforderungen an das Rechtsstaatsprinzip und der gerichtlichen Nachprüfbarkeit sowie den gesetzlichen und politischen Vorgaben des Landes Baden-Württemberg sowie der EU entsprechen.

- Die öffentliche Stelle muss dafür Sorge tragen, dass die eingesetzten KI-Systeme innerhalb vorgegebener Parameter arbeiten und den jeweils geltenden rechtlichen und technischen Anforderungen entsprechen.

Diese Anforderungen müssen sowohl bei der Entwicklung als auch während des gesamten Betriebs laufend sichergestellt werden. Dies gilt insbesondere bei Änderungen in der Rechtsetzung oder Rechtsprechung.

Durch dieses Gesetz wird keine abweichende Festlegung von Verantwortlichkeiten getroffen. Diese ergeben sich kontextbezogen aus den jeweils anwendbaren Rechtsvorschriften.

Von wenigen Ausnahmen abgesehen (insbesondere Artikel 10 Absatz 5 und Artikel 59 der KI-VO) enthält die KI-VO keine Vorgaben zur Verarbeitung von personenbezogenen Daten. § 11a schafft für die Entwicklung und das Training sowie weitere benannte Verarbeitungsschritte, die der KI-Einsatz erfordert, eine Rechtsgrundlage.

Bevor KI-Systeme in einer öffentlichen Stelle genutzt werden können, müssen sie für ihre Aufgabe im Rahmen der Entwicklung trainiert werden. Für Weiterentwicklungen bereits in Nutzung befindlicher KI-Systeme gilt dies entsprechend. Der Begriff des Trainings ist folglich umfassend gemeint und schließt sämtliche Trainingsformen mit ein, sowohl bei der Entwicklung und Initialisierung von KI-Systemen als auch bei der Nutzung und im Rahmen der Anpassung und Verbesserung bestehender KI-Systeme. Im Rahmen des Trainings kommen Trainings-, Validierungs- und Testdatensätze im Sinne der KI-VO zum Einsatz.

Die Verwendung von Datensätzen, die ausschließlich anonyme Daten enthalten, wird im LDSG nicht geregelt. Sie bedarf keiner datenschutzrechtlichen Erlaubnis. Soweit ein Datensatz personenbezogene Daten im Sinne von Artikel 4 Nummer 1 DSGVO enthält, schafft § 11a eine Rechtsgrundlage für deren Verarbeitung im Sinne von Artikel 4 Nummer 2 DSGVO nach Maßgabe des Artikels 6 Absatz 1 in Verbindung mit Absatz 3 Buchst. b DSGVO zum Zweck des Trainings von KI-Systemen.

Das Training von KI-Systemen mit personenbezogenen Daten hat dem Grundsatz der Datenminimierung entsprechend nach einem abgestuften Konzept zu erfolgen. Vorrangig sind nicht personenbezogene Daten für das Training zu verwenden. Soweit die für das Training verwendeten Daten personenbezogen sind, sind sie grundsätzlich zu anonymisieren (vgl. § 4 Absatz 2 neu). Ist das Training mit nicht personenbezogenen Daten nicht zweckmäßig oder die Anonymisierung mit unverhältnismäßigem Aufwand verbunden, sind die personenbezogenen Daten vor dem Training grundsätzlich zu pseudonymisieren. Pseudonymisierung ist nach Artikel 4 Nummer 5 DSGVO die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Sicherungsmaßnahmen unterliegen, die

gewährleisten, dass diese personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person wieder zugewiesen werden können. Ist das Training mit pseudonymisierten Daten wiederum nicht zweckmäßig oder der Aufwand der Pseudonymisierung unverhältnismäßig, dürfen die personenbezogenen Daten ohne vorherige Anonymisierung und Pseudonymisierung für das Training verarbeitet werden.

Der Trainingszweck wird nicht erreicht, wenn die beabsichtigte Art und Qualität der Ergebnisse, die durch das KI-System erzeugt werden, mit anonymen oder pseudonymen Daten nicht herbeigeführt werden kann.

Für die Entwicklung, das Training, Testen und die Validierung von KI-Systemen und Modellen stehen nach Artikel 57 ff. KI-VO die KI-Reallabore als Möglichkeit zur Verfügung, um in einer kontrollierten Umgebung die genannten Verfahrensschritte zu erleichtern. Daneben können sich insbesondere in der Justiz auch andere Verfahren zur Erprobung anbieten. Entscheidend für die datenschutzrechtliche Zulässigkeit ist die Einhaltung der datenschutzrechtlichen Grundsätze und ausreichender technischer und organisatorischer Maßnahmen.

Zu Nummer 13 (§ 12a neu – Verarbeitung zu Zwecken der parlamentarischen Kontrolle)

Für die Verarbeitung personenbezogener Daten zu Zwecken parlamentarischer Kontrolle wird zur Klarstellung eine Rechtsvorschrift in das LDSG eingefügt. Die Rechtsgrundsätze leiten sich primär aus der Landesverfassung ab. Die Landesregierung ist den Landtagsabgeordneten gegenüber auskunftspflichtig. Damit kann auch die Übermittlung personenbezogener Daten im Raum stehen, insbesondere bei der Beantwortung von Anfragen und Anträgen.

In diesen Fällen steht die Landesregierung vor der Aufgabe, das parlamentarische Fragerecht mit dem aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundrecht auf informationelle Selbstbestimmung in Einklang zu bringen. Denn der Informationsanspruch der einzelnen Abgeordneten besteht nicht grenzenlos. Das Fragerecht der Abgeordneten und die Antwortpflicht der Regierung können dadurch begrenzt sein, dass diese gemäß Artikel 2 Absatz 1 der Landesverfassung und Artikel 1 Absatz 3 des Grundgesetzes Grundrechte zu beachten haben. Hierzu zählt nach der Rechtsprechung des Bundesverfassungsgerichts im sogenannten Volkszählungsurteil das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Grundrecht auf informationelle Selbstbestimmung. Das Grundrecht gewährleistet die

Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und damit Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der auf ihn bezogenen, individualisierten oder individualisierbaren Daten.

Entsprechend den anerkannten Regeln bei der Kollision verfassungsrechtlich begründeter Rechtspositionen ist jeweils eine Abwägung anhand sämtlicher Umstände des Einzelfalls unter Berücksichtigung des Grundsatzes der praktischen Konkordanz vorzunehmen. Die widerstreitenden verfassungsrechtlichen Positionen sind demnach in einen schonenden und zugleich wirksamen Ausgleich zu bringen. Die Grundsätze dieser Abwägung können abstrakt-generell durch den Landesgesetzgeber vorgegeben werden.

Für streng persönliche Informationen, deren Preisgabe für die Betroffenen unzumutbar ist, wird ein absoluter Schutz angeordnet, ebenso, wenn der Eingriff in das informationelle Selbstbestimmungsrecht unverhältnismäßig ist. In beiden Fällen kommt die Vorlage an den Landtag nur unter besonderen datenschutzrechtlichen Vorkehrungen in Betracht, die eine Identifizierbarkeit der betroffenen Personen wirksam ausschließen. Dies wird regelmäßig eine anonymisierende Bearbeitung voraussetzen; in bestimmten Ausnahmefällen kann auch eine Pseudonymisierung der vorzulegenden Akten geboten sein, insbesondere, wenn ansonsten die Akten gänzlich unverständlich und hinsichtlich des Untersuchungsziels von vornherein unergiebig blieben.

Die gesetzliche Regelung orientiert sich an der verfassungsgerichtlichen Rechtsprechung des Verfassungsgerichtshofs für das Land Nordrhein-Westfalen vom 20. April 2021, Az.: VerfGH 177/20, https://openjur.de/u/2337610.html).

Zu beachten ist, dass spezielle Übermittlungsvorschriften dieser Regelung vorgehen, so beispielsweise die Regelungen des Sozialdatenschutzes (vgl. § 67b Zehntes Buch Sozialgesetzbuch - SGB X), die Regelungen zur Übermittlung nach dem Beamtenrecht (vgl. § 85 Landesbeamtengesetz - LBG) oder dem Verfassungsschutzrecht (vgl. §§ 10, 11 Landesverfassungsschutzgesetz - LVSG).

Zu Nummer 14 (§ 13 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken)

Zu Buchstabe a (Absatz 1)

Zu Buchstabe aa (Satz 1)

Zu Buchstabe aaa

Mit der eingefügten Erlaubnis zur zweckändernden Weiterverarbeitung vorhandener Daten zu Forschungs- oder Statistikzwecken (retrospektive Nutzung) wird der in der DSGVO angelegten Privilegierung der Forschung, wonach unter Einhaltung von Garantien für die Rechte und Freiheiten der betroffenen Personen die Weiterverarbeitung personenbezogener Daten für die Forschung zulässig ist, ausdrücklich Rechnung getragen. Dies gilt auch für die zweckändernde Weiterverarbeitung besonderer Kategorien personenbezogener Daten. Forschung ist, um valide Ergebnisse zu erzielen, auf die Verarbeitung großer Mengen von Daten angewiesen. Nicht immer können die personenbezogenen Daten anonymisiert werden. Solange die Daten zu Dokumentationszwecken für den ursprünglichen Erhebungszweck dokumentiert werden müssen, ist für die Weiterverwendung zu Forschungszwecken nur die Pseudonymisierung möglich. Die Daten bleiben damit personenbezogen. Öffentliche Stellen, die, wie von § 13 vorausgesetzt, gemeinwohlorientierte Forschung betreiben, bedürfen einer rechtssicheren Rechtsgrundlage, um personenbezogene Daten auch ohne Einwilligung weiterzuverarbeiten. Dementsprechend ist vom Anwendungsbereich des § 13 insbesondere die Verarbeitung von Gesundheitsdaten auf Grund des Vorrangs des Gesetzes zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz - GDNG) sowie des Landeskrankenhausgesetzes Baden-Württemberg (LKHG) für die von diesen Gesetzen erfassten Stellen ausgenommen. Der Vorrang fachspezifischer Gesetze ergibt sich im Übrigen aus § 2 Absatz 3 LDSG.

Die Regelung erfüllt die Voraussetzungen einer Rechtsgrundlage nach Artikel 6 Absatz 4 Halbsatz 1 in Verbindung mit Artikel 23 Absatz 1 der Verordnung (EU) 2016/679.

Absatz 1 erlaubt auch die Forschung mit Kooperationspartnern in gemeinsamer Verantwortung unter den genannten Voraussetzungen. Die Übermittlung an Dritte für deren eigene Forschungsvorhaben ist in Absatz 4 geregelt.

Zu Buchstabe bbb

In der Evaluierung wurde festgestellt, dass die Formulierung in Satz 1 des Absatz 1 der Zulässigkeit der Verarbeitung personenbezogener Daten, „wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können“ zum Missverständnis in der Praxis dergestalt geführt hat, dass ein Vorrang der Einwilligung als Grundlage für die Datenverarbeitung angenommen wurde. Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 DSGVO stehen gleichberechtigt nebeneinander; die einwilligungsbasierte Verarbeitung hat keinen Vorrang vor der auf gesetzlicher Grundlage beruhenden Verarbeitung.

Zur Klarstellung werden daher in Satz 1 die genannten Wörter ersetzt und stattdessen die Erforderlichkeit zum Maßstab für die Zulässigkeit eingeführt. Dies entspricht auch der von der DSGVO verwendeten Terminologie in Artikel 9 Absatz 2 Buchst. j DSGVO. Inhaltlich ist weiterhin zu prüfen, ob der Zweck mit weniger eingriffsintensiven Mitteln, insbesondere mit anonymisierten oder, falls dies nicht möglich ist, mit pseudonymisierten Daten, erreicht werden kann. Unterbleiben kann die Anonymisierung oder ersatzweise die Pseudonymisierung nur, wenn sie nicht möglich oder im Einzelfall unverhältnismäßig ist.

Zu Buchstabe bb

Einer landesgesetzlichen Regelung zur Bestimmung des Begriffs der besonderen Kategorien personenbezogener Daten bedarf es nicht. Die Begriffsbestimmungen sind, wie in § 2a Absatz bestimmt, der DSGVO zu entnehmen. Die besonderen Kategorien personenbezogener Daten werden in Artikel 9 Absatz 1 DSGVO definiert.

Zu Buchstabe b (Absatz 2 neu)

Die (Weiter)Verarbeitung allgemein zugänglicher Daten, z. B. bereits veröffentlichter Daten, wird für wissenschaftliche Forschungszwecke zugelassen. Ein Grund hiervon abzuweichen, besteht nur dann, wenn schutzwürdige Belange der betroffenen Person entgegenstehen, z. B. bei rechtswidrig erlangten, kompromittierenden Daten, Vorliegen eines Widerspruchs oder Daten, die unrechtmäßig veröffentlicht wurden. Die Informationspflicht kann unter den Voraussetzungen des Artikels 14 Absatz 5 Buchst. b DSGVO und § 8 entfallen.

Die Verarbeitung allgemein zugänglicher Daten kann die Entwicklung von KI-Anwendungen in der Forschung unterstützen. Für besondere Kategorien personenbezogener Daten gilt diesbezüglich Artikel 9 Absatz 2 Buchst. e DSGVO.

Zu Buchstabe c

Redaktionelle Folgeänderung zu Buchstabe b.

Zu Buchstabe d (Absatz 3 Satz 2 neu)

Die öffentliche Stelle muss gemäß Artikel 89 Absatz 1 DSGVO geeignete Garantien für die Rechte und Freiheiten der betroffenen Person treffen. Neben den in Absatz 3 genannten Maßnahmen der Anonymisierung und Pseudonymisierung sind insbesondere Maßnahmen zu treffen, um sicherzustellen, dass die in Artikel 5 DSGVO dargelegten Grundsätze der Verarbeitung personenbezogener Daten eingehalten werden. Zu verweisen ist insbesondere auf die Grundsätze der Datenminimierung, der Richtigkeit sowie der Vertraulichkeit und Integrität von Daten. Beispiele zur Umsetzung dieser Grundsätze mittels technischer und organisatorischer Maßnahmen sind insbesondere § 3 zu entnehmen, der Artikel 32 Absatz 1 DSGVO konkretisiert; insbesondere ist an Verschlüsselung oder Zugangs- und Zutrittsbeschränkungen (z. B. Multi-Faktor-Authentisierung) sowie ein Rechte- und Rollenkonzept zu denken. Die Höhe der Schutzmaßnahmen muss der Schutzbedürftigkeit der personenbezogenen Daten entsprechen; im allgemeinen Datenschutzrecht ist daher die Festlegung spezifischer Maßnahmen nicht angezeigt. Die Maßnahmen sind in einem Datenschutzkonzept niederzulegen; der Datenschutzbeauftragte der öffentlichen Stelle ist zu beteiligen (vgl. Artikel 38 Absatz 1 DSGVO).

Zu Buchstabe e

Der bisherige Absatz 3 wird Absatz 4.

Zu Buchstabe f (Absatz 5 neu)

Die DSGVO versteht den Begriff der wissenschaftlichen Forschung grundsätzlich weit: Neben Grundlagenforschung können auch die angewandte Forschung und die privat finanzierte Forschung eingeschlossen werden (vgl. Erwägungsgrund 159). Entscheidend für die Privilegierung der Forschung öffentlicher Stellen ist deren Verpflichtung auf das Gemeinwohl. Soweit privat finanzierte Forschung sich ebenfalls dem Gemeinwohl verpflichtet, wird die Übermittlung personenbezogener Daten zu Forschungszwecken legitimiert. Das Gemeinwohl wird in § 5 Absatz 1 Nummer 1 definiert. Die Regelung ermöglicht auch Verbundforschung mit privat finanzierter Forschung.

Die Weitergabe personenbezogener Daten für Forschungszwecke setzt gemäß Artikel 89 Absatz 1 DSGVO Garantien zugunsten der betroffenen Personen voraus. Hierzu ist der Empfänger von der übermittelnden öffentlichen Stelle zu verpflichten. Dementsprechend muss der Empfänger die Daten anonymisieren, sobald der Personenbezug nicht mehr erforderlich ist. Weitere Schutzmaßnahmen sind entsprechend ihrer Erforderlichkeit nach Artikel 25, 32 DSGVO zu treffen. Zur Konkretisierung wird die Einhaltung der Maßnahmen nach § 3 vorgeschrieben. Dies schließt die Pflicht zur Geheimhaltung ein. Die Daten dürfen außerdem nicht an Dritte weitergegeben werden. Daneben sind die Pflichten der DSGVO zu beachten, wie etwa die Beteiligung der oder des Datenschutzbeauftragten nach Artikel 38 DSGVO oder eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO. Die öffentliche Stelle prüft vor der Übermittlung, ob ausreichende Garantien beim Empfänger getroffen wurden. Sie muss jederzeit Auskunft über den Umgang mit den übermittelten personenbezogenen Daten verlangen können.

Auf der Grundlage von Artikel 9 Absatz 2 Buchst. j DSGVO ist auch die Übermittlung besonderer Kategorien personenbezogener Daten für Forschungszwecke zulässig.

Sofern spezielle Übermittlungsregelungen bestehen, gehen diese als Lex Specialis den allgemeinen Regelungen des § 13 LDSG vor. Dies betrifft insbesondere im Hinblick auf Geheimhaltungspflichten für statistische Daten die Regelung in § 16 Absatz 6, 10 des Bundesstatistikgesetzes oder zur Übermittlung von Sozialdaten für die Forschung und Planung die spezielle Vorschrift des § 75 des Zehnten Buches Sozialgesetzbuch (SGB X) oder zur Forschung mit Patienten die spezielle Regelung im Landeskrankenhausgesetz (LKHG).

Zu Buchstabe g

Redaktionelle Folgeänderung zu Buchstabe f.

Zu Nummer 15 (§ 15 – Datenverarbeitung bei Dienst- und Arbeitsverhältnissen)

Zu Buchstabe a (§ 15 Absatz 2)

Entsprechend dem Ergebnis der Evaluierung werden die Zwecke der Verarbeitung besonderer Kategorien personenbezogener Daten erweitert für die in Artikel 9 Absatz 2 Buchst. h DSGVO genannten Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin und der Beurteilung der Arbeitsfähigkeit der Beschäftigten, sofern die Verarbeitung auf einer rechtlichen Grundlage erfolgt.

Als rechtliche Grundlage für Maßnahmen zur Gesundheitsvorsorge kann auf die Dienstpflichten des Dienstherrn, die aus der Fürsorgepflicht folgen, verwiesen werden. Für Maßnahmen zur Aufrechterhaltung der körperlichen und psychischen Gesundheit der Beschäftigten kann es erforderlich sein, besondere Kategorien personenbezogener Daten, vor allem Gesundheitsdaten, zu erheben. Für sonstige personenbezogene Daten findet § 15 Absatz 1 Anwendung, da die Verarbeitung personenbezogener Daten zu den in Absatz 2 genannten Zwecken auch der Durchführung des jeweiligen Dienst- oder Arbeitsverhältnisses dient.

Für die Personalverwaltungen kann diese Vorschrift nur zur Anwendung kommen, wenn die Verarbeitung durch ein einem Berufsgeheimnis unterliegendes Fachpersonal (z. B. Ärzte) oder durch Personen erfolgt, die ebenfalls einer Geheimhaltungspflicht unterliegen oder wenn die Verarbeitung unter deren Verantwortung erfolgt. Gemäß § 203 Absatz 2 StGB sind Amtsträger, für den öffentlichen Dienst besonders Verpflichtete sowie Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen, sofern ihnen ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis anvertraut wurde, ebenso wie das genannte Fachpersonal als Geheimnisträger verpflichtet.

Sofern es an einer rechtlichen Grundlage zur Durchführung von Maßnahmen zu den genannten Zwecken fehlt, kann die Verarbeitung der besonderen Kategorien personenbezogener Daten nur aufgrund einer ausdrücklichen Einwilligung erfolgen.

Zu Buchstabe b (§ 15 Absatz 6)

Absatz 6 wird zur Vermeidung von Missverständnissen klarer gefasst. Es wird ferner klargestellt, dass die erfassten Daten nur für die in Satz 1 genannten Zwecke verarbeitet werden dürfen. Darüber hinaus ergibt sich aus Artikel 25 DSGVO in Verbindung mit § 3 LDSG, dass dem Schutzbedürfnis der Daten entsprechende technische und organisatorische Maßnahmen zu treffen sind. Insbesondere ist dafür zu sorgen, dass die biometrischen Daten nicht für andere Zwecke ausgelesen werden können.

Zu Buchstabe c (§ 15 Absatz 9 neu)

Die Nutzung von KI bei der Verarbeitung personenbezogener Daten in Dienst- und Arbeitsverhältnissen kann sowohl die Einstellung und Auswahl von Personen als auch die Durchführung oder Beendigung bestehender Beschäftigungsverhältnisse

betreffen. Erwähnt seien Lebenslauf-Parsing, Online-Assessments, mittels derer eine Auswahl unter Bewerberinnen und Bewerbern getroffen wird. Diese Nutzung von KI bringt spezifische Gefahren mit sich, indem statt von einem Menschen von einer Maschine aufgrund eines Algorithmus Festlegungen getroffen werden, die zum Nachteil einer bestimmten Person ausfallen können und sich auf Entscheidungen auswirken.

Dementsprechend gehören KI-Systeme, die für Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit eingesetzt werden, nach Artikel 6 Absatz 2 KI-VO in Verbindung mit Nummer 4 des Anhangs III zur KI-VO zu den Hochrisiko-Systemen. Eine Ausnahme besteht nach Artikel 6 Absatz 3 KI-VO lediglich, wenn das KI-System kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, so z. B bei ausschließlich vorbereitenden Aufgaben. Die Einstufung als nicht hochriskant ist im Beschäftigtenkontext wegen des bestehenden Abhängigkeitsverhältnisses nur in Ausnahmefällen anzunehmen.

Für Hochrisiko-Systeme sieht die KI ein Risikomanagementsystem vor, mit dem den wesentlichen Risiken begegnet werden muss (vgl. Artikel 9 KI-VO). Als Risiko gelten Gefahren für die Grundrechte betroffener Personen, im Besonderen die Gefahr von Diskriminierung.

Entsprechend Artikel 88 Absatz 2 DSGVO ist für Regelungen im Beschäftigtenverhältnis insbesondere für Transparenz zu sorgen. Ergänzend zu den Informationspflichten nach der KI-VO und der DSGVO wird daher als gesetzliche Pflicht konstituiert, die Beschäftigten sowie die Bewerberinnen und Bewerber über den Einsatz von KI-Systemen, ihre Dauer und ihre Zwecke zu unterrichten.

Artikel 22 DSGVO verbietet öffentlichen Stellen unabhängig von der KI-VO, einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Artikel 22 DSGVO gilt für die Anwendung von KI im Beschäftigtenverhältnis uneingeschränkt. Die Regelungen der KI-VO stellen keine Ausnahmeregelung im Sinne des Artikels 22 Absatz 2 Buchst. b DSGVO dar. Dies verbietet, dass Personalentscheidungen ausschließlich durch KI getroffen werden ebenso wie Profiling. Letzteres wird in Artikel 4 Nummer 4 DSGVO definiert als automatisierte Verarbeitung personenbezogener Daten, die persönliche Aspekte bewertet,

insbesondere indem sie die Arbeitsleistung, die Gesundheit, die Interessen, Zuverlässigkeit oder Verhalten analysiert und vorhersagt. Es ist zu verlangen, dass ein überprüfender Mensch einen Entscheidungsspielraum haben muss, die Computer-Entscheidung zu ändern (vgl. BeckOK DatenschutzR/von Lewinski, 49. Ed. 1.8.2024, DS-GVO Art. 22 Rn. 23-25.2).

Zu Nummer 16 (§ 16 – Öffentliche Auszeichnungen und Ehrungen)

In Ergänzung zur bisherigen Regelung der Entscheidung über öffentliche Auszeichnungen und Ehrungen wird klargestellt, dass ein bekannter Widerspruch der betroffenen Person eine entsprechende Datenverarbeitung verbietet. Dies gebietet es nicht, dass die öffentliche Stelle vorher entsprechende Erkundigungen einholt. Es ist wie bisher nicht erforderlich, dass die betroffene Person zustimmt.

Zu Nummer 17 (§ 17 – Verarbeitung personenbezogener Daten im öffentlichen Interesse)

§ 17 regelt als besondere Verarbeitungssituation die Verarbeitung personenbezogener Daten im öffentlichen Interesse. In Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten beruht sie auf Artikel 9 Absatz 2 Buchst. g DSGVO, der unter den dort genannten Voraussetzungen die Mitgliedstaaten legitimiert, die Verarbeitung besonderer Kategorien personenbezogener Daten aus Gründen eines erheblichen öffentlichen Interesses zuzulassen.

Gemäß Artikel 9 Absatz 2 Buchst. g DSGVO verlangt die Verarbeitung besonderer Kategorien personenbezogener Daten im erheblichen öffentlichen Interesse eine gesetzliche Regelung, die den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsieht. Es werden daher explizit bestimmte, in § 3 genannte Maßnahmen vorgeschrieben, die auf jeden Fall getroffen werden müssen. Es ist daher entsprechend § 3 Nummern 1 bis 3 Folgendes sicherzustellen:

- Protokollierungsmaßnahmen müssen sicherstellen, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten verarbeitet worden sind;

- der Zugang zu den personenbezogenen Daten ist innerhalb der öffentlichen Stelle soweit wie möglich zu beschränken;

- die an den Verarbeitungsvorgängen beteiligten Personen, also diejenigen, welche Zugang zu den personenbezogenen Daten haben, sind zu sensibilisieren und zu schulen.

Im Übrigen sind, sofern nicht bereits standardmäßig eingeführt und soweit erforderlich, ergänzend die übrigen in § 3 Satz 3 genannten Maßnahmen zu prüfen und zu treffen.

Zu Nummer 18 (§§ 17a, 17b neu)

Zu § 17a – Absicherung des Zugangs zu personenbezogenen Daten

Für die spezifische Verarbeitung personenbezogener Daten im Rahmen von Maßnahmen zum Schutz der Informations- und Cybersicherheit wird eine eigene Ermächtigungsgrundlage geschaffen und zusammen mit dem bisherigen § 17 Absatz 1 LDSG in einer Norm zusammengefasst.

Zu Absatz 1

Absatz 1 entspricht unverändert § 17 Absatz 1 LDSG alter Fassung.

Zu Absatz 2

Als Ergebnis der Evaluierung wurde der Bedarf erkannt, personenbezogene Daten für Maßnahmen zu verarbeiten, die zur Gewährleistung der Informationssicherheit, der Cybersicherheit oder des Funktionierens kritischer Infrastruktur erforderlich sind, wenn außenstehende Personen Zugang zu den relevanten Anlagen haben. Neben der Verarbeitung zu Authentifizierungszwecken kann es beispielsweise für ein Sicherheitsaudit, für Schulungs- oder Sensibilisierungsmaßnahmen erforderlich sein, personenbezogene Daten der genannten Personen zu verarbeiten, insbesondere zu erheben oder zu übermitteln. Die Informationssicherheit ist in § 2 Absatz 9 Cybersicherheitsgesetz (CSG) definiert; sie umfasst alle technischen und nichttechnischen Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Cybersicherheit umfasst nach § 2 Absatz 11 CSG alle Aspekte der Sicherheit in der Informationstechnik und den Schutz gesellschaftlich relevanter Prozesse vor Angriffen im gesamten Cyberraum.

Entsprechend der Regelung für Beschäftigte wird die Verarbeitung biometrischer Daten für Authentifizierungs- und Autorisierungszwecke geregelt: Sie ist im Hinblick

auf die erhöhten Gefahren, die von der Verarbeitung biometrischer Daten ausgehen, nur mit ausdrücklicher Zustimmung der betroffenen Person und als Ultima Ratio zulässig. Denn im Gegensatz zu Kennwörtern können biometrische Daten nicht zurückgesetzt werden, bieten aber andererseits einen höheren Schutz vor unbefugtem Zugang als jene.

Der Unterschied zu Absatz 1 besteht in der Anwendung auf Personen, die bereits (physischen) Zugang zu den genannten Datenverarbeitungsanlagen haben und der engeren Zweckbestimmung. Die Verarbeitung besonderer Kategorien personenbezogener Daten wird in der Regel nicht erforderlich sein; ansonsten ist sie ggf. auf § 17 zu stützen oder es ist eine Einwilligung einzuholen.

Für Beschäftigte kommt § 15 zur Anwendung, da diese nicht Dritte sind. In Bezug auf Videoüberwachung ist gegebenenfalls § 18a zusätzlich anzuwenden.

Zu § 17b – Öffentlichkeitsarbeit

Zu Absatz 1

Öffentliche Stellen benötigen rechtssichere Grundlagen für die Öffentlichkeitsarbeit. Kaum eine öffentliche Stelle kommt mehr ohne öffentlichen Auftritt aus, sei es mittels Informationsveranstaltungen, Informationsbroschüren oder in sozialen Medien. Regelmäßig werden hierfür personenbezogene Daten benötigt. Bisher wird für die datenschutzrechtliche Legitimation die Generalklausel des § 4 LDSG bemüht. Diese vermag aber keine Auskunft darüber zu geben, welche Art der Öffentlichkeitsarbeit zulässig ist. Deshalb soll in der Praxis mit § 17a mehr Sicherheit gegeben werden bezüglich dessen, was zu welchem Zweck zulässig ist. Es ist jedenfalls zu beachten, dass auch im Rahmen der Öffentlichkeitsarbeit alle datenschutzrechtlichen Grundsätze, insbesondere die aus Artikel 5 DSGVO, gelten.

Grundsätzlich ist die Öffentlichkeitsarbeit durch einen verfassungsrechtlichen oder gesetzlichen Auftrag zur politischen Bildung, zur Information der Bürgerinnen und Bürger verfassungsrechtlich gerechtfertigt und sorgt für Transparenz staatlichen Handelns für die Zivilgesellschaft. Dabei wird von einer objektiv gehaltenen Information der Öffentlichkeit ausgegangen. Dieser verfassungsrechtliche Auftrag ist in Einklang zu bringen mit dem informationellen Selbstbestimmungsrecht des Einzelnen, selbst über die Verwendung seiner Daten zu bestimmen. Die jeweilige Schutzbedürftigkeit der Adressatengruppe ist zu berücksichtigen; dies erfordert insbesondere im Hinblick auf Minderjährige besondere Prüfpflichten.

Mit der gesetzlichen Regelung wird die Eingriffsschwelle bestimmt, ab der zur Verarbeitung personenbezogener Daten die Einwilligung der betroffenen Person erforderlich ist. Hierbei wird in Bezug auf die Angemessenheit auch berücksichtigt, was vernünftigerweise von Personen, die öffentliche Dienste in Anspruch nehmen oder sich in öffentlichen Kanälen informieren, erwartet wird und deshalb davon auszugehen ist, dass voraussichtlich keine Einwendungen gegen die Verarbeitung bestehen. Vorausgesetzt wird, dass nur Mittel eingesetzt werden, die zum Zweck der Öffentlichkeitsarbeit erforderlich sind, das heißt nur in erforderlichem Umfang von der Ermächtigung Gebrauch gemacht wird. Legitimer werblicher Zweck kann die Nachwuchswerbung öffentlicher Stellen sein.

Zu den in der Regel legitimen Mitteln der Öffentlichkeitsarbeit gehören und werden explizit ohne Anspruch auf Vollständigkeit aufgezählt: die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen (z. B. Streaming) und deren Verbreitung, die Verwendung von Kontakt- und Adressdaten für Kontaktpflege und Einladungen zu Veranstaltungen einschließlich deren Organisation. Die Zusendung von Newslettern gehört nicht zur Kontaktpflege und bedarf der Einwilligung.

Die Zulassung der Verarbeitung personenbezogener Daten zum Zweck der Öffentlichkeitsarbeit erfolgt unbeschadet sonstiger Bestimmungen. Daher sind zumindest die Schranken der Fertigung von Bild, Film- und Tonaufnahmen während Veranstaltungen (Fotografie und Live-Streaming) und deren Verbreitung nach §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) zu beachten. Wegen der Strafbarkeit nach § 33 KunstUrhG erfolgt die Aufnahme in den Gesetzestext. Zu beachten ist insbesondere, dass Personen nur als Beiwerk erscheinen dürfen.

Die Nutzung sozialer Medien wird in Satz 2 nicht explizit erwähnt, da sie jeweils genauer Prüfung bedarf, ob ihr Einsatz nach Satz 1 gerechtfertigt ist. Die Nutzung sozialer Medien hat insbesondere die zu Facebook ergangene Rechtsprechung des Europäischen Gerichtshofs zu beachten. In einem richtungsweisenden Urteil hat der Europäische Gerichtshof im Jahr 2018 entschieden, dass Betreiber von Fanpages auf Facebook gemeinsam mit Facebook als Dienstanbieter für den Schutz der Nutzerdaten verantwortlich sind. Für die gemeinsame Verantwortlichkeit legt Artikel 26 DSGVO die zu beachtenden Pflichten fest.

Für sonstige soziale Medien sind ebenfalls die Voraussetzungen einer gemeinsamen Verantwortlichkeit nach Artikel 26 DSGVO zu prüfen. Die Prüfung der Tatbestandsvoraussetzungen des Artikels 26 DSGVO entscheidet darüber, ob eine

gemeinsame Verantwortlichkeit anzunehmen ist und wie weit diese reicht. Da die Voraussetzungen der Nutzung sozialer Medien von den Vorgaben der DSGVO bestimmt werden, muss eine Regelung zur Verantwortlichkeit im LDSG unterbleiben. Zur Orientierung kann die Broschüre des LfDI „Wesentliche Anforderungen an die behördliche Nutzung Sozialer Netzwerke“ dienen.

Zu Absatz 2

Zur Wahrung des Rechts auf Datenschutz ist den betroffenen Personen Gelegenheit zum Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten zu geben, und zwar ohne die Angabe von Gründen.

Zu Nummer 19 (§ 18 – Videoschutz öffentlich zugänglicher Räume)

Die Regelung zur Videoüberwachung dient dem Schutz von Personen und Objekten in öffentlich zugänglichen Räumen. Regelungsbedarf besteht aus den folgenden Gründen:

- Die Schutzbedürftigkeit des Objekts oder der Personen kann aufgrund der Gefahrenlage generell soweit gesteigert sein, dass außer Videoüberwachung keine vernünftige Alternative zur Verfügung steht. Dementsprechend soll die Anwendung der Videoüberwachung gesetzlich vereinfacht werden.

- Der Schutz von Personen im Bereich der geschützten Anlagen soll als besonders wichtiges öffentliches Interesse herausgestellt werden.

- Eine Verlängerung der maximalen Speicherfrist auf zwei Monate soll den verstärkten Schutz durch Videoüberwachung flankieren.

- Zur Überwachung des Eigentums öffentlicher Stellen, insbesondere solcher, die öffentliche Infrastruktur betreffen, kann auch die optisch-elektronische Überwachung unter Nutzung von KI-Systemen beitragen und sollte genutzt werden. Die Verarbeitung personenbezogener Daten bedarf, auch wenn sie ihrem Zweck nach nicht beabsichtigt ist, einer gesetzlichen Grundlage.

Zu Buchstabe a

Entsprechend der verstärkt herausgestellten Schutzfunktion der Videoüberwachung in Bezug auf Personen und Objekte wird in der Überschrift nunmehr von „Videoschutz“ gesprochen.

Zu Buchstabe b (Absatz 1 Sätze 2 und 3 neu)

Zu Satz 2

Nach Satz 1 ist die Abwägung mit den schutzwürdigen Interessen der betroffenen Personen für die Zulässigkeit der Videoüberwachung gefordert. Satz 2 soll klarstellen, dass der Schutz von Leben, Freiheit und Gesundheit von Personen, die sich im Bereich der nach Satz 1 geschützten Objekte aufhalten, für die Videoüberwachung ein besonders wichtiges öffentliches Interesse ist. Abzustellen ist jeweils auf den Zweck der Videoüberwachung. Gegebenenfalls kann die Abwägung auf der Grundlage dieser Regelung zugunsten der Videoüberwachung ausfallen.

Zu Satz 3

Grundsätzlich ist der Einsatz von Videoüberwachung nur zulässig, wenn kein milderes Mittel zur Verfügung steht, das mit geringerer Eingriffstiefe denselben Schutz gewährleistet. Wenn es sich um ein besonders schutzwürdiges Objekt handelt, wie sie sicherheitsrelevante Dienstgebäude (z. B. Polizeidienststellen) oder Einrichtungen (z. B. Mobile Wachen, Abschnittsbefehlsstellen in einer Großeinsatzlage der Polizei in einem nichtpolizeilichen Gebäude, ggf. Abstellflächen für Dienstfahrzeuge), Dienstfahrzeuge (zur Sicherung ihrer Einsatzbereitschaft), Kulturgüter (vgl. § 2 Absatz 1 Nr. 10 des Gesetzes zum Schutz von Kulturgut (Kulturgutschutzgesetz) oder öffentliche Verkehrsmittel (eine große Anzahl von Personen befindet sich auf engem Raum) darstellen, wird die genannte Abwägung regelmäßig zugunsten einer Videoüberwachung als geeignetstes Mittel ausfallen. Darüber hinaus entspricht es der Erwartung der Besucherinnen und Besucher der entsprechenden Örtlichkeiten, an den genannten Objekten eine Videoüberwachung vorzufinden. Damit einher geht dort eine gesteigerte Schutzbedürftigkeit, die durch Videoüberwachung besser gewährleistet werden kann. Es wird daher gesetzlich die Verhältnismäßigkeit im engeren Sinn, damit im Besonderen die Angemessenheit der Videoüberwachung als Mittel zum Schutz der genannten Objekte festgestellt. Dabei ist zu beachten, dass der Grundsatz der Datenminimierung eingehalten wird, also die Videoüberwachung so geringfügig wie möglich gehalten wird. Die weitere Voraussetzung, dass die Videoüberwachung erforderlich sein muss, also im Einzelfall eine konkrete oder abstrakte Gefahr vorliegen muss, damit eine

Videoüberwachung zulässig ist, wird damit nicht aufgehoben und entsprechend klargestellt.

Zu Buchstabe c (Absatz 2 neu)

Zugunsten der Transparenz von Videoüberwachung wird der Umfang der Informationspflicht im Überwachungsbereich konkretisiert. Der Umfang der Informationspflicht ergibt sich grundsätzlich aus Artikel 13 DSGVO. Mindestens die Kontaktdaten müssen erkennbar sein. Die weiteren Informationen, z. B. über den Zweck der Videoüberwachung und die Speicherdauer, kann die betroffene Person vom Verantwortlichen erhalten. Die Informationspflicht kann auch durch Anbringung eines QR-Codes mit Bereitstellung der Information an der angegebenen URL erfüllt werden. Eine Mustervorlage für ein Hinweisschild findet sich in der DIN 33450.

Zu Buchstabe d (Ergänzung Absatz 3)

Zur Klarstellung wird zur Kongruenz mit dem bisherigen Absatz 5 die Weiterverarbeitung zur Verfolgung von Rechtsansprüchen aufgenommen.

Zu Buchstabe e (Aufhebung des Absatz 4)

Die Vorschrift ist entbehrlich, da sie nur klarstellende Funktion hat. Absatz 4 wird daher aufgehoben. Die Informationspflicht wird durch die Maßnahmen nach Absatz 2 erfüllt.

Zu Buchstabe f

Redaktionelle Folgeänderung zu Buchstabe d.

Zu Buchstabe g

Die bisherige maximale Speicherdauer von vier Wochen wird entsprechend den Regelungen in Bayern, Rheinland-Pfalz und Sachsen auf zwei Monate ausgedehnt. Die maximale Speicherdauer soll im Spannungsverhältnis der präventiven Gefahrenabwehr beziehungsweise des staatlichen Interesses an Strafverfolgung und des grundrechtlich verbürgten Schutzes der betroffenen Personen, die keinen Anlass für die Videoüberwachung gegeben haben, die Grenze des verfassungsrechtlich Zulässigen gesetzlich regeln. Grundsätzlich verbleibt es bei der Pflicht, Videoaufzeichnungen zu löschen, sobald feststeht, dass diese für die aufgeführten

Zwecke nicht mehr benötigt werden. Für die Auswertung der Videoüberwachung im Hinblick auf relevante Vorkommnisse einschließlich des Geschehens davor und danach bedarf es aber einer ausreichenden maximalen Speicherdauer. Es sollte außerdem gewährleistet sein, dass im Fall von aufgezeichneten Tätlichkeiten (z. B. in öffentlichen Verkehrsmitteln) die Videoaufzeichnungen noch zur Verfügung stehen, wenn erst nach Ablauf von vier Wochen Anzeige erstattet wird. Dies gebietet der in Absatz 1 herausgestellte Schutz von Leben, Gesundheit und Freiheit der geschützten Personen. Ferner ist nach der Neuregelung in Absatz 1 Satz 2 und 3 zu erwarten, dass Videoüberwachung häufiger als präventives Mittel der Gefahrenabwehr eingesetzt werden wird und mehr strafrechtlich relevante Vorfälle erkannt werden, die zu bearbeiten sind. Eine sorgfältige Auswertung, für die qualifiziertes Fachpersonal erforderlich sein wird, kann diesbezüglich mehr als vier Wochen benötigen.

Durch eine längere Speicherfrist wird die Verhältnismäßigkeit der Datenspeicherung nicht in Frage gestellt, wenn dies im Einzelfall zur Auswertung der Videoaufzeichnungen zum Zweck der Strafverfolgung einschließlich der Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Geltendmachung von Rechtsansprüchen erforderlich ist und technisch-organisatorische Maßnahmen (wie z. B. Zugriffsbeschränkungen, sichere Speicherung) den Eingriff minimieren. Höchstspeicherdauer heißt aber auch weiterhin: Im konkreten Fall kann – und wird in der Regel – die rechtlich zulässige Frist der Speicherung deutlich kürzer sein. Werden die Videoaufzeichnungen durchgesehen und keine Vorkommnisse festgestellt, die für die genannten Zwecke der Gefahrenabwehr oder der Strafverfolgung relevant sind, so sind die Daten umgehend zu löschen.

Zu Buchstabe h (Absatz 6 neu)

Videoüberwachung kann auch nützlich sein, um den Erhaltungszustand und der Funktionsfähigkeit von Bauten, Anlagen u. ä. in öffentlicher Nutzung zu überwachen. Hierbei kommen zunehmend KI-Systeme zum Einsatz. Dabei ist die Verarbeitung personenbezogener Daten häufig unvermeidlich; sie ist aber nicht der Zweck der Videoüberwachung. Zu nennen sind hier exemplarisch die Pflege und Wartung öffentlicher Einrichtungen und Infrastruktur (z. B. Straßen, Brücken, Elektrizitätswerke, Wasserwerke) oder der Einsatz in der staatlichen oder kommunalen Bauwirtschaft, sofern diese öffentlich zugänglich sind. Die in Absatz 1 enthaltene Beschränkung auf öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen ist hier aufgehoben; es werden alle im Eigentum öffentlicher Stellen stehenden oder zu

öffentlichen Zwecken gewidmeten Gegenstände erfasst, also insbesondere auch Straßen.

Neben § 3a wird klarstellend auch die Nutzung von KI-Systemen zu dem genannten Zweck zugelassen, wenn damit die Verarbeitung personenbezogener Daten verbunden ist. Dies betrifft überwiegend Personen, die sich zufällig in den überwachten Räumen aufhalten, deren Identität aber wie bei der Videoüberwachung keine Rolle spielt.

Die Zulässigkeit beurteilt sich entsprechend der in Absatz 1 Satz 1 genannten Voraussetzungen, nämlich ob die Videoüberwachung verbunden mit der Nutzung von KI-Systemen zur Aufgabenerfüllung oder in Ausübung des Hausrechts im Einzelfall erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Auch hier wird mit der Zulassung im Einzelfall das Bestehen einer Gefahrenlage vorausgesetzt, wobei das Bestehen einer abstrakten Gefahr, z. B. der Materialermüdung, des Diebstahls oder des Vandalismus ausreicht. Der Eingriff sollte dann auch zeitlich und räumlich auf die Abwendung der Gefahr beschränkt werden.

Zu Nummer 20 (§§ 18a, 18b neu)

Zu § 18a – Videoüberwachung nicht öffentlich zugänglicher Räume

Zusätzlich zu § 18, der die Videoüberwachung öffentlich zugänglicher Räume regelt, wird eine Vorschrift zur Videoüberwachung nicht öffentlich zugänglicher Räume eingefügt. Maßstab für ihre Zulässigkeit ist wie für die Videoüberwachung in öffentlich zugänglichen Räumen in § 18 Absatz 6 ihre Erforderlichkeit im Einzelfall zur Überwachung des öffentlichen Eigentums und zu öffentlichen Zwecken gewidmeter (beweglicher und unbeweglicher) Gegenstände im Hinblick auf Erhaltungszustand und Funktionsfähigkeit. Gedacht werden kann an umzäunte Baustellen, Gasversorgung, Elektrizitäts- und Wasserwerke in umfriedetem Gelände, Serverräume, Geräte in Forschungseinrichtungen oder allgemein an die Nutzung von KI-Systemen im Gebäudemanagement. Mit der Videoüberwachung kann ebenso Vandalismus und Diebstahl vorgebeugt werden. Die Identifizierung von Personen kommt nur unter den Voraussetzungen des § 18 Absatz 3 in Betracht.

Die Videoüberwachung ist in § 18 LDSG für öffentlich zugängliche Räume geregelt und berücksichtigt die an diesen Orten bestehende Gefährdungslage für den Schutz von Personen und Objekten auf der einen Seite und das Recht auf informationelle

Selbstbestimmung auf der anderen Seite, die gegeneinander abzuwägen sind. Die Videoüberwachung im öffentlichen Raum erfasst überwiegend unbekannte Personen, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff in ihr informationelles Selbstbestimmungsrecht durch ihr Verhalten nicht veranlasst haben.

Dagegen sind bei der Videoüberwachung nicht öffentlich zugänglicher Räume, beispielsweise am Arbeitsplatz (z. B. auf Baustellen) oder im Universitätskontext, je nach den Gegebenheiten weitere Gesichtspunkte in die Interessenabwägung einzustellen. Insbesondere der Beschäftigtendatenschutz verlangt besondere Vorkehrungen. Dies gilt auch, wenn in die Videoüberwachung Dritte (wie z. B. Dienstleister oder Studierende) einbezogen werden sollen, da diese jederzeit identifizierbar sind. Auf der anderen Seite ist gegebenenfalls die besondere Schutzbedürftigkeit bestimmter Anlagen, z. B. im Hochschulbereich, einzubeziehen.

Die Schutzbedürftigkeit dieser betroffenen Personen wird als besonders hoch einzuschätzen sein, da sie sich der Videoüberwachung oder der Erfassung durch KI-Systeme nicht entziehen können. Deshalb müssen geeignete technisch-organisatorische Maßnahmen getroffen werden, die den Eingriff so minimal wie möglich gestalten. Zu überprüfen sind insbesondere die zeitliche und räumliche Ausdehnung der Überwachung und die Speicherdauer. Wo möglich muss auf die personenscharfe Aufzeichnung verzichtet werden. Die Videoüberwachung und ggf. die Nutzung von KI-Systemen ist genauso wie im öffentlichen Raum kenntlich zu machen. Die Löschung hat unverzüglich, das heißt ohne schuldhaftes Zögern, zu erfolgen, sobald die Daten nicht mehr benötigt werden.

Die Vorschrift regelt nur die Verarbeitung personenbezogener Daten, die, auch unabsichtlich, bei der Videoüberwachung (auch mittels KI) von Objekten erstellt werden. Die technischen Daten können dauerhaft gespeichert werden, soweit die personenbezogenen Daten entfernt wurden.

In Bezug auf Beschäftigte unterliegt die Weiterverarbeitung zur Aufdeckung von Straftaten und Pflichtverletzungen den Beschränkungen des § 15 Absatz 5 und 7.

Zu § 18b – Sonstige technische Überwachung

Ausgehend von der Tatsache, dass es eine Vielzahl technischer Möglichkeiten gibt, um die im öffentlichen Eigentum stehenden oder zu öffentlichen Zwecken gewidmeten Gegenstände auf ihren Erhaltungszustand und ihre Funktionsfähigkeit

zu überwachen, wird eine weitere Ermächtigungsgrundlage zu deren Nutzung einschließlich der Nutzung von KI-Systemen eingefügt. Insbesondere im Gebäudemanagement hat der Einsatz von KI zu Überwachungszwecken großes Potenzial und beschränkt sich nicht auf Videoüberwachung, Da hierbei die Verarbeitung personenbezogener Daten nicht immer ausgeschlossen werden kann, wird eine weitere Ermächtigungsgrundlage eingeführt.

Sofern hierbei Tonaufnahmen gefertigt werden, muss die Aufzeichnung von menschlichen Stimmen soweit wie möglich vermieden werden. Mindestens ist die Weiterverarbeitung solcher Tonaufnahmen ausgeschlossen; die Löschung muss automatisch innerhalb von 180 Sekunden erfolgen. Grund hierfür ist, dass mit Tonaufnahmen in den Kernbereich privater Lebensgestaltung eingegriffen werden kann, weshalb eine längere Speicherung ausgeschlossen werden muss. Außerdem erfordert der Überwachungszweck in der Regel keine Tonaufnahmen mit personenbezogenen Daten und kann daher nicht gerechtfertigt werden. Um eine Reaktionsmöglichkeit auf verdächtige Geräusche in Bezug auf den Überwachungszweck zu ermöglichen, darf die Speicherdauer von Tonaufnahmen nicht zu kurz sein. Hieraus resultiert die Speicherdauer von 180 Sekunden.

Zu Nummer 21 (§ 27a neu – Datenschutzaufsicht für digitale Dienste)

Die Bestimmung der Aufsicht der oder des LfDI für digitale Dienste ergänzt die Zuweisung der Zuständigkeit der oder des LfDI für die Ordnungswidrigkeiten nach § 3a der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten nach „§ 28 Absatz 1 Nummer 10, 11 und 13 des Telekommunikation-Telemedien-Datenschutz-Gesetzes“ (nunmehr § 28 Nummer 10, 11 und 13 TDDDG), soweit nicht der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig ist. Es handelt sich um eine klarstellende Vorschrift, da gemäß § 1 Absatz 1 Nummer 8 TDDDG bei digitalen Diensten die Aufsicht durch die nach Landesrecht zuständigen Behörden und § 40 des Bundesdatenschutzgesetzes unberührt bleibt. Insbesondere wird klargestellt, dass die oder der LfDI die Befugnisse nach Artikel 58 DSGVO ausüben kann.

Zu Nummer 22 (Inhaltsübersicht)

Als redaktionelle Folgeänderung zu den Nummern 1 bis 21 ist die Inhaltsübersicht anzupassen.

2. Zu Artikel 2 – Änderung des EGovG BW

Zu Nummer 1 (§ 17a neu – Automatisierter Erlass von Verwaltungsakten)

§ 35a des Landesverwaltungsverfahrensgesetzes statuiert einen landesrechtlichen Gesetzesvorbehalt für den vollständig automatisierten Erlass eines Verwaltungsaktes. Diesen Gesetzesvorbehalt füllt § 17a EGovG BW unter Berücksichtigung der Rahmenbedingungen des Artikels 22 DSGVO aus. Die weiteren datenschutzrechtlichen Verarbeitungsvoraussetzungen bleiben unberührt.

Zu Absatz 1

In Absatz 1 wird der Erprobungszweck als Leitlinie für die Anwendung des vollständig automatisierten Erlasses von Verwaltungsakten einschließlich der Nutzung von KI-Systemen in verschiedenen Anwendungsbereichen festgelegt, um nach erfolgreicher Erprobung der Landesregierung zu ermöglichen, den automatisierten Erlass von Verwaltungsakten in einzelnen Anwendungsbereichen dauerhaft zuzulassen. Auf Grundlage der bei der Erprobung gewonnenen Informationen kann der Rahmen für den automatisierten Erlass von Verwaltungsakten so weiterentwickelt werden, dass Gesellschaft, Verwaltung, Wirtschaft und Wissenschaft davon profitieren, ohne dass unvorhersehbare Risiken eingegangen werden.

Bestehende Regelungen, die auf der Grundlage von § 35a LVwVfG den automatisierten Erlass von Verwaltungsakten zugelassen haben, werden von dieser Regelung nicht berührt (vgl. z. B. § 32a des Finanzausgleichsgesetzes).

Zu Absatz 2

Nach Artikel 22 Absatz 2 Buchst. b DSGVO dürfen ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen gegenüber einer natürlichen Person, die ihr gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, durch Rechtsvorschriften zugelassen werden, wenn „diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten“.

Diesen Voraussetzungen wird bereits durch die Regelungen zum vollständig automatisierten Erlass eines Verwaltungsaktes nach § 35a LVwVfG, zum Untersuchungsgrundsatz beim Einsatz von automatischen Einrichtungen zum Erlass von Verwaltungsakten nach § 24 Absatz 1 Satz 3 LVwVfG, zum Anhörungsrecht nach § 28, zum Bekanntgabeerfordernis gem. § 41 LVwVfG sowie zu den

Rechtsbehelfsmöglichkeiten hinreichend Rechnung getragen (in diesem Sinne Ramsauer/Tegthoff, VwVfG, 24. Aufl. 2023, § 35a Rn. 7a, mit Nachweisen zu kritischen Stimmen aus der Literatur).

Als darüberhinausgehende Maßnahme zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen, wird in Absatz 2 die Erprobungsmöglichkeit auf solche Konstellationen beschränkt, bei denen die Chancen der effizienten Verwaltung die Risiken der Automatisation überwiegen. Ergänzend kann ein Risikomanagementsystem, wie in § 88 Absatz 5 der Abgabenordnung beschrieben, sinnvoll sein.

Zu Satz 1

Die für die Durchführung eines Verwaltungsverfahrens zuständige Behörde kann nach Satz 1 darüber entscheiden, ob sie den vollständig automatisierten Erlass von Verwaltungsakten erproben möchte. Dabei wird der Anwendungsbereich für die Erprobungsmöglichkeit unter Verweisung auf § 35a LVwVfG insoweit beschränkt, als für den vollständig automatisierten Erlass des Verwaltungsaktes weder ein Ermessen noch ein Beurteilungsspielraum bestehen darf. Überdies dürfen dieser Verfahrensweise keine überwiegenden Interessen von denjenigen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden, entgegenstehen.

Zu Satz 2

Satz 2 enthält Regelbeispiele, bei denen das Interesse an dem automatisierten Erlass eines Verwaltungsaktes den Interessen von denjenigen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden, nicht entgegenstehen dürfte. Soweit ein Verwaltungsakt mehrere Entscheidungen enthält, können die Regelbeispiele nebeneinander angewendet werden (z. B. Sachentscheidung nach Nummer 3 und Kostenentscheidung nach Nummer 4). Die Regelung ist nicht abschließend und kann Anhaltspunkte für vergleichbare Fälle geben, bei denen ebenfalls der vollständig automatisierte Erlass in Betracht kommt.

Zu Absatz 2 Satz 2 Nummer 1

Wenn diejenigen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden, ausdrücklich und freiwillig ihre Einwilligung zum vollständig automatisierten Erlass des Verwaltungsakts geben, ist diese Verfahrensweise unter

den Gesichtspunkten des Daten- und Rechtsschutzes unproblematisch. Da deren personenbezogenen Daten im Verwaltungsverfahren verarbeitet werden, ist bei der Bestimmung der Freiwilligkeit auf die sich im Datenschutzrecht herausgebildeten Grundsätze zurückzugreifen.

Zu Absatz 2 Satz 2 Nummer 2

Nach VGH BW, Beschluss vom 13.11.2020 – 2 S 2134/20, Leitsatz 1, ist ein vollautomatisiert erlassener Gebührenbescheid, der in Bezug auf die verfahrensrechtliche Grundlage umstritten ist, jedenfalls dann „geheilt“, wenn dieser Bescheid im Widerspruchsverfahren durch einen Amtswalter überprüft und der Widerspruchsbescheid unterschrieben worden ist. Falls also den betroffenen Interessen ausnahmsweise nicht im automatisierten Verfahren genügt wurde, kann dies durch den Amtswalter im Widerspruchsverfahren geheilt werden. Deshalb darf in diesem Fall der Widerspruchsbescheid auch nicht vollständig automatisiert erlassen werden.

Zu Absatz 2 Satz 2 Nummer 3

Die Regelung orientiert sich an § 39 Absatz 2 Nummer 1 LVwVfG, wonach eine Begründung entbehrlich ist, wenn dem Anliegen des Adressaten des Verwaltungsaktes gefolgt wird und zugleich Dritte nicht belastet werden. Dementsprechend erscheint aus Sicht des Rechtsschutzes auch der vollautomatisierte Erlass eines Verwaltungsaktes unproblematisch.

Zu Absatz 2 Satz 2 Nummer 4

Die Regelung orientiert sich an § 39 Absatz 2 Nummer 2 LVwVfG, wonach eine Begründung in den bestimmten Fällen entbehrlich ist, weil der Rechtsschutz – bei enger Auslegung als Ausnahmebestimmung – nicht beeinträchtigt wird. Dementsprechend erscheint auch der vollautomatisierte Erlass eines Verwaltungsaktes unproblematisch.

Zu Absatz 3

Mit der Anzeigepflicht nach Absatz 3 mindestens einen Monat vor Aufnahme des Verfahrens bei der obersten Fachaufsichtsbehörde und dem für das Verwaltungsverfahrensrecht zuständigen Innenministerium wird eine präventive Prüfung ermöglicht und die oberste Fachaufsichtsbehörde und das Innenministerium

können auf ähnliche Verfahren hinweisen oder aufsichtsrechtliche Maßnahmen prüfen und ergreifen. Daraufhin können auch etwa nach der DSGVO (bspw. Datenschutz-Folgenabschätzung) und der KI-VO (bspw. Grundrechts-Folgenabschätzung) erforderliche Unterlagen angefordert werden. Im Übrigen erfahren dadurch die oberste Fachaufsichtsbehörde und das Innenministerium, wann die Fristen nach Absatz 5 zu laufen beginnen.

Zu Absatz 4

Die Rahmenbedingungen der Evaluation werden in Absatz 4 festgelegt. Nach Nummer 4.2.8 Satz 2 der VwV Regelungen sind Rechtsvorschriften mit Erprobungsklauseln zu befristen. Dabei sollte die Befristung der Erprobung so gewählt werden, dass der vorübergehende Erprobungszweck zum Tragen kommt, aber gleichzeitig ausreichend Zeit für die Erprobung und den damit verbundenen regulatorischen Lernprozess zur Verfügung steht. Zwar könnte gerade auch bei einem Misserfolg der Erprobung ein Evaluationsbericht einen erheblichen Erkenntnisgewinn erbringen, jedoch könnte eine uneingeschränkte Berichtspflicht vor einer Erprobung abschrecken. Auch könnte die Berichterstellung unwirtschaftlich sein, wenn keine Fortführung der Erprobung geplant oder der Dauerbetrieb beabsichtigt ist.

Da mit der Erprobung unvorhergesehene Entwicklungen und Herausforderungen einhergehen können, ist es nicht sinnvoll, die Dauer der Experimentierphase gesetzlich einheitlich festzuschreiben, ohne dass im Einzelfall davon abgewichen werden kann. Wird der Evaluierungsbericht nicht innerhalb eines Jahres vorgelegt, darf der vollständig automatisierte Erlass von Verwaltungsakten nur mit Einverständnis der Fachaufsichtsbehörde im Einvernehmen mit dem Innenministerium für maximal ein Jahr fortgesetzt werden. Bis zum Ende der Jahresfrist und nach rechtzeitiger Vorlage des Evaluationsberichts kann die Verfahrensweise zum automatisierten Erlass von Verwaltungsakten weitergeführt werden. Wird der Evaluationsbericht fristgerecht vorgelegt, verlängert sich der Erprobungszeitraum automatisch um zwei Jahre, in denen die Landesregierung gegebenenfalls eine Verordnung nach Absatz 5 zur generellen Zulassung des vollautomatischen Erlasses beschließen kann.

Zu Absatz 5

Die wesentlichen rechtsstaatlichen Verfahrensgarantien sind im LVwVfG geregelt, so dass die Landesregierung zu ergänzenden Verfahrensregelungen – wie hier dem

vollständig automatisierten Erlass von Verwaltungsakten im Rahmen des § 35a LVwVfG – durch Gesetz ermächtigt werden kann. Durch die Auswertung des Evaluationsberichts verfügt die Landesregierung über die erforderlichen Informationen. In der Rechtsverordnung kann die Zulassung des vollständig automatisierten Erlasses von Verwaltungsakten von der Erfüllung bestimmter Bedingungen wie etwa einem Risikomanagementsystem nach dem Beispiel von § 88 Absatz 5 der Abgabenordnung abhängig gemacht werden.

Der Rahmen der Verordnungsermächtigung ist ausreichend bestimmt durch die Verweisung auf § 35a LVwVfG und die Voraussetzung, dass die Interessen von denjenigen, für den die Verwaltungsakte bestimmt sind oder von ihnen betroffen werden, voraussichtlich nicht entgegenstehen. Eine weitere Konkretisierung erfolgt durch die entsprechende Anwendung von Absatz 2 Satz 2.

Zu Nummer 2 (Inhaltsübersicht)

Als redaktionelle Folgeänderung zu Nummer 1 ist die Inhaltsübersicht anzupassen.

Zu Artikel 3 – Änderung des AGPStG

Nach § 4a AGPStG haben die unteren Fachaufsichtsbehörden, die mit der Standesamtsaufsicht betraut sind, zur Erfüllung ihrer Aufgaben Zugriff auf die in den Personenstandsregistern gespeicherten Daten. Die unteren Standesamtsaufsichten benötigen darüber hinaus auch Einsicht oder Zugriff auf die Sammelakten. Diese umfassen nach § 6 PStG die Dokumente, die einzelne Beurkundungen in den Personenstandsregistern betreffen. Sie umfassen die Dokumente, auf deren Grundlage die Beurkundung (Haupt- oder Folgebeurkundung) erfolgt ist. Diese werden in besonderen Akten (Sammelakten) aufbewahrt. Die Sammelakten können auch elektronisch geführt werden. Die Standesämter haben die Papiersammelakten entweder schon elektronisch erfasst oder sind noch dabei elektronische Sammelakten anzulegen. Für eine effektive zeit- und kostensparende Erfüllung der Aufsichtsaufgaben benötigen die Aufsichtsbehörden daher den elektronischen Zugriff auf die Sammelakten der Standesämter.

Zum Abruf befugt sind allein die mit der Standesamtsaufsicht betrauten Personen in den unteren Fachaufsichtsbehörden und auch nur zur Wahrnehmung ihrer Aufsichtsfunktion. Das gilt auch für den Fall, dass ihnen weitere Aufgaben innerhalb ihrer Behörde übertragen sind. Die Zweckbestimmung ermöglicht den Datenabruf sowohl zur Durchführung der durch Verwaltungsvorschrift des Innenministeriums

vorgeschriebenen regelmäßigen Aufsichtsprüfungen als auch zur Durchführung einer Einzelfallprüfung. Abgerufen werden dürfen alle in der elektronischen Sammelakte gespeicherten personenbezogenen Daten.

Die Standesämter sind verpflichtet, den Fachaufsichtsbehörden den Abruf zu ermöglichen, sofern sie bereits auf die elektronische Führung der Sammelakten umgestellt haben, bzw. diese elektronisch nacherfasst haben. Hingegen verpflichtet die Vorschrift die Standesämter nicht dazu, die Sammelakten bis zu einer bestimmten Frist elektronisch nachzuerfassen und zu führen.

Für die Einrichtung des automatisierten Abrufverfahrens sind sowohl personenstandsrechtliche als auch allgemeine datenschutzrechtliche Vorgaben zu beachten:

Die Benutzungsregelungen der §§ 61 ff. des Personenstandsgesetzes (PStG) sowie der §§ 63 ff. der Personenstandsverordnung (PStV) gelten auch für die Sammelakten. So folgt aus § 64 in Verbindung mit § 63 PStV u.a., dass die personenbezogenen Daten verschlüsselt übermittelt werden und zur Sicherung der ordnungsgemäßen Datenverarbeitung alle Abrufe durch die Standesämter protokolliert werden müssen. Zu protokollieren sind gem. § 64 Absatz 3 PStV für jeden automatisierten Datenabruf die Registrierungsdaten des abgerufenen Eintrags nach § 16 Absatz 2 Satz 1 PStV, die abrufende Person und Stelle, die in der Anfragenachricht angegebenen Auswahldaten, die abgerufenen Daten, soweit diese nicht über den Zeitpunkt des Abrufs festgestellt werden können, der Zeitpunkt des Abrufs, das Aktenzeichen oder eine sonstige Kennung der abrufenden Behörde, der Anlass des Abrufs und bei einem automatisierten Abruf die Bezeichnung des Verfahrens. Die abrufende Stelle trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs und die Protokolle sind vier Jahre nach Ablauf des Kalenderjahres, in dem der Abruf erfolgt ist, zu vernichten.

Die in den §§ 63 und 64 PStG geregelten Benutzungsbeschränkungen sind auch in Bezug auf die Sammelakten zu beachten. Diese gelten nicht nur gegenüber natürlichen Personen, sondern auch gegenüber Behörden, einschließlich der Aufsichtsbehörden. Der Schutz von Adoptierten, Personen, welche ihren Geschlechtseintrag nach § 2 Absatz 1 des Gesetzes über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG) und ihren Vornamen nach § 2 Absatz 3 SBGG geändert haben sowie in einer besonderen Gefährdungslage befindlichen Personen liefe ins Leere, wenn zwar die Benutzung der Personenstandsregister beschränkt, die der Sammelakten aber weiterhin zugelassen wäre.

Darüber hinaus sind die §§ 9 ff. PStV zu beachten, insbesondere müssen die erforderlichen technischen und organisatorischen Datensicherungsmaßnahmen auch in Bezug auf das Abrufverfahren getroffen werden. Auch für den Abruf der personenbezogenen Daten aus den Sammelakten ist nach § 13 PStV ein Betriebs- und Sicherheitskonzept zu erstellen.

Für die Verarbeitung der personenbezogenen Daten der Standesämter bzw. Kommunen durch die kommunalen IT-Dienstleister sind die Vorschriften zu Verantwortlichen und Auftragsverarbeitern in den Artikeln 24 ff. DSGVO zu beachten.

Zu Artikel 4 – Änderung des LIFG

Bisher enthielt § 2 Absatz 3 LIFG ausschließlich stellenbezogene Bereichsausnahmeregelungen, das heißt Ausnahmeregelungen, die an bestimmte informationspflichtige Stellen anknüpfen und diese Stellen entweder ganz oder hinsichtlich bestimmter Bereiche von der Informationspflicht nach dem LIFG ausnehmen.

Mit der Gesetzesänderung werden zwei informationsbezogene Bereichsausnahmeregelungen angefügt. Diese nehmen bestimmte Informationen insgesamt vom Anwendungsbereich des Gesetzes aus, unabhängig davon, bei welcher Stelle diese Informationen vorliegen.

Zu Absatz 3 Nummer 2

In Nummer 2 wird die stellenbezogene Bereichsausnahme für die Schulen nach § 2 des Schulgesetzes für Baden-Württemberg sowie Ausbildungs- und Prüfungsbehörden in Bezug auf Leistungsbeurteilungen und Prüfungen beibehalten. Dies ist erforderlich, da sich diese Stellen insofern nicht auf die neue Bereichsausnahmeregelung in Nummer 5 berufen könnten.

Zu Absatz 3 Nummer 5

Hinsichtlich der Kunst- und Wissenschaftsfreiheit wird die bisherige stellenbezogene Bereichsausnahme der Nummer 2 in eine informationsbezogene Bereichsausnahme umgewandelt (Nummer 5). Damit sind künftig alle Informationen, die den Bereich der Kunst- oder Wissenschaftsfreiheit betreffen, vom Anwendungsbereich des Gesetzes ausgenommen.

Die bisherige stellenbezogene Bereichsausnahme zugunsten der Kunst- und Wissenschaftsfreiheit konnte dazu führen, dass in Bezug auf ein- und dieselbe Information eine Stelle die Herausgabe aufgrund der Bereichsausnahme verweigern kann, eine andere Stelle hingegen nicht (vgl. hierzu Urteil des VGH BW vom 25.10.2023 – 10 S 125/22). Dieses Ergebnis begegnet verfassungsrechtlichen Bedenken, da die schrankenlos gewährleistete Kunst- und Wissenschaftsfreiheit nur durch entgegenstehende Belange mit Verfassungsrang zulässigerweise eingeschränkt werden kann, einem Rückgriff auf Ablehnungsgründe direkt aus der Verfassung jedoch laut VGH BW die Regelungssystematik des LIFG entgegensteht (vgl. Urteil vom 08.11.2023 – 10 S 916/22).

Mit der neuen informationsbezogenen Bereichsausnahmeregelung in Nummer 5 sollen die verfassungsrechtlich gewährleistete Kunst- und Wissenschaftsfreiheit umfassend geschützt und so verfassungsrechtliche Bedenken ausgeräumt werden.

Für die Beurteilung, ob die vorliegenden Informationen die Kunst- oder Wissenschaftsfreiheit der übermittelnden Stelle berühren, kann die informationspflichtige Stelle – den allgemeinen Grundsätzen des Verwaltungsverfahrensrechts nach § 24 LVwVfG entsprechend – die Stelle, von der die gegenständlichen Informationen übermittelt wurden zur Sachverhaltsaufklärung einbeziehen. Die Regelung zur Durchführung eines Drittbeteiligungsverfahrens nach § 8 LIFG ist hingegen nicht einschlägig, da durch die Bereichsausnahme zugunsten der Kunst- und Wissenschaftsfreiheit insofern bereits der Anwendungsbereich des LIFG nicht eröffnet ist.

Unter die Bereichsausnahmeregelung der Nummer 5 fallen auch solche Informationen, die im Zusammenhang mit Prüfungen und Leistungsbeurteilungen der Hochschulen nach § 1 des Landeshochschulgesetzes sowie der Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung unter die bisherige Regelung in § 2 Absatz 3 Nummer 2 zu fassen waren.

Zu Absatz 3 Nummer 6

In Nummer 6 wird eine informationsbezogene Bereichsausnahme zum Schutz des religionsgemeinschaftlichen Selbstbestimmungsrechts aus Artikel 140 GG in Verbindung mit Artikel 137 Absatz 3 der deutschen Verfassung vom 11. August 1919 (Weimarer Reichsverfassung, WRV) aufgenommen.

Kirchen, Religions- und Weltanschauungsgemeinschaften selbst sind schon bisher keine informationspflichtigen Stellen im Sinne des LIFG: Sie sind keine Stellen des Landes im Sinne des § 2 Absatz 1 Nummer 1 bzw. unterstehen nicht der Aufsicht des Landes nach § 2 Absatz 1 Nummer 3 und nehmen auch keine öffentlich-rechtlichen Verwaltungsaufgaben nach § 2 Absatz 1 wahr.

Mit der neu aufgenommenen Regelung sollen nun auch Informationen, die bei anderen Stellen zu religiösen Körperschaften vorhanden sind und die dem Schutzbereich des religionsgemeinschaftlichen Selbstbestimmungsrechts aus Artikel 140 GG in Verbindung mit Artikel 137 Absatz 3 WRV unterfallen, vom Anwendungsbereich des LIFG eindeutig ausgenommen werden. Der VGH BW stellte fest, dass das Fehlen einer Ausnahmevorschrift im LIFG für den Zugang zu Informationen, die der verfassungsrechtlichen Selbstverwaltungsgarantie einer Religionsgemeinschaft zuzurechnen sind, auf einer planwidrigen Regelungslücke beruht und behalf sich im konkreten Fall mit der Bildung einer Analogie (Urteil vom 08.11.2023 – 10 S 916/22). Diese Regelungslücke soll durch die neue Bereichsausnahmevorschrift geschlossen werden.

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts (u.a. Beschluss vom 21.9.1976 – 2 BvR 350/75; Beschluss vom 11.10.1977 – 2 BvR 209/76; Beschluss vom 4.6.1985 – 2 BvR 1703/83; Beschluss vom 25.02.1987- 1 BvR 47/8) bestimmen die Kirchen, Religions- und Weltanschauungsgemeinschaften im Wesentlichen selbst darüber, was zum privilegierten Rechtsbereich des Artikel 137 Absatz 3 WRV, also zu „ihren Angelegenheiten“, zählt. In Zweifelsfällen sind die Kirchen, Religions- und Weltanschauungsgemeinschaften daher durch die informationspflichtige Stelle in die Entscheidung einzubeziehen. Die Regelung zur Durchführung eines Drittbeteiligungsverfahrens nach § 8 LIFG ist hingegen nicht einschlägig, da die Informationen, die dem Schutzbereich des religionsgemeinschaftlichen Selbstbestimmungsrechts aus Artikel 140 GG in Verbindung mit Artikel 137 Absatz 3 WRV unterfallen, bereits vom Anwendungsbereich des LIFG ausgenommen sind.

Zu Artikel 5 – Änderung des LMedienG

Zu Nummer 1

Zu Buchstabe a

Die Ergänzung um die Fensterprogramme und Regionalfensterprogramme ist der Neuregelung der von der allgemeinen Regel abweichenden Zulassungsdauer für Fensterprogrammveranstalter in § 23 Absatz 3 Satz 2 geschuldet. Da für diese künftig eine eigenständige Regelung hinsichtlich der Zulassungsdauer besteht, sollten sie auch in der hiesigen Norm explizit aufgeführt werden.

Zu Buchstabe b

Die Änderung dient der Anpassung an die in § 23 Absatz 3 Satz 2 neu geregelte Zulassungsdauer für Fensterprogrammveranstalter.

Zu Nummer 2

Die Neufassung dient der Anpassung des LMedienG an die Änderungen im Medienstaatsvertrag durch den Fünften Staatsvertrag zur Änderung medienrechtlicher Staatsverträge, der am 1. Oktober 2024 in Kraft trat. Durch § 59 Absatz 4 Medienstaatsvertrag sind die beiden bundesweit verbreiteten reichweitenstärksten Fernsehvollprogramme in bestimmtem Umfang zur Aufnahme von Regionalfensterprogrammen verpflichtet. In § 59 Absatz 4 Satz 1 Medienstaatsvertrag wurde eine Klarstellung im Sinne des bisherigen Normverständnisses des Gesetzgebers vorgenommen, sodass die reichweitenstärksten bundesweit verbreiteten Fernsehvollprogramme der beiden größten Veranstaltergruppen auch weiterhin jeweils gleichermaßen zur Meinungsvielfaltssicherung über die Regionalfensterregelung verpflichtet werden. Eine Änderung der materiellen Rechtslage ist mit der Neufassung des § 23 Absatz 3 insofern nicht verbunden.

Daneben machen die o. g. Änderungen des Medienstaatsvertrags eine Begrenzung der Zulassungsdauer für Fensterprogrammveranstalter auf zehn Jahre erforderlich. § 59 Absatz 4 Satz 8 des Medienstaatsvertrags knüpft nämlich die Verpflichtung zur Aufnahme von Regionalfensterprogrammen an die Dauer der Zulassung. Falls – wie bisher – nur eine unbefristete Zulassung ausgesprochen werden könnte, könnten auch Regionalfensterprogramme nur dauerhaft aufgenommen und nicht begrenzt werden, wenn nicht der Fall eines Entzugs der Zulassung einträte.

Zu Nummer 3

Die Änderung dient der Anpassung des LMedienG an die aktuelle bundesgesetzliche Rechtslage. Mit dem Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des

Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze wurde das DDG beschlossen, das am 14. Mai 2024 in Kraft trat. Gleichzeitig trat durch das erstgenannte Gesetz das TMG außer Kraft. Regelungen des TMG wurden in das DDG überführt, weshalb entsprechende Anpassungen im LMedienG notwendig sind.

Zu Nummer 4

Die Zuständigkeit nach § 33 Absatz 1 DDG, vormals § 11 Absatz 1 TMG, wird vom Regierungspräsidium Karlsruhe auf die Landesanstalt für Kommunikation übertragen. Grund hierfür ist die Sachnähe zu der Zuständigkeit der Landesanstalt nach § 30 Absatz 2 Satz LMedienG für die Aufsicht über die Einhaltung der Bestimmungen des DDG.

In Bezug auf § 11 Absatz 2 Nummer 1 bis 3 TMG ist die Gesetzesänderung wegen der Überführung des TMG in das DDG erforderlich.

Zu Artikel 6 – Änderung der OWiZuVO

Zu Nummer 1 (§ 3a – Zuständigkeit der oder des Landesbeauftragten für den Datenschutz)

Das TTDSG wurde mit Wirkung vom 14. Mai 2024 überführt in das TDDDG. Der Verweis in § 3a OWiZuVO ist daher an die neue Bezeichnung anzupassen;

Zu Nummer 2 (§ 4 – Zuständigkeit der Regierungspräsidien)

Nach der Übertragung der Zuständigkeit für die Ordnungswidrigkeit nach § 33 Absatz 1 DDG auf die Landesanstalt für Kommunikation ist § 4 Absatz 2 Satz 1 Nummer 4 OWiZuVO anzupassen und der Verweis auf das TTDSG wie in § 3a zu korrigieren.

Zu Artikel 7 – Inkrafttreten

Das Gesetz tritt am Tag nach der Verkündung des Gesetzes in Kraft.