Drucksache 17/9983
Eingang 2.12.2025

Präsidentin des Landtags
von Baden-Württemberg
Frau Muhterem Aras MdL
Haus des Landtags
Konrad-Adenauer-Straße 3
70173 Stuttgart

2. Dezember 2025

Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze

Anlagen
Gesetzentwurf mit Vorblatt und Begründung
Stellungnahme des Normenkontrollrats Baden-Württemberg

Sehr geehrte Frau Landtagspräsidentin,

als Anlage übersende ich Ihnen gemäß Artikel 59 Absatz 1 der Verfassung des Landes Baden-Württemberg den von der Landesregierung beschlossenen

Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze.

Ich bitte Sie, die Beschlussfassung des Landtags herbeizuführen.

Die federführende Zuständigkeit liegt beim Ministerium des Inneren, für Digitalisierung und Kommunen, beteiligt sind das Staatsministerium, das Ministerium für Finanzen, das Ministerium für Kultus, Jugend und Sport, das Ministerium für Wissenschaft, Forschung und Kunst, das Ministerium für Umwelt, Klima und Energiewirtschaft, das Ministerium für Wirtschaft, Arbeit und Tourismus, das Ministerium für Soziales, Gesundheit und Integration, das Ministerium der Justiz und für Migration, das Ministerium für Verkehr, das Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz und das Ministerium für Landesentwicklung und Wohnen.

Mit freundlichen Grüßen

gez. Winfried Kretschmann

Vorabexemplar

- vor förmlicher Prüfung durch die Landtagsverwaltung -

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 verfassungsrechtlichen 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 Änderungen 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 dienen der Rechtssicherheit und sollen 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“ durch die Wörter „und der Gemeindeprüfungsanstalt Baden-Württemberg“ ersetzt.

   c) Absatz 5 wird wie folgt gefasst:

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

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 über künstliche Intelligenz oder ein vergleichbares Modell, welches lediglich einen oder mehrere spezielle Verwendungszwecke aufweist, einschließlich KI-Modelle für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen.“

3. § 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) Die neue Nummer 6 wird wie folgt gefasst:

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

6. § 5 Absatz 1 wird wie folgt geändert:

a) In Nummer 1 werden nach dem Wort „ist“ ein Semikolon und 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 angefügt:

„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 von Rechtsansprüchen oder Verteidigung gegen Rechtsansprüche Dritter erforderlich ist.

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

(4) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde öffentliche Stelle. Erfolgt die Übermittlung

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

(5) Automatisierte Abrufverfahren oder eine gemeinsame automatisierte Datei, in oder aus der mehrere öffentliche Stellen personenbezogene Daten verarbeiten, dürfen eingerichtet werden, soweit die rechtlichen Voraussetzungen zur Übermittlung vorliegen und die Einrichtung unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden. Automatisierte Abrufverfahren für Abrufe aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung offenstehen, dürfen ungeachtet der Bestimmungen in Satz 1 eingerichtet werden.“

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

„§ 7a

Auftragsverarbeitung; Verordnungsermächtigung

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

1. Gegenstand und Dauer der Verarbeitung,

2. Art und Zweck der Verarbeitung,

3. die Art der personenbezogenen Daten und

4. die Kategorien betroffener Personen.

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

(2) Die Landesregierung wird ermächtigt, durch Rechtsverordnung

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

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

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

4. weitere Nutzungsbedingungen festzulegen,

die Bestandteile der Auftragsverarbeitungsverträge nach Absatz 1 werden.

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

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

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 oder 2, ergreift die öffentliche Stelle geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 oder Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache.“

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) In Satz 1 werden die Wörter „verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können“ durch die Wörter „verarbeiten und vorhandene Daten der genannten Art weiterverarbeiten, 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) Dem neuen Absatz 3 wird folgender Satz angefügt:

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

e) Der bisherige Absatz 3 wird Absatz 4.

f) Nach dem neuen 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 auf Verlangen die Einhaltung dieser Verpflichtungen nachzuweisen.“

g) Der bisherige Absatz 4 wird Absatz 6.

15. § 15 wird wie folgt geändert:

a) Absatz 2 wird folgender Satz angefügt:

„Besondere Kategorien personenbezogener Daten dürfen entsprechend Satz 1 auch verarbeitet werden, soweit die Verarbeitung für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin oder der Beurteilung der Arbeitsfähigkeit der Beschäftigten erforderlich ist und wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.“

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 eingewilligt und für die Erreichung der Zwecke steht in beiden Fällen kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung. Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.“

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:

a) Absatz 1 wird aufgehoben.

b) 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 Absatz 1 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 einwilligt und kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung steht; zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.

§ 17b

Öffentlichkeitsarbeit

(1) Soweit der öffentlichen Stelle ein Auftrag zur politischen Bildung oder zur Bürgerinformation obliegt, dürfen öffentliche Stellen unbeschadet sonstiger

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

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

19. § 18 wird wie folgt geändert:

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

b) Absatz 1 wird wie folgt gefasst

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

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 darauf hinzuweisen, wo die weiteren Informationen des Verantwortlichen nach Artikel 13 der Verordnung (EU) 2016/679 verfügbar sind.“

d) In Absatz 3 wird nach dem Wort „Sicherheit“ das Wort „oder“ durch ein Komma 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 die Absätze 4 und 5.

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

h) Es wird folgender Absatz 6 angefügt:

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

1. Leib oder Leben von Personen zu schützen, oder

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

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

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 Absätze 5, 7 und 9 gelten entsprechend.

§ 18b

Sonstige technische Überwachung

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

Datenschutz-Gesetzes 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 § 17a eingefügt:

„§ 17a

Automatisierter Erlass von Verwaltungsakten; Verordnungsermächtigung

(1) Dieser Paragraf dient der Erprobung und nach erfolgreicher Erprobung der Zulassung 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) in der jeweils geltenden Fassung.

(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. kein Anlass besteht, den Einzelfall durch Amtsträger zu bearbeiten, da die vorliegenden Informationen und die Angaben derjenigen, für die der Verwaltungsakt bestimmt oder die von ihm betroffen werden, keine vom Regelfall abweichenden Hinweise enthalten.

(3) Mindestens einen Monat vor Aufnahme des Verfahrens zum vollständig automatisierten Erlass von Verwaltungsakten ist der obersten Fachaufsichtsbehörde oder der zuständigen Rechtsaufsichtsbehörde 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 oder der zuständigen Rechtsaufsichtsbehörde 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 oder der zuständigen Rechtsaufsichtsbehörde 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 § 35a 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:

„(3) 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. Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, Hochschulen nach § 1 des Landeshochschulgesetzes, 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 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 die Wörter „Vollprogramm oder Spartenprogramm“ durch die Wörter „Vollprogramm, Spartenprogramm, Fensterprogramm oder Regionalfensterprogramm“ ersetzt.

   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:

   „(3) In den beiden, jeweils unterschiedlichen Unternehmen nach § 62 des Medienstaatsvertrages 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 vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) in der jeweils geltenden Fassung, 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“ durch die Wörter „§ 33 Absatz 1 und Absatz 2 Nummer 1 und 2 des Digitale-Dienste-Gesetzes“ ersetzt.

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 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“ ersetzt.

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

„4. § 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 (§ 17b).

- Die Videoüberwachung (§ 18 LDSG) wird zur Erfüllung öffentlicher Aufgaben zugelassen, sofern sie im Einzelfall erforderlich ist; die Beschränkung auf den Schutz von Objekten und Personen entfällt. Darüber hinaus wird Videoschutz als generell geeignetes Mittel zum Schutz besonders sicherheitsrelevanter Objekte eingeführt; 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, um Leib oder Leben von Personen zu schützen oder Bauwerke und Infrastruktur der öffentlichen Hand technisch zu überwachen. Zwar wird in Bezug auf die zweite Alternative 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 elektronische Führung der Personenstandsregister ist seit dem 1. Januar 2009 zulässig und seit dem 1. Januar 2014 verpflichtend. 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 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 Satz 1 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 In Tsd. Euro	Restliche Jahre der Finanzplanung In Tsd. Euro		
1	**Land** Ausgaben insgesamt	0	0			
	davon 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.

X. Ergebnis der Anhörung

1. Angehörte Stellen

Zu dem Gesetzentwurf wurden die Kommunalen Landesverbände nach Artikel 71 Absatz 4 der Landesverfassung sowie 133 weitere Behörden, Verbände und Organisationen angehört. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI), die Beauftragte der Landesregierung für die Belange von Menschen mit Behinderungen, der Normenprüfungsausschuss und der Normenkontrollrat wurden zeitgleich beteiligt sowie der Gesetzentwurf im Beteiligungsportal des Landes zur Kommentierung freigeschaltet.

Folgende angehörte Stellen haben eine inhaltliche Stellungnahme abgegeben:

- Anwaltsverband Baden-Württemberg im Deutschen AnwaltVerein e. V. (Anwaltsverband BW)

- Arbeitsgemeinschaft der Hauptpersonalratsvorsitzenden des Landes Baden-Württemberg (ARGE-HPR)

- BBW - Beamtenbund Tarifunion (BBW)

- Baden-Württembergischer Handwerkstag e. V. (Handwerk BW)

- Baden-Württembergischer Industrie- und Handelskammertag (BWIHK)

- Baden-Württembergischer Notarverein e. V.

- Deutscher Richterbund Baden-Württemberg (DRB BW)

- Deutsche Vereinigung der Schöffinnen und Schöffen, Landesverband Baden-Württemberg e.V. (DVS-BW)

- Duale Hochschule Baden-Württemberg (DHBW)

- Gemeindeprüfungsanstalt (GPA)

- Hochschulen für Angewandte Wissenschaften Baden-Württemberg (HAW)

- Karlsruher Institut für Technologie (KIT)

- Komm.ONE

- Landesrektorenkonferenz der Pädagogischen Hochschulen Baden-Württemberg (LRK-PH)

- Landeszahnärztekammer Baden-Württemberg

- Landtag

- Rechtsanwaltskammer Stuttgart

- Sparkassenverband Baden-Württemberg

- Transparency International Deutschland e. V. – Regionalgruppe Baden-Württemberg

- Universitäten Konstanz, Stuttgart, Ulm, Freiburg jeweils mit Bezug auf die Stellungnahme der Zentrale Datenschutzstelle der baden-württembergischen Universitäten (ZENDAS).

- Universität Heidelberg

- Universitäten Tübingen, Freiburg mit Bezug zur Änderung des LIFG

- Universitätskliniken Freiburg, Heidelberg, Tübingen, Ulm

Die Kommunalen Landesverbände haben eine gemeinsame Stellungnahme übersandt. Der LfDI hat eine Stellungnahme abgegeben. Der Normenkontrollrat (NKR) hat keine weitere Stellungnahme abgegeben. Seine Stellungnahme datiert vom 14. Mai 2025. Der Normenprüfungsausschuss hat redaktionelle Anmerkungen zum Gesetzentwurf übermittelt. Über das Beteiligungsportal Baden-Württemberg wurde ein Kommentar abgegeben.

2. Zusammenfassung der Stellungnahmen

a) Zur Änderung des LDSG

Die Kommunalen Landesverbände (KLV) begrüßen grundsätzlich die Anpassungen des LDSG aufgrund der Evaluierung sowie der durch neue Gesetzgebung und Rechtsprechung erkannten Änderungsbedarfe. Dies sorge für größere Rechtssicherheit. Insgesamt bedürfe das Datenschutzrecht einer Vereinheitlichung und Entbürokratisierung. Die Öffnung in Richtung Künstlicher Intelligenz (KI) wird positiv bewertet. Die in § 9a und § 10 Absatz 4 gefundenen Lösungen werden als praxisnah und verhältnismäßig angesehen. Als weiterer Änderungsvorschlag wird angeregt, die Regelung des § 7a auch für kommunale Auftragsverarbeiter vorzusehen, um einheitliche Standards durchzusetzen. Zu § 17b wird die Frage der Anwendbarkeit auf die Übertragung von Gemeinderatssitzungen gestellt. Besonderes Augenmerk wird auf die Videoüberwachung gelegt. § 18 Absatz 1 solle um einen Passus ergänzt werden, der sich an § 21 Absatz 1 Nummer 1 des LDSG Rheinland-Pfalz orientiere: In Rheinland-Pfalz sei die Videoüberwachung bereits zulässig, wenn dies zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich sei. Damit wäre es beispielsweise möglich, bestimmte Örtlichkeiten im Siedlungsbereich, aber auch in der freien Natur, zu überwachen, die nach Erkenntnissen der zuständigen Behörden regelmäßig zur Entsorgung von Abfällen („wildem Müll“) genutzt werden. Für die Umsteigeknoten des öffentlichen Personennahverkehrs wird die ausdrückliche Aufnahme in die Nummer 1 des § 18 Absatz 1 vorgeschlagen. Diese seien Orte mit hohem Personenaufkommen, besonderer Bedeutung für die öffentliche Sicherheit und erhöhter Anfälligkeit für Straftaten (z. B. Diebstahl, Körperverletzung, Vandalismus, Belästigung). Videoüberwachung sei maßgeblich zur Erhöhung der objektiven Sicherheit. Die Ausweitung der Informationspflichten wird abgelehnt. Der Verlängerung der Speicherfrist auf zwei Monate wird zugestimmt. Im Übrigen wird initiativ die Änderung der Gemeindeordnung für eine Öffnungsklausel für KI bei Erstellung der Gemeinderatsprotokolle vorgeschlagen.

Der LfDI sieht in zahlreichen Punkten Nachbesserungs- und Konkretisierungsbedarf. Es fehlt ihm insbesondere an der Regelung konkreter verpflichtender technischer und organisatorischer Maßnahmen zugunsten des Datenschutzes. Außerdem bemängelt er an mehreren Stellen eine ungenügende Normenklarheit. Die KI-Regelung hält er, ohne die Interessen der betroffenen Personen ausreichend in einer Abwägung zu berücksichtigen, für zu pauschal. Insbesondere bezüglich der Einschränkung des Löschungsanspruchs müsse wegen des Grundsatzes der Speicherbegrenzung die Anwendung von KI zurücktreten, wenn kein erhebliches öffentliches Interesse an der Verarbeitung bestünde. Im Justizbereich hält er den Landesgesetzgeber nicht für

befugt, Regelungen zur Anwendung von KI zu treffen. Für die Nutzung personenbezogener Daten für die Forschung fordert er weitreichendere Garantien.

Der NKR begrüßt die Umsetzung der in der Evaluierung festgestellten Änderungsbedarfe. Im Datenschutzrecht müssten die Spielräume der DSGVO genutzt werden, um „Gold-Plating“ zu vermeiden. Nach Ansicht des NKR gebe es noch mehr Ansatzpunkte für eine Entlastung der Verwaltung von bürokratischen Pflichten, z. B. bei den Informationspflichten, die nicht über das zwingend erforderliche Maß erweitert werden sollten. Die Regelung zum Training von KI wird grundsätzlich begrüßt; es sei aber wichtig, hinsichtlich der Anforderungen an Zweckbindung und Rechtfertigung einen Gleichklang zur KI-VO herzustellen. Ausdrücklich begrüßt wird der Wegfall der aufwändigen Vorrangprüfung anderer Mittel für die Anwendung der Videoüberwachung bei sicherheitsrelevanten Objekten.

Die Architektenkammer Baden-Württemberg hat keine Einwendungen.

Die ARGE HPR bezieht sich auf die Beschränkung der Betroffenenrechte bei KI-Anwendung. Für einen hohen Schutz personenbezogener Daten müssten die Rechte auf Löschung und Berichtigung umfänglich aufrechterhalten werden. An dem Einsatz von Filtern bestehen diesbezüglich Bedenken. Die Beurteilung der Arbeitsfähigkeit einzelner Beschäftigter wird für nicht zulässig erachtet. Für die Beurteilung der Arbeitsfähigkeit der Beschäftigten wird jedenfalls ärztliches Personal für erforderlich gehalten. Die Regelung zur Videoüberwachung in §§ 18 Absatz 6, 18a stehe im Widerspruch zum besonderen Schutz der Schülerinnen und Schüler. Auch die Persönlichkeitsrechte der Lehrkräfte seien gefährdet.

Der Anwaltsverband BW unterstützt die Umsetzung der Evaluierung des LDSG in vielen Punkten. Kritisch sieht er die Beschränkung der Betroffenenrechte bei KI-Nutzung, die erleichterte Vorrangprüfung bei der Videoüberwachung sowie die Videoüberwachung nicht öffentlich zugänglicher Räume. Nach dem Verständnis des Anwaltsverbands BW müssten Regelungen für den Einsatz von KI in der Justiz eher in die bundesrechtlichen Prozessordnungen oder ins LDSG-JB aufgenommen werden,

Der BBW - Beamtenbund Tarifunion sieht die vorgesehene Einschränkung des Berichtigungsrechts bei durch KI-System und KI-Modelle verarbeiteten personenbezogenen Daten kritisch. Das Grundrecht auf Datenschutz werde faktisch ausgehöhlt, da eine Korrektur ausgeschlossen bleibe, sobald diese mit hohem technischem oder wirtschaftlichem Aufwand oder erheblichen ökologischen Folgen

verbunden wäre. Der Gesetzgeber sollte durch Vorgaben zu Transparenz, Nachvollziehbarkeit und technische Mindeststandards sicherstellen, dass das Berichtigungsrecht durchgesetzt werden könne.

Der BWIHK sieht den Vorteil einer Rechtsgrundlage für den KI-Einsatz, wobei die datenschutzrechtlichen Anforderungen nicht weitergehen dürften als die nach der KI-VO. Die neuen Zweckänderungsvorschriften in § 5 Nummer 3 und 5 werden ebenfalls gutgeheißen. In mehreren Vorschriften wird aber zusätzlicher bürokratischer Aufwand und „Gold-Plating" bemängelt.

Der DRB BW befürwortet die Prüfung des Einsatzes von KI-basierten Systemen zur Unterstützung der richterlichen und staatsanwaltschaftlichen Arbeit. Es wird daher angeregt, auch die Staatsanwaltschaften im Entwurf aufzunehmen, um auch dort eine sichere Grundlage für den Einsatz von KI-Systemen zu schaffen. Beim Einsatz von KI sei stets darauf zu achten, dass Entscheidungen der Justiz auch künftig nicht durch KI-Systeme, sondern durch Richter und Staatsanwälte getroffen werden. KI-Systemen dürfe es im Hinblick auf die Unabhängigkeit der Justiz nicht möglich sein, das Entscheidungsverhalten von Richtern und Staatsanwälten individuell auszuwerten. Weiter dürften der Gerichts- und Behördenverwaltung aufgrund datenschutzrechtlicher Regelungen im Zusammenhang mit dem Einsatz von KI-Systemen keine zusätzlichen Dokumentationspflichten auferlegt werden, welche die sowieso schon hohe Arbeitsbelastung weiter erhöhten.

Der DVS-BW begrüßt den verbesserten übergreifenden Datenzugriff sowie die Ausweitung der Videoüberwachung. Die Überwachung des öffentlichen Raums sei seiner Ansicht nach aber zu sehr beschränkt. Es fehlten in der Auflistung öffentliche Plätze, Gartenanlagen und Parks, Bahnhöfe und Haltestellen oder auch rund um die Uhr zugängliche Müllsammelstellen, in denen sich bevorzugt und zunehmend Straftaten und Ordnungswidrigkeiten ereigneten. Auch die Videoüberwachung in nicht öffentlich zugänglichen Räumen sei zu sehr eingeschränkt.

Die DHBW trägt zahlreiche Änderungsanregungen vor, die die KI-Regelung, §§ 6, 7a, 13, 17b und 18 betreffen. Im Wesentlichen wird die KI-Regelung als hilfreich erachtet. Im Übrigen werden Präzisierungen und Klarstellungen verlangt.

Die GPA weist darauf hin, dass sie gleichartige Tätigkeiten wie der Rechnungshof in eigener Verantwortlichkeit wahrnimmt. Sie regt daher an, sie in Bezug auf ihre Prüftätigkeit in § 2 Absatz 4 neben dem Rechnungshof aufzunehmen.

Die HAW macht sich basierend auf der Einschätzung von ZENDAS die Ausführungen dieser zu den §§ 3a, 8, 17b, 18 Absatz 6, 18a und die ergänzenden Vorschläge zu eigen.

Das KIT macht sich die Stellungnahme von ZENDAS in Bezug auf §§ 3a, 7a, 8 und 17b zu eigen. Zusätzlich wird empfohlen, auf das Widerspruchsrecht nach § 17b Absatz 2 zu verzichten: Das Widerspruchsrecht nach Artikel 21 Absatz 1 DSGVO wird für ausreichend erachtet.

Die Komm.ONE begrüßt die Regelungen zum Einsatz von KI-Systemen und zur KI-Nutzung. Auch die damit verbundene Beschränkung der Betroffenenrechte entspreche den derzeitigen Erkenntnissen der Wissenschaft (keine Löschung von personenbezogenen Daten in KI-Modellen möglich, sondern nur Filterung des Outputs im KI-System bis zum Neutraining des Modells). Zu begrüßen sei auch die Regelung in §11a zum Training von KI-Modellen, weil damit die Mitglieder und Kunden der Komm.ONE erstmalig rechtlich die Möglichkeit erhielten, auch personenbezogene Daten in das Training von Modellen einzubeziehen und somit Hindernisse wegfielen, dass die Kunden die Komm.ONE mit dem Training der Daten der Gemeinde beauftragten. Kritisiert werden einzelne Formulierungen, die näher ausgeführt oder legal definiert werden sollten, Außerdem wird angeregt, wie in Hessen gesetzlich die Anwendung einzelner Datenschutzregelungen des LDSG für Wettbewerbsunternehmen wie die Komm.ONE zu regeln.

Die LRK-PH hält eine Klarstellung erforderlich, dass bzw. ob § 3a eine umfassende, eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten bei Nutzung eines KI-Systems darstellt. Die Regelung des § 8 Absatz 2 könnte dem Forschungszweck zuwiderlaufen. In § 17b wird die Anwendbarkeit auf die Hochschulen sowie das Verhältnis zu § 15 nachgefragt.

Die Landeszahnärztekammer begrüßt grundsätzlich die vorgesehenen Änderungen, insbesondere die erhöhte Rechtssicherheit im Bereich des Datenaustauschs in der Verwaltung sowie beim Einsatz von KI-Systemen.

Der Landtag weist auf den Änderungsbedarf in § 2 Absatz 5 durch die kürzlich erfolgte Änderung des Landesdatenschutzgesetzes hin. Im Übrigen hat er redaktionelle Anmerkungen.

Der Notarverein begrüßt die neue Rechtsgrundlage für die Anonymisierung und die Möglichkeit der Zweckänderung für allgemein anerkannte öffentliche Interessen nach

§ 5 Absatz 1 Nummer 1. Vorhandene Datenbestände könnten im Interesse an einer geordneten und effektiven Rechtspflege für die Verbesserung interner Optimierungen, etwa IT- und KI-Lösungen genutzt werden. Kritisch sieht er das Nebeneinander von Datenschutzbehörde und Dienstaufsicht durch die Justiz nach der Bundesnotarordnung.

Die Rechtsanwaltskammer Stuttgart nimmt angesichts der Beschränkung der Betroffenenrechte eine kritische Haltung zur Nutzung von KI ein. Die Gesetzesbegründung erscheine pauschal und wenig dezidiert.

Der Sparkassenverband Baden-Württemberg begrüßt den Ansatz zur Modernisierung des LDSG. Seine Anliegen sind: keine Überregulierung neben der DSGVO, klare, einheitliche und verständliche Regelungen, Stärkung digitaler Verfahren, Bürokratieabbau statt zusätzlicher Belastungen. Zum Teil sieht er diesbezüglich noch Nachbesserungsbedarf, u. a. die konsequente Umsetzung von „Digital first“ sowie längere Übergangsfristen für neue Pflichten.

Die Universitäten Freiburg, Konstanz, Stuttgart und Ulm (im Folgenden ZENDAS) verweisen auf die hohe Relevanz des Datenschutzrechts für die Arbeit der Hochschulen in Verwaltung, Forschung und Lehre. Sie wünschen sich für die Nutzung von KI eine eigenständige Rechtsgrundlage. In Bezug auf die Einschränkung der Betroffenenrechte bei KI-Anwendungen wird die Verhältnismäßigkeit in Frage gestellt. Zugleich wird aber eine Beschränkung des Auskunftsrechts vorgeschlagen. Zu § 8 Absatz 2 wird vorgebracht, dass im Interesse der wissenschaftlichen Forschung von einer Bereitstellung von Informationen für die Öffentlichkeit abgesehen werden müsse. Die Regelungen der §§ 11a, 13 und 16 werden begrüßt. In Bezug auf die Öffentlichkeitsarbeit wird die Streichung des Widerspruchsrechts gefordert sowie eine Klarstellung für die Verarbeitung von Beschäftigtendaten angeregt. Gegen die Regelung der Videoüberwachung bestünden rechtliche Bedenken, im Besonderen gegen die gesetzliche Fiktion der Videoüberwachung als angemessenes Mittel hinsichtlich bestimmter Schutzobjekte, gegen die neue Ausgestaltung der Informationspflicht sowie gegen die längere Speicherfrist. Das von Hochschulen betriebene Auslastungsmanagement bei hochschulgenutzten Flächen wird erwähnt, aber nicht der Videoüberwachung zugerechnet.

Das Universitätsklinikum Freiburg spricht sich grundsätzlich zustimmend zum Gesetzentwurf aus und bewertet ihn als praxisorientiert und innovationsfreundlich. Es befürwortet die Gesetzesziele einer klaren Rechtsgrundlage für die Nutzung von KI,

der Förderung der Datennutzung durch Reduktion des Personenbezugs und der Stärkung der Forschungskooperation. Vermisst wird in Bezug auf § 9a die Definition eines unverhältnismäßig hohen Aufwands.

Das Universitätsklinikum Heidelberg sieht die Änderungen im LDSG positiv als innovativ und sachgerecht, insbesondere die datenschutzrechtlichen Regelungen zur Nutzung von KI. Vermisst werden die Regelung besonderer Anforderungen an den Einsatz von KI sowie eine Definition synthetischer Daten. § 9a leide an der Unbestimmtheit geeigneter Maßnahmen zur Berücksichtigung des Berichtigungsrechts sowie des Maßstabs für die Verhältnismäßigkeit zu treffender Maßnahmen. Auch die Forschungsregelung wird begrüßt; allerdings wird für die Weitergabe an Dritte ein Widerspruchsrecht für die betroffenen Personen befürwortet. Die Regelung des § 18 Absatz 6 wird insofern als rechtlich bedenklich bewertet, als vulnerable Personengruppen betroffen sein könnten. Im Hinblick auf § 18a wird auf die besondere Bedeutung von Schutzmaßnahmen zugunsten der Beschäftigten hingewiesen.

Das Universitätsklinikum Tübingen kritisiert die strenge Regelung der Authentifizierung für Beschäftigte als realitätsfern. Die „Aufweichung“ von Betroffenenrechten beim KI-Einsatz wird als unionsrechtswidrig abgelehnt. Der Schutz von Berufsgeheimnisträgern werde nicht berücksichtigt. Das KI-Training mit besonderen Kategorien personenbezogener Daten bedürfe einer spezifischen Rechtsgrundlage unter Berücksichtigung von Artikel 89 DSGVO. Für die Videoüberwachung wird eine kürzere Speicherdauer sowie eine Datenschutz-Folgenabschätzung für jede automatisierte KI-Auswertung verlangt.

Das Universitätsklinikum Ulm steht den geplanten Änderungen, insbesondere die Verarbeitung von Daten durch KI-Systeme zu adressieren, positiv gegenüber. In Bezug auf § 13 Absatz 5 wird eine Konkretisierung der „gemeinwohlbezogenen Forschungszwecke“ angeregt.

b) Zur Änderung des EGovG BW

Die KLV regen die Prüfung einer weitergehenden Experimentierklausel wie in § 155 Absatz 4 der Abgabenordnung an. Die Einwilligung nach Absatz 2 Satz 2 Nummer 1 müsse in Textform zu erteilen sein. Für die bessere Handhabbarkeit bringen sie einen Änderungsvorschlag zu Absatz 2 Satz 2 Nummer 4 ein.

Der LfDI vermisst eine Abgrenzung zu der Regelung der Erprobung und des Einsatzes von KI im LDSG. Des Weiteren bemängelt er fehlende Regelungen zum Risikomanagement, die wegen der spezifischen Gefahren der automatisierten Verarbeitung gemäß Artikel 22 Absatz 2 Buchstabe b DSGVO erforderlich seien.

Der NKR begrüßt die Einführung der Erprobungsklausel für den automatisierten Erlass von Verwaltungsakten. Dies könne langfristig zu einer erheblichen Verwaltungsvereinfachung führen.

Der Anwaltsverband leitet aus dem Recht auf rechtliches Gehör und dem Recht auf ein faires Verfahren ab, dass die Einzelperson nicht nur Objekt des Verfahrens sein dürfe. Dies schließe den Einsatz eines algorithmischen Systems als Entscheider aus.

Die ARGE-HPR befürchtet eine möglicherweise fehlerhafte Bearbeitung durch KI-Technik. Die Erprobung müsse durch fachkundige Sachbearbeitungen kontrolliert werden.

Der BBW - Beamtenbund Tarifunion beurteilt die Möglichkeit, Verwaltungsakte automatisiert durch KI zu erlassen, kritisch. Hierdurch würde der Rechtsstaat geschwächt.

Handwerk BW begrüßt die Erprobungsregelung des § 17a EGovG BW ausdrücklich als mutigen Schritt in Richtung digitaler und effizienter Verwaltung. Es wird um die Einbeziehung der Rechtsaufsicht in die Regelungen des Absatz 3 und 4 gebeten.

Die Rechtsanwaltskammer Stuttgart bezieht sich auf die vorgesehene Evaluierung der Erprobungsregelung und möchte hierbei einbezogen werden.

Der Universität Freiburg geht die Erprobungsregelung aus rechtsstaatlichen Erwägungen zu weit. Der Normgeber sei gefragt, um bereichsspezifische Zulassungen und den Übergang in die reguläre Anwendung zu regeln.

ZENDAS möchte ergänzend eine Rechtsgrundlage für den Abruf der Identifikationsnummer zur Zulassung zum Hochschulstudium eingefügt haben.

c) Zur Änderung des LIFG

Die KLV teilen die im Gesetzentwurf geäußerte Einschätzung, dass die Änderungen im LIFG verfassungsrechtlich angezeigt sind und so zur Rechtssicherheit beitragen.

Darüber hinaus weisen sie auf ihre Änderungsvorschläge und Empfehlungen hin, die sie anlässlich der Evaluation des LIFG in einer gemeinsamen Stellungnahme im Jahr 2022 formuliert hatten und setzen sich weiterhin dafür ein, das LIFG im Sinne einer funktionierenden Verwaltung anzupassen bzw. zurückzuführen.

Der LfDI kritisiert, dass durch die Ausweitung der Bereichsausnahmen der Zugang zu amtlichen Informationen weiter beschränkt werde. Er hält die Aufnahme informationsbezogener Bereichsausnahmen für systemwidrig. Zusätzlich führe die Verwendung von unbestimmten Rechtsbegriffen und der weite Anwendungsbereich zu Schwierigkeiten bei der Rechtsanwendung und zu einem erhöhten bürokratischen Aufwand. Die vorgesehene Erweiterung der Bereichsausnahme zum Schutz der Wissenschaftsfreiheit hält der LfDI auch nach der Rechtsprechung des VGH BW für nicht erforderlich. Die Regelungslücke in Bezug auf das religionsgemeinschaftliche Selbstbestimmungsrecht und die Notwendigkeit, diese zu schließen, erkennt der LfDI hingegen grundsätzlich an. Eine entsprechende Regelung sollte aber in § 6 LIFG und nicht in § 2 LIFG erfolgen.

Die Regionalgruppe Baden-Württemberg von Transparency International Deutschland e.V. hält die vorgeschlagenen Erweiterungen der Bereichsausnahmen zum Schutz der Kunst- und Wissenschaftsfreiheit sowie des religionsgemeinschaftlichen Selbstbestimmungsrechts im Hinblick auf die zitierte Rechtsprechung des VGH BW für nachvollziehbar. Gleichzeitig fordert die Regionalgruppe, das Informationszugangsrecht zu reformieren und verweist insofern auf ihren zusammen mit dem Landesverband „Mehr Demokratie e.V.“ im Februar 2021 verfassten Vorschlag für ein Transparenzgesetz.

Die Universität Freiburg setzt sich dafür ein, dass sich weiterhin aus dem Gesetzestext – und nicht lediglich aus der Gesetzesbegründung – ergibt, dass Leistungsbeurteilungen und Prüfungen der Hochschulen vom Informationszugang ausgenommen sind.

Die Universität Tübingen sowie das KIT begrüßen die Intention der Neuregelung zur Kunst- und Wissenschaftsfreiheit, befürchten jedoch durch das Hinzutreten des Begriffs der „Freiheit“ in der Neuregelung ein Absenken des Schutzniveaus zu Lasten der Kunst- und Wissenschaftsfreiheit sowie Unsicherheiten in der Rechtsanwendung. Es wird vorgeschlagen, stattdessen die bisherige stellenbezogene Bereichsausnahmeregelung beizubehalten und um die „zuständige Behörde gemäß § 8 Absatz 1 Tierschutzgesetz“ zu erweitern.

3. Änderungen aufgrund des Ergebnisses der Anhörung

Aufgrund der vorgebrachten Einwände und Anregungen wurden folgende inhaltliche Änderungen des Gesetzentwurfs vorgenommen.

Zu Artikel 1 § 2

- Die GPA wird neben dem Rechnungshof in die Vorschrift aufgenommen. Nach § 113 Absatz 1 Satz 2 der Gemeindeordnung (GemO) handelt die GPA im Auftrag der Rechtsaufsichtsbehörde unter eigener Verantwortung. In Bezug auf diese Unabhängigkeit ist ihre Prüftätigkeit der des Rechnungshofs vergleichbar.

Zu Artikel 1 § 4

Als Absatz 2 Satz 2 wird die Ermächtigung zur Anonymisierung und zur Herstellung synthetischer Daten auf die besonderen Kategorien personenbezogener Daten erstreckt.

Zu Artikel 1 § 6

- In Absatz 2 Nummer 3 wird eine redaktionelle Klarstellung in Bezug auf die Verteidigung gegen Rechtsansprüche Dritter vorgenommen.

- In Absatz 3 wird klargestellt, dass Absatz 3 für die Übermittlung an Stellen der genannten Länder gilt. Der Begriff „öffentliche Stellen“ ist zu vermeiden, da er in § 2 Absatz 1 als solche des Landes legal definiert ist.

Zu Artikel 1 § 7a

- In die Verordnungsermächtigung des § 7a des Gesetzentwurfs wird der Bezug auf Absatz 1 ergänzt, um die Nichtanwendbarkeit für die Hochschulen auch hier klarzustellen.

Zu Artikel 1 § 8

- Wegen der im Forschungsbereich häufig nicht angezeigten Information der betroffenen Person bei Erhebung der Daten wird in Absatz 2 die Nummer 5 des Absatz 1 gestrichen. Dies hebt nicht die Verpflichtung auf, sobald wie möglich die Information zu erteilen bzw. nachzuholen.

Zu Artikel 1 § 13 Absatz 5

- Es wird präzisiert, dass die übermittelnde Stelle befähigt werden muss, Nachweise über die Einhaltung der vom Datenempfänger zu übernehmenden Verpflichtungen zu fordern.

Zu Artikel 1 § 15

- In Absatz 2 Satz 2 wird ein Bezug auf Satz 1 eingefügt, um zu verdeutlichen, dass für diese Alternative ebenfalls Voraussetzung für die Verarbeitung ist, dass kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

- In Absatz 6 wird entsprechend den Begrifflichkeiten der DSGVO die ausdrückliche Einwilligung statt „Zustimmung“ in der entsprechenden Alternative verlangt.

Zu Artikel 1 § 17a Absatz 2

- Entsprechend der Regelung in § 15 Absatz 6 wird in Bezug auf die Authentifizierung klargestellt, dass die biometrischen Daten nicht zu anderen Zwecken verarbeitet werden dürfen.

Zu Artikel 1 § 18

- In Absatz 1 wird die Beschränkung auf den Schutz bestimmter Objekte und Personen (bisher Absatz 1 Nummern 1 und 2) aufgehoben.

- In Absatz 2 wird die Informationspflicht konkretisiert. Es ist „darauf hinzuweisen, wo die weiteren Informationen des Verantwortlichen nach Artikel 13 der Verordnung (EU) 2016/679 vom Verantwortlichen verfügbar sind.“

- In Absatz 6 wird die Videoüberwachung unter Nutzung von KI-Systemen geregelt; neben die bisherige Alternative tritt der Schutz von Leib oder Leben von Personen als weiterer Anwendungsfall.

Zu Artikel 2 § 17a

- In Absatz 1 wird die Ermächtigung um die Formulierung „und nach erfolgreicher Erprobung der Zulassung“ ergänzt, um die Zweckbestimmung des § 17a präziser zu

fassen, da er neben der Erprobung auch der Zulassung des automatisierten Erlasses von Verwaltungsakten nach deren erfolgreicher Erprobung dient.

- In Absatz 2 wird der Entwurf für Nr. 4 durch die folgende Formulierung ersetzt: „kein Anlass besteht, den Einzelfall durch Amtsträger zu bearbeiten, da die vorliegenden Informationen und die Angaben derjenigen, für die der Verwaltungsakt bestimmt ist oder die von ihm betroffen werden, keine vom Regelfall abweichenden Hinweise enthalten.

- In Absatz 3 und 4 erfolgt die Ergänzung um den Begriff „oder der zuständigen Rechtsaufsichtsbehörde“, um beispielsweise bei Körperschaften des öffentlichen Rechts wie den Berufskammern, die keine Fachaufsicht haben, eine zuständige Behörde festzulegen.

Zu Artikel 4 § 2 Absatz 3

- Entsprechend dem Vorschlag der Universität Freiburg wird der bisherige Gesetzeswortlaut der Regelung in § 2 Absatz 3 Nummer 2 LIFG in Bezug auf „Leistungsbeurteilungen und Prüfungen“ aus Gründen der Rechtssicherheit beibehalten und es werden dementsprechend weiterhin alle Stellen, die sich auf die Bereichsausnahme berufen können sollen, dort aufgezählt.

- Dem Einwand der Universität Tübingen sowie des KIT entsprechend, wird auf die Verwendung des Begriffs der „Freiheit“ in der Neuregelung des § 2 Absatz 3 Nummer 5 LIFG verzichtet; hierdurch soll verhindert werden, dass Unsicherheiten in der Rechtsanwendung zu einem nicht bezweckten Absenken des Schutzniveaus zu Lasten Kunst- und Wissenschaftsfreiheit im Vergleich zur bisherigen Regelung führen.

4. Behandlung der sonstigen erheblichen Einwände und Anregungen

Von den Verbänden und Institutionen wurden außerdem folgende wesentlichen Anregungen oder Einwände vorgebracht, die nicht zu Änderungen des Gesetzentwurfs geführt haben.

a) Zur Änderung des LDSG

Zu § 2

Zu Absatz 1

- Die KLV schlagen vor, statt auf ein „anderes Gesetz“ direkt auf § 67 Absatz 4 SGB X zu referieren, um die Transparenz zu erhöhen. Der LfDI hält die Regelung für entbehrlich; dies ergebe sich bereits aus dem Vorrang anderer Gesetze nach § 2 Absatz 3.

Haltung der Landesregierung

Die Regelung wird beibehalten. Sie trägt eher dazu bei, den Verantwortlichen genau zu bestimmen.

Zu Absatz 5

- Der LfDI bezweifelt die Gesetzgebungskompetenz für die Nutzung von KI in der Justiz. Diese müsste vom Bundesgesetzgeber in den Prozessordnungen geregelt werden. Auch sei fraglich, ob die Erprobung von Systemen der KI der justiziellen Tätigkeit zuzurechnen sei. Der Anwaltsverband stellt ebenfalls die Frage nach der Verortung der Norm. Wegen der kompetenzrechtlichen Bedenken und der grundlegenden Bedeutung der Justizgrundrechte spricht sich der Anwaltsverband BW dagegen aus, den Einsatz von KI im justiziellen Bereich im LDSG zu regeln.

Haltung der Landesregierung

Die Auffassung des LfDI wird nicht geteilt. Auch der Bundesgesetzgeber scheint nicht davon auszugehen, dass die Prozessordnungen stets abschließend sind. In dem Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 (BT-Drucksache 19/4671) wird etwa zur Strafprozessordnung ausgeführt: „Soweit die StPO eigene, nicht abschließende datenschutzrechtliche Vorschriften enthält, treten sie ergänzend neben die allgemeinen Regelungen des BDSG (2018)“ (a.a.O., S. 44). Des Weiteren wird zum Einführungsgesetz zum Gerichtsverfassungsgesetz wie folgt ausgeführt: „Für den Bereich der Richtlinie (EU) 2016/680 besteht insoweit kein Regelungsbedarf; hier stellen die §§ 12 ff. EGGVG und insbesondere § 21 EGGVG eine bereichsspezifische Sonderregelung des Datenschutzes dar, die nach § 1 Absatz 2 Satz 1 BDSG (2018) den Vorschriften des BDSG (2018) als Lex Specialis vorgehen. Sie genügen als Sonderbestimmungen für die Übermittlung personenbezogener Daten mit Zweckänderung den Anforderungen des Artikels 4 Absatz 2 der Richtlinie (EU)

2016/680“ (a.a.O., S. 52). Es wird demnach ausdrücklich klargestellt, dass es sich um Sonderbestimmungen (ausschließlich) für die Übermittlung personenbezogener Daten handelt (vgl. auch Lückemann in: Zöller, Zivilprozessordnung, 36. Auflage, 10/2025, Vorbemerkungen zu §§ 12-22 EGGVG, Rn. 1 am Ende). Zuletzt wird im Anschluss an die Änderungen der Prozess- und Verfahrensordnungen die subsidiäre Geltung des Bundesdatenschutzgesetzes klargestellt: „Soweit in spezifischen Rechtsvorschriften des Bundes oder in landesrechtlichen Regelungen keine besonderen Beschränkungen der Pflichten und Rechte nach den Artikeln 12 bis 22, Artikel 34 und Artikel 5 der Datenschutz Grundverordnung enthalten sind, gelten im Bereich der justiziellen Tätigkeit der Gerichte und Justizbehörden subsidiär die im BDSG (2018) enthaltenen allgemeinen Beschränkungen (§ 1 Absatz 1 Satz 1 in Verbindung insbesondere mit den §§ 32 ff. BDSG (2018))“ (a.a.O., S. 53).

Des Weiteren soll nochmals betont werden, dass die KI-Reallabore als Sonderregelung angesehen werden und Artikel 57 Absatz 10 KI-VO grundsätzlich nicht die Justiz betrifft. Soweit Erprobungen im Echtbetrieb durchgeführt werden, ist die richterliche Unabhängigkeit betroffen und eine Aufsicht des LfDI nach Artikel 55 Absatz 3 DSGO ausgeschlossen. Dabei ist die sehr weite Auslegung des EuGH in seinem Urteil vom 24.03.2022 – C-245/20 –, das der LfDI selbst genannt hat, zugrunde zu legen. Hiernach sind „Verarbeitungsvorgänge von der Zuständigkeit der Aufsichtsbehörde ausgeschlossen (…), deren Kontrolle durch diese Behörde mittelbar oder unmittelbar die Unabhängigkeit der Mitglieder oder der Entscheidungen der Gerichte beeinflussen könnte.“ Eine Kontrolle von Softwaretests ist zwangsläufig auf deren Funktionsweise und die Frage, ob und wie die Anwendung genutzt werden kann, gerichtet, wodurch eine Aufsichtsbehörde zumindest mittelbar Einfluss auf die richterliche Unabhängigkeit erlangen würde.

Den Ausführungen des Anwaltsverbands, dass es vorrangig nicht um Datenschutzrecht, sondern um das Recht auf ein faires rechtsstaatliches Verfahren gehe, wird widersprochen. Im Landesdatenschutzgesetz werden weiterhin ausschließlich Aspekte des Datenschutzes normiert. Die aufgeworfenen Fragestellungen sind an anderer Stelle zu behandeln. Beispielsweise sei auf die Strategie für den Einsatz von Künstlicher Intelligenz in der Justiz, am 2. April 2025 durch den E-Justice-Rat verabschiedet, hingewiesen.

Der Umstand, dass teilweise dieselben gesetzlichen Regelungen für die Verwaltung und die Justiz gelten, verletzt den Grundsatz der Gewaltenteilung nicht.

Zu den allgemeinen Ausführungen, dass der Einsatz eines algorithmischen Systems anstelle eines Richters als natürliche Personen zur abschließenden Entscheidungsfindung unzulässig sei, wird auf den auf den Erwägungsgrund 61 der KI-VO verwiesen, der die folgende Textpassage beinhaltet: „Der Einsatz von KI-Instrumenten kann die Entscheidungsgewalt von Richtern oder die Unabhängigkeit der Justiz unterstützen, sollte sie aber nicht ersetzen; die endgültige Entscheidungsfindung muss eine von Menschen gesteuerte Tätigkeit bleiben.“ Der Einsatz von KI in der Justiz orientiert sich streng an den Normen und Erwägungsgründen der KI-VO. Die Justiz setzt lediglich auf Assistenzsysteme, die die Justizangehörigen unterstützen, jedoch selbst keine endgültigen Entscheidungen treffen wird.

Zu § 2a

- Vom NKR sowie den KLV wird die Anführung von neun EU-Vorschriften kritisiert, da diese die Nutzerfreundlichkeit und Transparenz störe.

- Vom LfDI, vom BWIHK, von der Komm.ONE und vom Universitätsklinikum Heidelberg wird die Definition synthetischer Daten vermisst.

Haltung der Landesregierung

Die Anregungen werden nicht aufgegriffen. Es handelt sich um die Angabe der amtlichen Bezeichnung der KI-VO, die bei der ersten Zitierung vorgeschrieben ist.

Die neu eingefügten Begriffsbestimmungen in § 2a dienen der Einheit der Rechtsordnung durch Verweisung auf bereits bestehende Begriffsbestimmungen. Demgegenüber hat sich für den unbestimmten Rechtsbegriff der synthetischen Daten noch keine allgemein anerkannte Definition herausgebildet, die übernommen werden könnte. Eine gesetzliche Definition sollte daher aktuell noch vermieden werden.

Absatz 3

- Der LfDI kritisiert die Erweiterung der Definition von KI-Modellen um solche mit speziellen Verwendungszwecken. Dies stehe im Widerspruch zur KI-VO.

Haltung der Landesregierung

Die Ausführungen hinsichtlich der gebotenen Abgrenzung GPAI und KI-Systemen werden als zwar richtig beurteilt, verkennen aber, dass es hier nicht um den Unterschied zwischen GPAI und KI-Systemen, sondern um den Unterschied zwischen GPAI und KI-Modellen mit speziellem Verwendungszweck geht. Ein KI-Modell mit speziellem Verwendungszweck ist kein KI-System.

Zu § 3

- Die KLV kritisieren die neu eingefügte Nummer 6: Abschottung von internen Systemen vor unbefugten Zugriffen des öffentlichen Telekommunikationsnetzes“. Es sei annähernd unmöglich, einen kommunalen Arbeitsplatz vom Internet zu trennen. Angeregt wird eine Konkretisierung, beispielsweise, den Begriff „Abschottung“ durch „den geeigneten technischen Schutz“ zu ersetzen.

Haltung der Landesregierung

Der Vorschlag wird nicht übernommen, denn „der geeignete technische Schutz“ stellt keine Konkretisierung der technischen und organisatorischen Maßnahmen dar, die über das ohnehin bereits geltende Verhältnismäßigkeitsprinzip hinausgeht. Im Übrigen wird der Begriff der Abschottung in der Begründung ausreichend erläutert. Dort werden beispielhaft VLAN und Firewall als technische Maßnahmen der physischen Trennung erwähnt.

Zu § 3a

Stellungnahmen der Universitätskliniken Freiburg und Heidelberg, ZENDAS, LRK-PH, LfDI, KIT, BWIHK, Anwaltsverband BW

- Das Universitätsklinikum Freiburg begrüßt die Regelung und regt an, dass der Gesetzgeber oder die Aufsichtsbehörden konkrete Hilfsmittel (z. B. Prüfleitfäden oder Standardanforderungen) bereitstellen.

- Das Universitätsklinikum Heidelberg begrüßt die Regelung, jedoch könne die Klausel expliziter darauf eingehen, dass neben den allgemeinen Datenschutzvorschriften besonderen Anforderungen an den Einsatz von KI gelten würden. Überdies könnte man ggf. einen klareren Verweis auf die Gesetze hinzufügen, welche in diesem Kontext relevant seien.

- Der LfDI betont, dass KI-Tools nicht ausschließlich als einfache Betriebsmittel betrachtet werden sollten, denn ein wesentlicher Unterschied bestehe beispielsweise darin, ob ein KI-System mit personenbezogenen Daten (nach-)trainiert werde oder nicht. Ein pauschaler Erlaubnistatbestand könne keinesfalls die im Einzelfall erforderliche Abwägung ersetzen, um zu klären, ob die Verarbeitung eine erforderliche und verhältnismäßige Maßnahme darstelle (Wesensgehaltsgarantie im Grundrechtsschutz) und welche technischen sowie organisatorischen Maßnahmen erforderlich seien. Ein möglicher Ansatz könnte darin bestehen, dass KI-Systeme und KI-Modelle mit einer nicht nur geringen Eingriffsintensität zunächst zwingend in einem Reallabor geprüft werden müssten. Sollte die Nutzung der KI jedoch weiterhin mit einem hohen Risiko verbunden sein, wäre ein spezifisches parlamentarisches Gesetz erforderlich.

- Das KIT sowie ZENDAS regen an, § 3a LDSG als eigenständige umfassende Rechtsgrundlage auszugestalten. Nach Ansicht der DHBW hat die Regelung nur deklaratorische Wirkung.

- Der BWIHK regt an, einen „klarstellenden Verweis“ in § 3a auf § 11a aufzunehmen.

- Der Anwaltsverband BW kann nicht erkennen, dass in § 3a die wesentlichen datenschutzrechtlichen Fragen nach dem Verantwortlichen, der Rechtsgrundlage, den Schutzmaßnahmen, der Einhaltung der Grundsätze der Datenverarbeitung, der Datenschutz-Folgenabschätzung, der Betroffenenrechte, der Information der Betroffenen, der Drittlandübertragung und der Kategorien verwertbarer Daten ausreichend berücksichtigt wurden.

Haltung der Landesregierung

Die Aufsichtsbehörden werden prüfen, inwieweit konkrete Hilfsmittel bereitgestellt werden können. Im Übrigen werden die Anregungen nicht aufgegriffen.

Explizitere Klauseln und Verweise würden den Gesetzestext unübersichtlich machen und bieten die Gefahr, dass sie regelmäßig umfangreich zu aktualisieren wären.

Nur wenn kein (Nach-)Training des KI-Systems stattfindet, soll § 3a die Nutzung von KI-Systemen als Betriebsmittel legitimieren; ansonsten bedarf es daneben das Vorliegen der Voraussetzungen des § 11a. Falls bei einem KI-System das Risiko (noch) nicht eingeschätzt werden kann, erweist sich dazu ein Test in einem KI-Reallabor in der Regel mit Beteiligung des LfDI als sinnvolles Mittel zur

Risikobewertung. Das Erfordernis von geeigneten technischen und organisatorischen Maßnahmen ergibt sich bereits aus § 3. Die Nutzung der KI trotz verbleibenden hohen Risikos, welche durch ein parlamentarisches Gesetz legitimiert werden sollte, dürfte wenig praxisrelevant sein.

Durch die Möglichkeit, ergänzend auf die bereits in der Praxis bewährte Regelung in § 4 sowie sonstige Regelungen, die eine Datenverarbeitung erlauben, zurückzugreifen, wird eine umfassende Rechtsgrundlage geschaffen.

Ein „klarstellender Verweis“ in § 3a auf § 11a ist nicht sinnvoll, weil die Nutzung von KI-Systemen nach § 3a unabhängig von Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen nach § 11a ist. Lediglich wenn die Daten aus der Nutzung von KI-System gleichzeitig zum Training eines KI-Modells verwendet werden, sind für das Training des KI-Modells die Voraussetzungen des § 11a zu prüfen.

Die vom Anwaltsverband BW aufgezeigten Aspekte sind in der DSGVO, KI-VO bzw. im LDSG mit den vorgeschlagenen Änderungen berücksichtigt.

Zu § 4

- Die KLV regen an, den neuen Absatz 2 in einen neuen § 4a zu überführen, damit nicht eine Vielzahl von Datenschutzerklärungen angepasst werden müssten. Der Anwaltsverband BW begrüßt die Regelung

Haltung der Landesregierung

Der Vorschlag wird nicht aufgegriffen. Die Regelung des neuen Absatz 2 steht systematisch in Zusammenhang mit dem bisherigen § 4, der in Absatz 1 übernommen wird, da die Zulässigkeit der Verarbeitung personenbezogener Daten geregelt wird. Außerdem wird davon ausgegangen, dass eine Anpassung der Datenschutzerklärung bei der turnusmäßigen Überprüfung der Erklärung erfolgen kann.

Absatz 2

Stellungnahmen der BWIHK, DHBW, LfDI, ZENDAS, Universitätskliniken Freiburg und Ulm

- Der LfDI vertritt die Ansicht, dass die Norm inhaltlich unbegrenzt bleibe, was seines Erachtens sowohl mit Blick auf die Normenklarheit, die Voraussetzungen einer Rechtsgrundlage nach Artikel 6 Absatz 3 DSGVO als auch den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz unzulässig sei. Es bestehe ein Wertungswiderspruch zum Umgang mit Statistikdaten, für die eine Reihe besonders strenger Vorgaben gelten, während hier jedoch keinerlei besondere Schutzmaßnahmen für den Anonymisierungs-/Synthetisierungsprozess genannt seien. Er empfiehlt deswegen, die Erlaubnis zur Erstellung von anonymen und synthetischen Daten an die Zwecke der Forschung oder der KI-Entwicklung zu binden und in den entsprechenden Vorschriften in Form eines Stufenkonzepts zu ergänzen. Ansonsten erlaube der Zweck der Datenminimierung es global, Daten zu jedem erdenklichen Zweck zu anonymisieren oder zu synthetisieren. Zusätzlich sollte ein Verfahren zur regelmäßigen Überprüfung der Anonymität der Daten vorgeschrieben werden.

- Die DHBW regt die Klarstellung an, ob die Formulierung „zum Zweck der Datenminimierung“ eine Einschränkung dergestalt bedeutet, dass nur zu diesem Zweck (d.h. anstelle einer Löschung) anonymisiert werden darf und nicht etwa, um eine Kopie eines Datenbestandes anzufertigen und diese nach Anonymisierung zu Forschungszwecken (Forschung wird zumindest in der Begründung genannt) oder dem Training eines KI-Modells weiterzuverwenden. Auch wird um Klarstellung gebeten, ob die Herstellung von synthetischen Daten ein Unterfall der Anonymisierung sei.

- Der BWIHK regt an, die § 4 Absatz 2 LDSG dahingehend zu erweitern, dass auch aus pseudonymisierten Daten synthetische Daten hergestellt werden können.

Haltung der Landesregierung

Die Empfehlung des LfDI, die Erlaubnis zur Erstellung von anonymen und synthetischen Daten an die Zwecke der Forschung oder der KI-Entwicklung zu binden, wird nicht aufgegriffen. Anonyme Daten werden entsprechend dem Grundsatz der Datenminimierung auch in anderen Kontexten benötigt (etwa, wenn bei personenbezogenen Akten deren Anzahl ermittelt wird, um die Einhaltung bestimmter Kennzahlen festzustellen). Artikel 6 Absatz 3 DSGVO wird genügt, indem der Zweck der Datenminimierung angegeben wird und die Regelung des § 4 Absatz 2 auch unter Berücksichtigung der Sicherstellung des Datenschutzes nach § 3 und der Regelungen über die Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO anzuwenden ist. Zwar sind die Voraussetzungen der Rechtsgrundlage sehr weit

formuliert, aber durch eine Anonymisierung bzw. Synthetisierung wird allenfalls marginal in die Rechte der Betroffenen eingegriffen, so dass dem Verhältnismäßigkeitsgrundsatz genüge geleistet ist. Die vom LfDI gewünschte Pflicht zur regelmäßigen Überprüfung der Anonymität der Daten besteht immer, wenn vermeintlich anonyme Daten weiterverarbeitet werden.

Der von der DHBW anregten Klarstelllungen bedarf es nicht. Eine Anonymisierung „zum Zwecke der Datenminimierung“ bedeutet nicht, dass dies anstelle einer Löschung erfolgen müsste. Der Zweck der Datenminimierung wird bei einer Anonymisierung auch erfüllt, wenn der bisherige Datenbestand für den ursprünglichen Zweck weiterverwendet wird und die anonymisierten Daten für das Training eines KI-Modells verwendet werden sollen. Das Ergebnis der Herstellung von synthetischen Daten und Anonymisierung ist identisch, weil in beiden Fällen danach anonyme Daten vorliegen. Die Herstellung von synthetischen Daten ist aber in der Regel aufwändiger als eine normale Anonymisierung.

Die Anregung des BWIHK wird nicht aufgegriffen, weil pseudonymisierte Daten bereits von der Regelung des § 4 Absatz 2 LDSG erfasst werden.

Zu § 5

- Der LfDI hegt Zweifel an der Europarechtskonformität von Absatz 1 Nummer 1, da es an der Festlegung konkreter Zwecke und Ziele der Verarbeitung fehle.

Haltung der Landesregierung

Aus der Gesetzesformulierung ergibt sich, dass nicht irgendwelche für gut befundene öffentliche Interessen die Zweckänderung rechtfertigen können, sondern nur gesetzlich anerkannte allgemeine öffentliche Interessen. Solche können beispielsweise der Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) entnommen werden.

Zu Absatz 1 Nummer 5

- Der LfDI bewertet die neue Nummer 5 als staatliche Bevormundung. Es sollte die Einwilligung der betroffenen Person zur zweckändernden Verarbeitung eingeholt werden.

Haltung der Landesregierung

Die Regelung wird beibehalten. Sie stellt eine Erleichterung sowohl für die Bürgerinnen und Bürger als auch für die Verwaltung dar.

Zu § 6

- Der LfDI hält die Regelung des Absatz 5 für zu unbestimmt. Er sieht keine Notwendigkeit einer Generalklausel für gemeinsame Dateien.

- Das Universitätsklinikum Tübingen hält die Verlagerung der Verantwortung bei automatisierten Abrufen ausschließlich auf die abrufende Stelle für eine Verletzung der Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO.

Haltung der Landesregierung

Die Regelung wird für normenklar gehalten. In der Praxis kann sich ein Bedürfnis für gemeinsame Dateien ergeben, wenn verschiedene öffentliche Stellen gemeinsam in einer Datei arbeiten. Dies kann eine erhebliche Arbeitserleichterung darstellen. Die Vorschrift sieht ausdrücklich Schutzmaßnahmen zugunsten der betroffenen Personen vor.

Die Verantwortung für die Rechtmäßigkeit des einzelnen Abrufs muss dem abrufenden Dritten obliegen, da die Rechtmäßigkeit dieser Datenerhebung in seiner Verantwortungssphäre liegt.

Zu § 7a

- Die KLV regen die Erstreckung der Regelung auf Auftragsverarbeitung durch kommunale Stellen an. Erwähnt werden die Leistungen der Kommunen, die für die Schulen erbracht werden, Jagdkataster und Geoinformationsdienste für kreisangehörige Gemeinden.

- ZENDAS stellt die Frage, ob Absatz 3 für Hochschulen anwendbar ist und wünscht eine Klarstellung im Gesetz.

- Der BWIHK sowie der NKR vermuten Gold-Plating hinter der vorgesehenen Ersetzung einzelvertraglicher Regelungen durch gesetzlich festgelegte Nutzungsbedingungen. Sie stellen die Frage, wozu es dieser überhaupt bedürfe,

wenn sich der Inhalt der bisherigen Auftragsverarbeitungsverträge ohnehin aus Artikel 28 DSGVO ergebe. Unklarheit besteht in Bezug auf den Bestand bestehender einzelvertraglicher Regelungen.

Haltung der Landesregierung

Der Vorschlag der KLV wird nicht aufgegriffen. Die Vorschrift des § 7a betrifft die Auftragsverarbeitung durch staatliche Behörden, also die unmittelbare Landesverwaltung (z. B. BITBW) oder Anstalten des öffentlichen Rechts in alleiniger Trägerschaft des Landes (z. B. L-Bank). Hier besteht das berechtigte Interesse an der Vereinheitlichung der Auftragsverarbeitungsverträge. Es ist nicht ersichtlich, dass das Land die Auftragsverarbeitungsverträge der Kommunen interessengerecht gestalten könnte. Ggf. können die Kommunen eigene Musterverträge entwickeln.

Nach Auffassung der Landesregierung ist Absatz 3 nicht auf die Hochschulen anwendbar, da die Hochschulen nach dem Landeshochschulgesetz nicht der Fachaufsicht unterliegen.

Die Anforderungen an die Auftragsverarbeitung müssen nach Artikel 28 Absatz 3 DSGVO vertraglich oder auf Grundlage eines anderen Rechtsinstruments geregelt werden. Im Übrigen verbleibt auch nach § 7a die Freiheit, es bei bisherigen abweichenden Vertragsregelungen zu belassen, wenn diese Artikel 28 DSGVO entsprechen.

Zu § 8

- Der BWIHK sieht Absatz 2 als zusätzliche bürokratische Informationspflicht. Die Vorschrift wird vom NKR ebenso abgelehnt.

Haltung der Landesregierung

Die Regelung wurde eingefügt, um den Anforderungen des Artikels 23 Absatz 2 DSGVO zu entsprechen. Die Informationspflicht kann durch Aufnahme der Information in die Webseite, auch in abstrakt-genereller Form, erfüllt werden.

Zu §§ 9a, 10 Absatz 4

Stellungnahmen der ARGE-HPR, des Anwaltsverbands BW, BBW, BWIHK, NKR, Rechtsanwaltskammer Stuttgart, ZENDAS, Universitätskliniken Freiburg und Heidelberg,

- Die Regelung wird vom NKR, vom BWIHK und der DHBW sowie dem Universitätsklinikum Freiburg mit kleinen Einschränkungen positiv bewertet. Ähnlich kann das Universitätsklinikum Freiburg die Regelung „nachvollziehen“. ZENDAS begrüßt die Regelung für die Praxis und hat dabei allerdings auch rechtliche Bedenken. Im Übrigen wird vielfach kritisiert, dass der Berichtigungs- und Löschungsanspruch eingeschränkt wird. Dies sei in Bezug auf den Verhältnismäßigkeitsgrundsatz problematisch. Filterung bedeute außerdem eine zusätzliche problematische Datenverarbeitung. Die Betroffenenrechte am verhältnismäßigen Aufwand festzumachen, wird teils für eine unangemessene Belastung der betroffenen Personen gehalten. Teils wird die Unbestimmtheit der zu treffenden Maßnahmen kritisiert. Es fehle am Maßstab für die Beurteilung der Verhältnismäßigkeit

Im Einzelnen:

- Nach Ansicht der ARGE-HPR sollte zum hohen Schutz der personenbezogenen Daten ausgeschlossen werden, dass solche KI-Systeme/KI-Modelle mit personenbezogenen Daten trainiert würden, solange eine Korrektur fehlerhafter personenbezogener Daten in KI-Systemen oder KI-Modellen technisch nicht vorgesehen sei. Der nachträgliche Einbau von Filtern zur Berichtigung oder sonstige geeignete Maßnahmen, um entsprechende Mängel unschädlich zu machen, erscheine sehr aufwändig und in einer KI-Anwendung nicht sicher und dauerhaft umsetzbar.

- Der BBW und die Rechtsanwaltskammer Stuttgart bewerten die Beschränkung des Rechts auf Berichtigung durch § 9a und Löschung durch § 10 Absatz 4 kritisch. Nach Ansicht des BBW sollte vielmehr „der Gesetzgeber durch verbindliche Vorgaben zu Transparenz, Nachvollziehbarkeit und technischen Mindeststandards sicherstellen, dass das Berichtigungsrecht auch im Kontext von KI-Systemen tatsächlich durchgesetzt werden kann.“ Nach Ansicht der Rechtsanwaltskammer Stuttgart bestünden Zweifel, inwieweit der Einsatz von KI „unverzichtbar“ sei. Ein überwiegendes öffentliches Interesse am Einsatz von KI in der Verwaltung könne der Gesetzentwurf nicht begründen, zumal nicht dargelegt werde, wie sichergestellt werden solle, dass eine Verwaltungsentscheidung nicht auf eine unrichtige Ein- oder Ausgabe der KI gestützt werde.

- Die Universitätskliniken Freiburg und Heidelberg regen eine präzise Definition des „unverhältnismäßig hohen Aufwands“ an. Umgekehrt regt die DHBW an, die an Stelle der Berichtigung tretenden Filter oder sonstigen geeigneten Maßnahmen als zwingende Voraussetzungen festzulegen und eine Dokumentationspflicht aufzunehmen, wenn Betroffenenrechte nicht umgesetzt werden können.

- ZENDAS äußert Zweifel daran, dass die Beschränkung der Betroffenenrechte verhältnismäßig sei, insbesondere, weil für die Filterlösung eine weitere Datenverarbeitung erforderlich sei. Auch seien in der Praxis für betroffene Personen bei der vorgesehenen Regelung Auseinandersetzungen mit Verantwortlichen darüber zu befürchten, ob der Aufwand für eine Maßnahme verhältnismäßig sei oder nicht. Sofern diese rechtlichen Bedenken gegen die Beschränkung der Rechte nicht geteilt würden, wird darum gebeten, auch eine entsprechende Beschränkung des Auskunftsrechts aufzunehmen.

- Das Universitätsklinikum Heidelberg regt außerdem noch an, weitere konkrete Beispiele für geeignete Maßnahmen neben einem Filter zu nennen.

- Das Universitätsklinikum Tübingen bewertet die Regelugen als unionsrechtswidrig und unbestimmt und schlägt eine Regelung unter Verweisung auf Artikel 23 DSGVO insgesamt – und bei der Löschung außerdem insgesamt auf Artikel 17 DSGVO – vor.

- Der LfDI erachtet die Voraussetzungen des Artikel 23 Absatz 1 DSGVO nur dann als erfüllt an, wenn die Anwendung von KI in der Verwaltung unverzichtbar sei, um effizient, in der gebotenen Qualität und ressourcenschonend die gesetzlichen Aufgaben zu erfüllen. Dies solle in einem ergänzenden Satz 3 eingefügt werden: „Die Beschränkung aus Satz 1 gilt nur, wenn der konkrete Einsatz der KI, die einen Berichtigungsanspruch nicht oder nur eingeschränkt ermöglicht, unverzichtbar ist, um effizient, in der gebotenen Qualität und ressourcenschonend die gesetzlichen Aufgaben zu erfüllen.“

Speziell zur Löschung weist der LfDI darauf hin, dass eine im Extremfall unbeschränkte Speicherung mit den Anforderungen der DSGVO, die eine Speicherbegrenzung verlange, nicht vereinbar sei, weshalb für die Beschränkung des Rechts auf Löschung eine separate Regelung erfolgen solle.

- Der Anwaltsverband kann eine ausreichende Rechtfertigung für die Beschränkung des Betroffenenrechts beim Einsatz von KI nicht erkennen, weil es nach seiner Sicht einer gänzlichen Abschaffung solcher Ansprüche gleichkommen würde. Es scheine

doch eher um Bequemlichkeit zu gehen und Anreize zu fehlen, dass die öffentliche Verwaltung sorgfältiger arbeite und nur hochwertige KI einsetze. Die Unzulässigkeit der Beschränkung der Betroffenenrechte wird insbesondere daraus gefolgert, dass der BFH, Urteil vom 14.01.2025, Az. IX R 25/22, zum Auskunftsanspruch nach Artikel 15 DSGVO klargestellt habe, dass der Auskunftsanspruch nicht mit dem Argument des unverhältnismäßigen Aufwands verweigert werden dürfe.

Haltung der Landesregierung

Die Vorgaben an Transparenz, Nachvollziehbarkeit und technische Mindeststandards ergeben sich für KI-Systeme und KI-Modelle aus den verbindlichen Vorgaben der EU in der KI-VO und den Durchführungsakten. Ergänzende Regelungen des Landesgesetzgebers wären europarechtlich problematisch.

Mit den Änderungen soll das Landesrecht für die zukünftigen Herausforderungen wie den fortschreitenden Fachkräftemangel infolge des demografischen Wandels aufgestellt werden. Bis 2030 werden etwa nach Berechnungen von McKinsey (Action, bitte! Wie der öffentliche Sektor den Mangel an digitalen Fachkräften meistern kann, 2023) im öffentlichen Sektor rund 840.000 Vollzeit-Fachkräfte fehlen. Dementsprechend weist auch der Deutsche Städte und Gemeindebund darauf hin: „Digitale Lösungen wie Automatisierung und künstliche Intelligenz können dazu beitragen, die drohenden Folgen in vielen Bereichen abzumildern."

Der Einsatz von KI bedeutet nicht notwendigerweise, dass die bisherigen Methoden ineffektiv waren, sondern vielmehr, dass sich die Verwaltung – ebenso, wie dies in den letzten Jahren auch in der Anwaltschaft beobachtet werden konnte – dem technologischen Wandel anpasst. Der Entwurf zeigt, dass die Verwaltung stets nach Wegen sucht, ihre Arbeit zu verbessern und effizienter zu gestalten. Der Einsatz von KI ist ein logischer Schritt in dieser Entwicklung.

Öffentliche Stellen werden häufig KI-Modelle übernehmen und entweder nachtrainieren oder in KI-Systeme integrieren. Fehlerhaften personenbezogenen Daten dürften in den großen Sprachmodellen bereits enthalten sein, bevor öffentliche Stellen überhaupt mit dem Training beginnen. Für die bereits in den KI-Modellen vorhandenen fehlerhaften personenbezogenen Daten bedarf es einer Beschränkung der Berichtigungs-/Löschungsrechte, damit diese KI-Systeme einsetzbar bleiben.

Die Unzulässigkeit der Beschränkung von Berichtigungs-/Löschungsrecht lässt sich nicht aus der vom Anwaltsverband Baden-Württemberg zitierten Entscheidung des

BFH zum Auskunftsrecht ableiten. In der Entscheidung hat der BFH lediglich festgestellt, dass sich aus der DSGVO, der Regelung des § 32c der Abgabenordnung oder dem Rechtsgedanken des § 275 Absatz 2 des Bürgerlichen Gesetzbuches im konkreten Fall keine Beschränkung des Auskunftsanspruchs ergebe. Nicht entschieden wurde, inwieweit ein Gesetzgeber auf der Grundlage von Artikel 23 DSGVO die Betroffenenrechte einschränken kann.

Die Vorteile bei der Filterlösung durch diese Datenverarbeitung überwiegen aufgrund der gesetzlich nach § 9a Satz 4 (in Verbindung mit § 10 Absatz 4) festgelegten strengen Zweckbindung die Nachteile dieser Datenverarbeitung.

Filter zur Berichtigung bekannter fehlerhafter Ausgaben von KI-Modellen sind in kommerziellen Produkten regelmäßig integriert und an deren sicherer und dauerhaften Umsetzung bestehen keine durchgreifenden Zweifel.

Bei der Einschränkung der Betroffenenrechte wird dem Verhältnismäßigkeitsgrundsatz dadurch Rechnung getragen, dass der Berichtigungsanspruch (§ 9a) bzw. Löschungsanspruch (§ 10 Absatz 4) nur ausgeschlossen ist, „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“. Dadurch, dass an die Stelle der Berichtigung ein Filter oder sonstige geeignete Maßnahmen treten, erfolgt eine Abwägung des Interesses des Einzelnen an der Wahrnehmung seiner Betroffenenrechte mit dem erheblichen öffentlichen Interesse am Einsatz von KI. Aus dem Wortlaut des § 9a (in Verbindung mit § 10 Absatz 4) und dem Regelungszusammenhang mit Artikel 23 Absatz 1 Buchst. e DSGVO ergibt sich die Darlegungslast der öffentlichen Stelle, dass die Berichtigung bzw. Löschung „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“.

Die Frage des unverhältnismäßigen hohen Aufwands ist eine Frage des Einzelfalls, die nicht durch den Gesetzgeber präzise definiert werden kann.

Die Annahme der DHBW, dass die Implementierung von Filtern oder sonstigen geeigneten Maßnahmen in der Regel ohne erheblichen Aufwand möglich sei, wird geteilt. Daraus folgt allerdings nicht, dass auf das Merkmal der Verhältnismäßigkeit zu verzichten ist. Die angeregte Dokumentationspflicht bedarf keiner Regelung in §

9a, weil sich dies aus der allgemeinen Rechenschaftspflicht des Artikel 5 Absatz 2 DSGVO ergibt.

Eine entsprechende Beschränkung des Auskunftsrechts wird für nicht erforderlich bewertet, weil nicht ersichtlich ist, warum die Geltendmachung des Auskunftsrechts ähnlich schwerwiegende Folgen wie die Geltendmachung eines Berichtigungsanspruchs oder Löschungsanspruchs hätte.

Die Nennung weiterer geeigneter Maßnahmen neben Filtern kommt mangels bereits bekannter technischer Möglichkeiten nicht in Betracht. Die Formulierung sollte aber zukunftsoffen noch keine weiteren Möglichkeiten ausschließen. Sobald zukünftig im Einzelfall geeignetere Maßnahmen zur Verfügung stehen, sind diese je nach Beurteilung der Verhältnismäßigkeit des Aufwands zu ergreifen.

In der Stellungnahme des Universitätsklinikums Tübingen wird verkannt, dass mit den formulierten Voraussetzungen („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“) eine Konkretisierungsleistung in Bezug auf Artikel 23 Absatz 1 Buchst. e DSGVO vorgenommen wurde, die dessen Änderungsvorschlag mit einer pauschalen Verweisung auf Artikel 23 DSGVO (und Artikel 17 DSGVO) nicht erbringt. Überdies erscheint die vorgeschlagene Verweisung auf Artikel 17 DSGVO im Hinblick auf das unionsrechtliche Normwiederholungsverbot problematisch.

Die vom LfDI vorgeschlagene Ergänzung lässt sich nicht aus Artikel 23 DSGVO ableiten. Artikel 23 DSGVO stellt auf die konkrete Beschränkung des Betroffenenrechts ab, fordert aber nicht, dass das verwendete KI-System oder KI-Modell „unverzichtbar“ ist, „um effizient, in der gebotenen Qualität und ressourcenschonend die gesetzlichen Aufgaben zu erfüllen.“

Auch dem Vorschlag einer speziell für die Löschung ausformulierten Regelung wird nicht gefolgt. Artikel 23 DSGVO differenziert auch nicht zwischen den Betroffenenrechten der Berichtigung und der Löschung.

Zu § 11a

Stellungnahmen der BWIHK, DHBW, NKR, Universitätskliniken Freiburg und Heidelberg, Anwaltsverband BW

- Der BWIHK bewertet § 11a an sich als eine positive Regelung und wirft allerdings die Frage auf, ob neben der europäischen KI-VO diese Regelung erforderlich und kohärent sei. Außerdem geht der BWIHK davon aus, dass das Tatbestandsmerkmal „effektiv“ zu Auslegungsproblemen führen werde. Überdies würde die einschränkende Zweckbindung („… zum Zweck der Erfüllung von in der Zuständigkeit der öffentlichen Stelle liegenden Auflagen…“) dazu führen, dass die IHK keine KI-Modelle und KI-Systeme entwickeln könnte, wenn sie dafür personenbezogene Daten bräuchte, denn Forschung und Entwicklung wären – zumindest nach Lesart des BWIHK – nicht unbedingt eine IHK-Aufgabe. § 11a sei daher eine schärfere Regelung als die KI-VO und dieses sog. „Gold Plating“ werde abgelehnt. In diesem Sinne appelliert auch der NKR bei der Regelung des § 11a nicht über die Anforderungen der KI-VO an die Zweckbindung hinaus zu gehen.

- Der LfDI weist darauf hin, dass die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen, sofern eine nicht nur geringe Eingriffsintensität in die Rechte und Freiheiten betroffener Personen vorliegt, ausschließlich innerhalb eines Reallabors erfolgen sollte. Auch könne die Verlagerung der Zulässigkeitsprüfung auf die verantwortliche Stelle zu erheblicher Rechtsunsicherheit führen. Überdies könne ein pauschaler Erlaubnistatbestand keinesfalls die im Einzelfall erforderlich Abwägung ersetzen, ob die Verarbeitung eine erforderliche und verhältnismäßige Maßnahme darstelle und ob ggf. technische und organisatorische Maßnahmen erforderlich seien.

- Weitergehend regt die DHBW an, das in der Gesetzesbegründung enthaltene abgestufte Konzept zur Einhaltung des Grundsatzes der Datenminimierung auch in den Gesetzeswortlaut aufzunehmen, um einer ausufernden Nutzung personenbezogener Daten für das KI-Training entgegenzuwirken. Außerdem wird um Klarstellung gebeten, ob die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen mit personenbezogenen Daten nur für den Zweck erfolgen dürfe, für welchen die Daten ohnehin bereits verwendet würden oder ob damit auch andere, weitere Zwecke verfolgt werden dürften.

- Das Universitätsklinikum Tübingen schreibt, dass der Entwurf fehlerhaft auf „Art. 6 Abs. 1 i. V. m. Abs. 3 Buchst. b DSGVO“ verweise und das Training mit Gesundheitsdaten eine spezifische Rechtsgrundlage mit strengen Garantien brauche. Auch verlange der EU AI Act zudem eine Risikoklassifizierung von KI-Systemen sowie besondere Pflichten für Hochrisikosysteme, die im Entwurf nicht berücksichtigt seien. Außerdem schlägt es folgende Fassung vor: „Die Verarbeitung

personenbezogener Daten zum Training und zur Weiterentwicklung von KI-Systemen ist zulässig, wenn:

1. eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. e DSGVO besteht und durch Unionsrecht oder nationales Recht gedeckt ist,

2. bei besonderen Kategorien zusätzlich eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vorliegt,

3. geeignete Garantien nach Art. 89 DSGVO umgesetzt werden, insbesondere Pseudonymisierung

oder Anonymisierung,

4. eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) vor Beginn der Verarbeitung durchgeführt

wird,

5. die Anforderungen des EU AI Act, insbesondere hinsichtlich Risikoklassifizierung, Risikomanagement und Transparenz, eingehalten werden."

- Die Universitätskliniken Freiburg und Heidelberg begrüßen die Regelung. Das Universitätsklinikum Freiburg regt an, dass der Gesetzgeber oder die Aufsichtsbehörden konkrete Hilfsmittel (z. B. Prüfleitfäden oder Standardanforderungen zur Nachvollziehbarkeit lernender Systeme) bereitstellen.

- Der Anwaltsverband Baden-Württemberg vermisst bei § 11a eine Abwägung mit dem Aspekt, dass einmal in eine KI-Software eingegebene personenbezogene Daten möglicherweise nicht mehr extrahiert werden könnten, insbesondere, wenn sie fehlerhaft seien, ein Löschverlangen bestehe oder es um mehrschichtige KI gehe.

Haltung der Landesregierung

Die KI-VO trifft von wenigen Ausnahmen abgesehen (insbes. Artikel 10 Absatz 5) keine Regelungen zum Datenschutz. Dabei bleibt abzuwarten, wie sich die Diskussion zur Frage der analogen Anwendung von Artikel 10 Absatz 5 Satz 1 KI-VO auf nicht zielgerichtete Datenverarbeitung zum Zwecke des KI-Trainings entwickelt (in diesem Sinne Paal, Recht der Datenverarbeitung (RDV) 2025, 230, 237).

Jedenfalls schränkt § 11a den Einsatz von KI-Systemen und KI-Modellen nicht über die Anforderungen der KI-VO hinaus ein.

Eine datenschutzrechtliche Grundlage für eine öffentliche Stelle bedarf der Regelung einer Zweckbestimmung, wie sich aus Artikel 6 Absatz 3 Satz 2 DSGVO ergibt. Zur Erfüllung von in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben (z. B. Mitgliederverwaltung) können auf Basis von § 11a ein KI-Modell trainiert werden, wenn die übrigen Voraussetzungen vorliegen.

Der Stellungnahme des LfDI schließt sich die Landesregierung insofern an, als je nach Eingriffstiefe zu differenzieren ist; ein pauschaler Erlaubnistatbestand ist nicht bezweckt. Der risikobasierte Ansatz der DSGVO verlangt allerdings (auch), die dogmatische Konstruktion von Artikel 9 Absatz 1 DSGVO so zur Anwendung zu bringen, dass der Zweck der Norm – sprich der Schutz vor spezifischen Gefährdungen – nicht zu einer pauschalen Blockade risikoangepasster Verarbeitungsmodelle fehlgeleitet wird (Paal, Recht der Datenverarbeitung (RDV) 2025, 230, 236). Ein ausschließliches Training im Reallabor wird nicht für erforderlich gehalten. Gemäß Artikel 35 DSGVO ist die Konsultation der Datenschutzaufsicht bei riskanten Datenverarbeitungen vorgesehen.

Die Anregungen der DHBW werden nicht aufgegriffen. Das in der Gesetzesbegründung enthaltene abgestufte Konzept ergibt sich aus allgemeinen Grundsätzen und bedarf keiner ausdrücklichen Normierung in § 11a. Der Zweck, für den die Daten ohnehin bereits verwendet werden, ist ein anderer Zweck als die Entwicklung, das Training, das Testen, die Validierung oder Beobachtung von KI-Systemen und KI-Modellen.

Die Stellungnahme des Universitätsklinikums Tübingen weist zutreffend darauf hin, dass die Verweisung in der Begründung auf Artikel 6 Absatz 1 Buchst. e in Verbindung mit Absatz 3 Buchst. b DSGVO für die Verarbeitung von Gesundheitsdaten nicht ausreicht. Für Gesundheitsdaten ergibt sich eine spezifische Rechtsgrundlage aus § 11a Satz 2 in Verbindung mit Artikel 9 Absatz 2 DSGVO oder einer speziellen Rechtsgrundlage. Der Hinweis auf die Risikoklassifizierung von KI-Systemen, die im Entwurf nicht berücksichtigt sei, verkennt, dass die KI-VO unmittelbar gilt. Nummer 5 des Vorschlags Universitätsklinikums Tübingen missachtet außerdem das unionsrechtliche Normwiederholungsverbot. Den vorgeschlagenen Nummern 1 bis 4 fehlt eine Konkretisierung gegenüber den ohnehin geltenden Regelungen der DSGVO.

Der Aspekt, dass einmal in eine KI-Software eingegebene personenbezogene Daten möglicherweise nicht mehr extrahiert werden können, wurde bei § 9a bzw. § 10 Absatz 4 insoweit berücksichtigt, als Betroffene anstatt der Berichtigung bzw. Löschung grundsätzlich einen Filter oder sonstige geeignete Maßnahmen verlangen können.

Die Aufsichtsbehörden werden prüfen, inwieweit konkrete Hilfsmittel bereitgestellt werden können.

Zu § 12a

Der LfDI hält nur die Übermittlung personenbezogener Daten zu Zwecken der parlamentarischen Kontrolle für erforderlich.

Haltung der Landesregierung

Im Wesentlichen wird die Verarbeitung personenbezogener Daten die Übermittlung an den Landtag umfassen. Es sollen aber auch die der Übermittlung vorausgehenden Verarbeitungsschritte erfasst sein. Die Regelung entspricht § 23 des Landesdatenschutzgesetzes Rheinland-Pfalz und § 27 des Gesetzes zum Schutz personenbezogener Daten im Land Brandenburg.

Zu § 13

Zu Absatz 1

- Der LfDI hält die öffentlichen Stellen nur dann für berechtigt, für Forschung personenbezogene Daten zu verarbeiten, wenn ihnen eine entsprechende Aufgabe zugewiesen wurde. Der LfDI sieht weiter keinen Grund, die Weiterverarbeitung ausdrücklich zu regeln, da diese bereits durch Artikel 5 Absatz 1 Buchst. b DSGVO erlaubt sei. Dagegen begrüßen die KLV die Öffnung für die Forschung; insbesondere sollte der öffentliche Gesundheitsdienst einbezogen werden.

Haltung der Landesregierung

Die Auffassung des LfDI wird nicht geteilt. Es muss den öffentlichen Stellen im Rahmen ihrer Aufgabenerfüllung erlaubt sein, Forschungsvorhaben durchzuführen. Hierfür spricht auch die Regelung in Artikel 5 Absatz 1 Buchst. b DSGVO Forschung stellt einen Annex zur jeweiligen Aufgabe dar. Ein Beispiel hierfür ist die

Mobilitätsforschung oder die kriminalpolizeiliche Forschung. Die ausdrückliche Legitimation für die Sekundärforschung wird für berechtigt gehalten. Auch im Bayerischen Datenschutzgesetz ist eine Zweckänderung zugunsten der Forschung in Artikel 6 Absatz 2 Nummer 3 Buchst. c vorgesehen. Die Aufgaben des öffentlichen Gesundheitsdienstes einschließlich der Forschung sind im Gesetz über den öffentlichen Gesundheitsdienst (ÖGDG) geregelt.

Zu Absatz 2

- Der LfDI hält die Verarbeitung öffentlich zugänglicher Daten für Forschungszwecke nicht pauschal für zulässig.

Haltung der Landesregierung

Aus der Norm ergibt sich eindeutig, dass die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen sind. Dies ist jeweils zu prüfen.

Zu Absatz 3

- Der LfDI fordert konkretere Maßnahmen zum Schutz der betroffenen Personen.

Haltung der Landesregierung

Die zu treffenden Maßnahmen müssen sich nach der Schutzbedürftigkeit der Daten richten. Bei der Vielfalt möglicher Forschungsvorhaben müssen die zu treffenden technischen und organisatorischen Maßnahmen im Einzelfall bestimmt werden. Hier besteht der Unterschied zu der geregelten Forschung mit Gesundheitsdaten und genetischen Daten. Diesbezüglich finden die spezifischen Regelungen vorrangige Anwendung. Forschung mit genetischen Daten ist im LDSG nicht bezweckt, da der damit verbundene Grundrechtseingriff eine spezifische Regelung erfordert.

Zu Absatz 5

- Der LfDI sowie das Universitätsklinikum Heidelberg fordern in Bezug auf die Regelung der Weitergabe an Dritte zugunsten der betroffenen Personen ein Widerspruchsrecht in Form einer Opt-Out-Lösung.

- Der LfDI fordert über die vorgeschriebenen Maßnahmen hinaus weitere vom Empfänger zu übernehmende Verpflichtungen. Dagegen würde der BWIHK eine gesetzliche Regelung der Verpflichtungen des Empfängers begrüßen.

- Das Universitätsklinikum Ulm sowie die DHBW hält eine Konkretisierung der „gemeinwohlbezogenen Forschungszwecke“ für wünschenswert.

- Das Universitätsklinikum Tübingen hält die Regelung für unklar, da sie zu Parallelregelungen führen könne. Die KI-VO sehe einen spezifischen Sandbox-Mechanismus vor, der nationale Sonderregelungen ausschließe.

Haltung der Landesregierung

Den betroffenen Personen steht das Widerspruchsrecht nach Artikel 21 DSGVO zur Verfügung. Ein darüberhinausgehendes Widerspruchsrecht wird nicht für erforderlich gehalten. Der Forschung wird ein hohes Gewicht zugunsten der Allgemeinheit zugemessen, weshalb die Regelung eingeführt wird. Die Verarbeitung von Gesundheitsdaten im Krankenhausbereich richtet sich nicht nach dem LDSG, sondern nach dem Landeskrankenhausgesetz. Das dort bestehende Widerspruchsrecht ist zu beachten.

Die vorgeschriebenen Maßnahmen werden als ausreichend erachtet. Der Empfänger ist, nachdem ihm die Daten unter Einhaltung der normierten Schutzmaßnahmen überlassen wurden, der Verantwortliche in Bezug auf die Einhaltung der Datenschutzanforderungen. Diesbezüglich unterliegt er ebenfalls der Datenschutzaufsicht. Der Verweis auf § 3 schließt die Geheimhaltungspflicht ein. Die gesetzliche Regelung der Verpflichtungen des Empfängers unterliegt nicht der Kompetenz des Landesgesetzgebers. Das Bundesdatenschutzgesetz regelt die das Datenschutzrecht der nichtöffentlichen Stellen.

Der Gemeinwohlbegriff ist in § 5 Absatz 1 Nummer 1 als gesetzlich anerkannte allgemeine öffentlichen Interessen definiert. Gemeinwohlorientierte Unternehmen sind daher solche, deren Forschung der Förderung dieser Interessen dient. Beispiele sind Forschung zur Bewältigung drängender sozialer und ökologischer Herausforderungen.

Die KI-VO findet Anwendung, sofern ihr Anwendungsbereich eröffnet ist: Gemäß Artikel 2 Absatz 8 KI-VO gilt die KI-VO nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr

gebracht oder in Betrieb genommen werden. Solche Tätigkeiten werden im Einklang mit dem geltenden Unionsrecht durchgeführt. Maßgeblich ist danach vor allem die DSGVO. Absatz 5 dient dazu, eine datenschutzrechtliche Befugnis zur Übermittlung von Forschungsdaten zu begründen. Eine solche ist in der KI-VO nicht zu finden.

Zu § 15

Zu Absatz 2 Satz 2

- Der LfDI sowie die ARGE-HPR halten es nicht mit Artikel 9 Absatz 3 DSGVO für vereinbar, wenn anderes als ärztliches Personal die besonderen Kategorien personenbezogener Daten für die genannten Zwecke verarbeitet.

Haltung der Landesregierung

Die Auffassung wird nicht geteilt. Die Formulierung entspricht Artikel 9 Absatz 3 DSGVO. Im Übrigen bestimmt nicht das Datenschutzrecht, wer die Arbeitsfähigkeit Beschäftigter beurteilen darf; sondern dies ergibt sich aus berufsrechtlichen, beamtenrechtlichen oder arbeitsrechtlichen sowie strafrechtlichen Vorschriften.

Zu Absatz 6

- Das Universitätsklinikum Tübingen wendet sich gegen die Regelung der Authentifizierung mittels biometrischer Daten als Ultima Ratio. Dies sei kontraproduktiv, da es den Einsatz von TouchID und FaceID verhindere, obwohl die Anforderungen in diesem Bereich durch die NIS-2-Regelungen stiegen. Die KLV argumentieren ebenfalls gegen diese Regelung, die bewährte Anmeldeoptionen verhindern würde.

Haltung der Landesregierung

Biometrische Daten verdienen besonderen Schutz. Dies bedeutet nicht, dass biometrische Identifizierung ausgeschlossen ist. Als geeignet im Sinne der Vorschrift sind Authentifizierungsmittel anzusehen, die den (Cyber)-Sicherheitsanforderungen entsprechen. Daher muss es nicht zwingend beim PIN-Einsatz bleiben.

Zu Absatz 9

Der BWIHK bewertet die Hinweispflicht im Beschäftigtenverhältnis auf den Einsatz von KI-Systemen als „Gold-Plating“, das über die Anforderungen der DSGVO hinausgehe. Auch der NKR stellt die Erforderlichkeit in Frage. Dagegen wird sie vom Universitätsklinikum Freiburg ausdrücklich als Beitrag zur Transparenz und Fairness interner Entscheidungsprozesse begrüßt.

Haltung der Landesregierung

Es handelt sich um eine Pflicht, die den KI-Einsatz für die Durchführung des Beschäftigungsverhältnisses selbst, wie er in § 15 Absatz 1 geregelt ist, betrifft. Sie umfasst nicht den Umgang der Mitarbeitenden mit KI. Die Informationspflicht sorgt für Transparenz entsprechend dem Grundsatz nach Artikel 5 Absatz 1 Buchst. a DSGVO und bedeutet daher kein Gold-Plating.

Zu § 16

- Der LfDI hält den Ausschluss der Betroffenenrechte nicht für haltbar.

Haltung der Landesregierung

Die neue Regelung stellt eine Klarstellung dar. Eine Neufassung bleibt einer weiteren Prüfung vorbehalten.

Zu § 17

- Der LfDI begrüßt die Herauslösung aus der bisherigen Vorschrift. Er regt jedoch an, die Vorschrift in den „Allgemeinen Teil“ zu verschieben. Der LfDI versteht die Norm als Generalklausel, die für alle Verarbeitungen personenbezogener Daten gilt.

Haltung der Landesregierung

Entgegen der Auffassung des LfDI ist die Vorschrift des § 17 nicht als Generalklausel, sondern auf der Grundlage des Artikels 9 Absatz 2 Buchst. g als Auffangtatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten konzipiert, falls eine bereichsspezifische Rechtsgrundlage nicht zur Verfügung steht (vgl. Begründung in der Landtagsdrucksache 16/3930, S. 106).

Zu § 17b

- Zwar begrüßt der LfDI die Spezialregelung zur Öffentlichkeitsarbeit, bewertet sie aber als zu weit gefasst. Insbesondere könnten werbliche Zwecke nicht darunter gefasst werden, da es um die objektive Information der Öffentlichkeit gehe. Es bestünden Fragen zur Art personenbezogener Daten sowie zur Zielgruppe der Öffentlichkeitsarbeit. Die Fertigung von Fotografien und Videoaufnahmen sei eine eingriffsintensive Maßnahme und daher nur mit Einwilligung möglich.

- Von ZENDAS, der DHBW, der HAW und der LRK-PH wird die Anwendbarkeit auf die Öffentlichkeitsarbeit der Hochschulen und das Verhältnis zu § 15 nachgefragt. Die DHBW führt hierzu die Verarbeitung personenbezogener Daten von Beschäftigten und Studierenden, z. B. bei der Information über Forschungsvorhaben oder der Fertigung von Bild- und Tonaufnahmen interner Veranstaltungen, an. ZENDAS ist der Auffassung, dass das voraussetzungslose Widerspruchsrecht die Öffentlichkeitsarbeit der Hochschulen beeinträchtigen könne. Das KIT fordert aus denselben Gründen die ersatzlose Streichung des Widerspruchsrechts.

Haltung der Landesregierung

Die Regelung wird für angemessen gehalten, um die Öffentlichkeit zu informieren. Personenbezogene Daten dienen dazu, die Informationen zielgruppengerecht steuern zu können. Werbliche Zwecke sind legitime Zwecke insofern, als es um die Verbreitung von Angeboten öffentlicher Stellen geht. Diese können beispielsweise in Kommunen die Zusendung von Angeboten der kommunalen Einrichtungen (z. B. Theater, Musikschulen, Bäder o. ä.) sein. Die Erhebung der Daten hat selbstverständlich diskriminierungsfrei zu erfolgen. Des Weiteren sind alle sonstigen Vorgaben für den Einsatz von Social Media zu berücksichtigen. Die Norm selbst verlangt, dass die schutzwürdigen Interessen der betroffenen Personen zu beachten sind. Dies kann insbesondere Einschränkungen bei der Information Minderjähriger bedeuten. Die Anfertigung von Fotografien und Videoaufnahmen wird einer Opt-Out-Regelung unterworfen. Mit dem voraussetzungslosen Widerspruchsrecht wird das informationelle Selbstbestimmungsrecht der betroffenen Personen ausreichend gewahrt.

Als spezielles Gesetz geht das Landeshochschulgesetz, soweit es die Öffentlichkeitsarbeit regelt, gemäß § 1 Absatz 3 LDSG vor. Dort ist kein Widerspruchsrecht normiert. Vorrangig zum LHG gilt jedoch das KunstUrhG, das für Abbildungen außer in den in § 23 genannten Fällen die Einwilligung der abgebildeten Person voraussetzt. Sofern daneben noch § 15 LDSG zur Anwendung kommt, dürfen Beschäftigtendaten nur für die Durchführung des Beschäftigtenverhältnisses im

erforderlichen Umfang verarbeitet werden. Inwieweit dies für die Öffentlichkeitsarbeit zutrifft, muss im Einzelfall bestimmt werden.

- Die KLV sehen die Übertragung von Gemeinderatssitzungen als Instrument der Öffentlichkeitsarbeit an. Sie gehen davon aus, dass der Begriff „Veranstaltungen“ auch Gremiensitzungen umfasst.

Haltung der Landesregierung

Entgegen der Darstellung der KLV dürfte es sich bei Gemeinderatssitzungen zunächst nicht um „Veranstaltungen“ im Sinne des § 17b handeln.

Ferner dürfte die von den KLV erwähnte Rechtsunsicherheit im Zusammenhang mit der Anfertigung von Ton- und Bildaufnahmen von Gremiensitzungen (auch zum Zwecke der Übertragung, beispielsweise per Live-Streaming) bzw. der digitalen Sitzungsteilnahme nicht mehr bestehen. Denn durch das Gesetz zur Änderung kommunalrechtlicher und weiterer Vorschriften vom 22. Juli 2025 (GBl. 2015 Nr. 71) wurde jeweils ein rechtssicherer Rahmen für diese Themenbereiche, also sowohl für die Anfertigung von Ton- und Bildaufnahmen von Gremiensitzungen, als auch für die digitale Sitzungsteilnahme, geschaffen (vgl. u. a. §§ 35 Absatz 3 und 37a GemO; §§ 30 Absatz 3 und 32a Landkreisordnung (LKrO). Hier wurden (gerade zur Vermeidung von Rechtsunsicherheiten) insbesondere auch Regelungen hinsichtlich der Folgen technischer Störungen während der Gremiensitzungen, als auch (jedenfalls in der Begründung des Regierungsentwurfs) Ausführungen zu der Frage des datenschutzrechtlichen Einwilligungserfordernisses aufgenommen (vgl. LT-Drucksachen 17/8922, S. 38 ff. und 43 ff.).

Ergänzend ist auf Folgendes hinzuweisen:

§ 17b LDSG-E dürfte sich allenfalls auf den Regelungsbereich des (neu eingeführten) § 35 Absatz 3 GemO (und damit auf das Thema „Anfertigung von Ton- und Bildaufnahmen“) beziehen, nicht jedoch auf die von den KLV zitierten § 37a GemO bzw. § 32a LKrO, welche die digitale Sitzungsteilnahme der Gremienmitglieder zum Gegenstand haben.

Auch die Darstellungen der KLV zu einer vermeintlichen Rechtsunsicherheit im Zusammenhang mit der Frage einer wirksamen (datenschutzrechtlichen) Einwilligung für bestimmte Personengruppen unter Verweis auf die Ausführungen des LfDI (LfDI BW (2019) Leitfaden für Gemeinden, Gremienübertragungen im Internet –

Einwilligung; S. 96) dürften sich durch die oben dargestellten Regelungen, welche durch das Gesetz zur Änderung kommunalrechtlicher und weiterer Vorschriften eingeführt worden sind, bzw. die entsprechenden Ausführungen in der Begründung des Regierungsentwurfs zwischenzeitlich weitgehend überholt haben. Denn die §§ 35 Absatz 3 und 37a GemO bzw. §§ 30 Absatz 3 und 32a LKrO sind leges speciales zu § 17b.

Zu § 18

- Vom LfDI, ZENDAS und der BWIHK wird die Überschrift in Frage gestellt, da es im Gesetzestext um „Videoüberwachung“ gehe.

Haltung der Landesregierung

Die Überschrift „Videoschutz“ bringt deutlicher als bisher zum Ausdruck, dass es um den Schutz, nicht um die Überwachung von Personen und Objekten geht. Im Gesetzestext bleibt es bei dem eingeführten Begriff der „Videoüberwachung“, um eine einheitliche Verwendung sicherzustellen und die Tätigkeit an sich zu beschreiben.

Zu Absatz 1 Satz 2

- Der LfDI stellt in Frage, dass der Schutz von Leben, Gesundheit und Freiheit als besonders wichtiges Schutzgut hervorgehoben werden dürfe, da auch das Recht auf Datenschutz ein Grundrecht sei und daher immer eine Abwägung stattfinden müsse.

Haltung der Landesregierung

Die Hervorhebung wie geschehen hebt die Verpflichtung zur Abwägung nicht auf. Es ist aber dem Gesetzgeber nicht verwehrt, selbst die Abwägungsentscheidung zu prägen.

Zu Absatz 1 Satz 3

- Die Fiktion der Angemessenheit der Videoüberwachung für bestimmte Objekte wird vom LfDI, dem Anwaltsverband und ZENDAS für verfassungswidrig gehalten, da die Angemessenheit sich nach den Umständen des Einzelfalls beurteile. Dagegen begrüßt der NKR die Erleichterung der Vorrangprüfung. Der DVS-BW möchte eine Ausweitung auf öffentliche Plätze, Gartenanlagen und Parks, Bahnhöfe und

Haltestellen sowie Müllsammelstellen, da sich dort vermehrt Straftaten und Ordnungswidrigkeiten ereigneten.

Haltung der Landesregierung

Die neu eingeführte Fiktion der Angemessenheit der Videoüberwachung für bestimmte als besonders sicherheitsrelevant eingestufte Objekte führt eine abstrakt-generelle Bewertung der Videoüberwachung als angemessenes Mittel ein. Sie soll die öffentlichen Stellen entlasten, eine Vorrangprüfung auch in Fällen vorzunehmen, in denen Videoüberwachung letztlich das wirksamste Schutzmittel ist, das heißt kein gleich geeignetes milderes Mittel zur Verfügung steht. Wenn Videoüberwachung als ein wirksames Mittel für die Gefahrenabwehr betrachtet wird, wie in der Regelung des § 18 zum Ausdruck kommt, und der Einsatz sichergestellt werden soll, ist es angezeigt, dies die Mittelauswahl betreffend gesetzgeberisch zum Ausdruck zu bringen. Die Annahme der Angemessenheit bleibt aber beschränkt auf die Fälle, in denen der Videoschutz erforderlich ist, also bei der nachweisbaren erheblichen Gefährdung hochwertiger Schutzgüter. Maßnahmen mit geringerer Eingriffstiefe sind damit nicht ausgeschlossen und können ebenfalls eingesetzt werden. Die Einhaltung der Datenschutzgrundsätze und der Schutz nicht beteiligter Personen durch technische Maßnahmen, wird außerdem vorausgesetzt.

Die Auflistung der Objekte, für die das Mittel der Videoüberwachung als angemessen bewertet wird, ist bewusst beschränkt auf sicherheitsrelevante und kulturell bedeutsame Objekte. Im Übrigen bedarf es einer Abwägung im Einzelfall. Schließlich stellt Videoüberwachung einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, der nur zulässig ist, wenn er verhältnismäßig ist. Außerdem dient Videoüberwachung nach § 18 nicht der Kriminalitätsbekämpfung.

Zu Absatz 2

- Nach Auffassung des LfDI und des Anwaltsverbands genügen die nach Absatz 2 zu machenden Angaben nicht, um der Informationspflicht nach Artikel 13 DSGVO nachzukommen. Dagegen würde der BWIHK es als Erleichterung ansehen, wenn generell ein Piktogramm (Kamerasymbol) ausreichen würde und ausnahmslos alle anderen Informationen erfragt werden könnten. Der NKR sieht für erweiterte Informationspflichten keine Erforderlichkeit und ist der Auffassung, dass getroffene verhältnismäßige Erleichterungen nicht mit neuen Erschwernissen „bezahlt“ werden sollten. Die KLV lehnen die Ausweitung der anzubringenden Informationen ebenfalls ab.

Haltung der Landesregierung

Da die Informationen nach Artikel 13 DSGVO bei Erhebung erteilt werden müssen, kann ein einfaches Piktogramm mit Kamerasymbol nicht genügen. Die gewählte Lösung der Angabe der Kontaktdaten und der Stelle, wo die Informationen verfügbar sind, wird für handhabbar gehalten. Auch hierfür können Piktogramme gewählt werden.

Zu Absatz 4

- Der LfDI, der Anwaltsverband, das Universitätsklinikum Tübingen sowie ZENDAS stellen sich gegen die Verlängerung der Speicherfrist auf zwei Monate. Der LfDI verweist auf die Verpflichtung zur unverzüglichen Löschung: Der Anwaltsverband fordert, bei fehlenden Ressourcen zur Auswertung der Videoaufnahmen mehr Personal vorzusehen. Die KLV und der BWIHK begrüßen die verlängerte Löschfrist.

Haltung der Landesregierung

Die Speicherfrist von zwei Monaten stellt die maximale Speicherdauer dar, die nur ausnahmsweise angemessen ist. Im Einzelfall kann sie aber erforderlich sein. Der besonderen Begründungspflicht wird zugestimmt. Der LfDI selbst führt hierfür Ferien und Urlaubszeiten an. Ein ausreichender Schutz der Daten durch organisatorische und technische Maßnahmen minimiert den Grundrechtseingriff.

Zu Absatz 6

- Das Universitätsklinikum Heidelberg hat Bedenken, weil sich betroffene Personen, auch besonders schutzbedürftige, der Verarbeitung ihrer Daten durch das KI-System nicht entziehen könnten. Die ARGE-HPR äußert zu § 18 Absatz 6 (und § 18a) erhebliche Bedenken in Bezug auf Videoüberwachung von Schülerinnen und Schüler sowie Lehrkräfte.

- Der LfDI bezweifelt die Normenklarheit der Regelung. Insbesondere dürften die Anforderungen des § 44 Absatz 3 des Polizeigesetzes nicht unterlaufen werden.

- Dem Universitätsklinikum Tübingen fehlt es an einer Pflicht zur Datenschutz-Folgenabschätzung bei KI-gestützter Analyse, außerdem an der Berücksichtigung der Pflichten für Hochrisikosysteme nach der KI-VO.

- Von ZENDAS wird das von Hochschulen betriebene Auslastungsmanagement bei hochschulgenutzten Flächen u. a. mit Hilfe optisch-elektronischer Einrichtungen und KI erwähnt, aber nicht der Videoüberwachung zugerechnet, da es nicht auf den Personenbezug ankomme. Es würden aber Klaraufnahmen mit anschließender Verfremdung stattfinden.

Haltung der Landesregierung

Es sind Vorkehrungen zu treffen, um die Aufzeichnung der Daten auf das Minimum zu beschränken, insbesondere die Verarbeitung personenbezogener Daten möglichst insgesamt zu vermeiden, zumal sie nichts zu dem Verarbeitungszweck beitragen. Im Übrigen wird der ARGE-HPR zugestimmt, dass es einer Klärung bedarf, ob, unter welchen Voraussetzungen, in welchem Umfang und mit welchen geeigneten technischen und organisatorischen Maßnahmen Videoüberwachung zukünftig auch in Schulgebäuden und auf dem Schulgelände möglich sein soll. Der richtige Platz hierfür findet sich, sofern angestrebt, im Schulgesetz.

Es wird kein Zusammenhang mit der Videoüberwachung nach dem Polizeigesetz (PolG) gesehen, da Zweck der Videoüberwachung nach Absatz 6 nicht die Straftatenbekämpfung, sondern der Schutz öffentlichen Eigentums und öffentlicher Infrastruktur als öffentliche Aufgabe ist. Der in der Begründung erwähnte Vandalismus kann im Einzelfall eine Überprüfung des Erhaltungszustands und der Funktionsfähigkeit rechtfertigen; es kommt aber auf die Verhältnismäßigkeit an.

Die Pflicht zur Datenschutz-Folgenabschätzung kann sich aus Artikel 35 DSGVO ergeben. Die KI-VO ist als unmittelbar geltendes Recht zu beachten

Die Neuregelung der §§ 18 ff. beschränkt sich auf die genannten Zwecke. Wie sich aus § 3a ergibt, ist daneben Raum für den Einsatz von KI, sofern eine Rechtsgrundlage zur Verfügung steht.

Zu § 18a

- Seitens des Universitätsklinikums Heidelberg wird darauf hingewiesen, dass Videoüberwachung in öffentlich nicht zugänglichen Räumen eine erhebliche psychische Belastung für Mitarbeitende darstellen könne. Es bedürfe daher expliziter Schutzmaßnahmen. Auch der LfDI weist auf den höheren Schutzbedarf bei Videoüberwachung in nicht öffentlich zugänglichen Räumen hin. Die Rechtsgrundlage sollte sich daher auf enge Anwendungsfälle beschränken. Dagegen

möchte der BWIHK als weitere Zwecke den Schutz des Hausrechts und den Schutz von Leben, Gesundheit und Freiheit der sich in öffentlichen Einrichtungen aufhaltenden Personen hinzufügen.

- Aus Sicht des Universitätsklinikums Freiburg wäre eine klare gesetzliche Ausnahme für sicherheitsrelevante Dauerüberwachungen (z. B. in Intensivstationen, Notaufnahmen) hilfreich.

Haltung der Landesregierung

Der Gesetzentwurf sieht die besondere Schutzbedürftigkeit beschäftigter Personen. Auch hier ist der Eingriff so gering wie möglich zu halten. Der Schutz der Grundrechte der betroffenen Personen setzt insbesondere dem Einsatz von Videoüberwachung am Arbeitsplatz Grenzen, insbesondere wenn es um die Intimsphäre und den Kernbereich privater Lebensgestaltung geht. Die schutzwürdigen Interessen betroffenen Personen müssen gegen das Interesse an der Überwachung abgewogen werden. Der Eingriff sollte auf jeden Fall räumlich und zeitlich beschränkt werden. Sofern Videoüberwachung zu dem genannten Zweck zu Zeiten ausreicht, in denen keine Personen anwesend sind, ist dies vorzuziehen.

Videoüberwachung zum Schutz der von der BWIHK genannten Zwecke ist von § 18 Absatz 6 nicht intendiert. Soweit die öffentlichen Einrichtungen öffentlich zugänglich sind, gilt § 18 Absatz 1. In nicht öffentlich zugänglichen Bereichen gilt, sofern Beschäftigte betroffen sind, § 15. Ggf. kann auch § 17a Absatz 2 in Verbindung mit § 3a den Einsatz von KI erlauben.

Sicherheitsrelevante Dauerüberwachungen können nach speziellen Regelungen zulässig sein. Subsidiär gilt § 15 Absatz 7, wonach optisch-elektronische Einrichtungen zum Zweck der Verhaltens- und Leistungskontrolle Beschäftigter unzulässig sind. Artikel 9 Absatz 2 Buchst. c DSGVO kann zum Schutz lebenswichtiger Interessen ebenfalls eine Rechtsgrundlage liefern.

Zu § 18b

- Der LfDI sieht auch hier die Anforderungen an die Bestimmtheit der Norm nicht erfüllt. Es sei nicht ersichtlich, welche Arten von Überwachungen zu welchem Zweck und unter welchen Umständen geregelt werden sollen. Auf die Strafbarkeit nach § 201 StGB wird hingewiesen. Dagegen bewertet der BWIHK die Überwachung mit sonstigen technischen Mitteln positiv. In Betracht komme der Einsatz von Sensorik

(Vibration, Geräusch, Bewegung). In Bezug auf die Speicherdauer bestünden Unklarheiten. Auch für diese Form der Überwachung solle der Schutz von Leben, Gesundheit und Freiheit der sich in öffentlichen Einrichtungen aufhaltenden Personen als zusätzlicher Zweck eingefügt werden. Ein weiterer Einsatzzweck wird in der sensorischen Überwachung zur Sicherung operativer Zwecke (z. B. Beschlussfähigkeit eines Gremiums, Erreichen von Kapazitäten bei einer großen Veranstaltung) gesehen.

Haltung der Landesregierung

Die Auffassung des LfDI wird nicht geteilt. Es geht keinesfalls um die Überwachung um der Überwachung willen. Vielmehr geht es darum, zum Schutz der Funktionsfähigkeit öffentlichen Eigentums und öffentlicher Infrastruktur weitere technische Mittel, selbstverständlich unter Beachtung der Verhältnismäßigkeit einsetzen zu können. Die Auswertung von Tonaufnahmen wird bewusst beschränkt. Dabei geht es nicht um das Abhören von Personen, sondern um verdächtige Geräusche in Bezug auf die überwachten Objekte. Jeweils nach 180 Sekunden Aufnahmedauer hat eine automatisierte Löschung zu erfolgen, sofern personenbezogene Daten betroffen sind. Sonstige technische Überwachung zum Schutz von Leben, Gesundheit und Freiheit von Personen einzusetzen, begegnet im Hinblick auf die Eingriffsintensität verfassungsrechtlichen Bedenken und ist daher nicht intendiert.

Darüber hinaus werden ergänzende Vorschläge dargelegt:

Zu den Normzielen

- Der Sparkassenverband dringt auf eine ausdrückliche Digitalisierungspflicht („Digital-First“). Zahlreiche Verweise auf Schriftformerfordernisse oder papiergebundene Verfahren blieben bestehen. Außerdem plädiert er für eine Übergangsfrist für neue Pflichten.

Haltung der Landesregierung

Das LDSG enthält keine Schriftformerfordernisse und auch keine Verweise auf solche. Vielmehr soll es gerade die digitale Verwaltung stärken. Im Übrigen hat es sich die Landesregierung zur Aufgabe gemacht, Schriftformerfordernisse abzuschaffen. Das LDSG ist aber nicht der richtige Ort dafür. Darüber hinaus sind keine Pflichten erkennbar, die eine Übergangsfrist erfordern würden.

Schutz vor Verstößen gegen § 203 StGB

- Das Universitätsklinikum Tübingen sieht nicht hinreichend berücksichtigt, dass Berufsgeheimnisträger durch Datenübermittlungen gegen § 203 StGB verstoßen könnten. Auch die KI-VO sanktioniere unzulässige KI-Einsätze. In Bezug auf die Geheimnisse nach § 203 StGB müsse vorher eine Pseudonymisierung oder Anonymisierung erfolgen oder eine ausdrückliche Ermächtigung vorliegen.

Haltung der Landesregierung

Das LDSG enthält in § 12 eine Vorschrift zur Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Im Übrigen sanktioniert § 203 StGB nur die unbefugte Offenbarung von Privatgeheimnissen. Das Gebot, die Daten, soweit möglich, zu anonymisieren oder zu pseudonymisieren ist durchgängig im LDSG berücksichtigt. Es ergibt sich aus dem Grundsatz der Datenminimierung in Artikel 5 Absatz 1 Buchst. c DSGVO.

Zu § 2 Absatz 5

- Der DRB möchte die Staatsanwälte in die Regelung für die Justiz einbezogen wissen.

Haltung der Landesregierung

Die Staatsanwaltschaften sind in dem Entwurf nicht ausdrücklich genannt. Sie sind allerdings erfasst, soweit sie eine Verwaltungstätigkeit zu anderen Zwecken als denen der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung ausüben. Im Übrigen können sie nicht in den Regelungsentwurf einbezogen werden. Die DSGVO findet nach ihrem Art. 2 Absatz 2 Buchst. d auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit grundsätzlich keine Anwendung. Entsprechende Regelungen sind der Richtlinie (EU) 2016/680 vom 27. April 2016 (JI-Richtlinie) und ihren Umsetzungsgesetzen (LDSG-JB; Verfahrensordnungen bzw. BDSG) und damit anderen Regelungsvorhaben vorbehalten.

- Der Notarverein stellt die Frage, wer für die datenschutzrechtlichen Prüfungen zuständig ist. Die Datenschutzaufsicht sollte bei einer Stelle konzentriert werden.

Haltung der Landesregierung

In der Kürze der zur Verfügung stehenden Zeit kann das Anliegen des Baden-Württembergischen Notarvereins e.V. nicht umfassend geprüft und beurteilt werden. Das Justizministerium wird den Vorschlag im Rahmen künftiger Regelungsvorhaben nochmals rechtlich prüfen und ggf. umsetzen, soweit eine Gesetzgebungskompetenz des Landes besteht.

Zu § 2 Absatz 6

- Die Komm.ONE regt die Erstreckung einzelner Vorschriften des LDSG auf Wettbewerbsunternehmen an.

Haltung der Landesregierung

Die neue Fragestellung bleibt außen vor, da sie vertiefender Untersuchung bedarf, die in diesem Regelungsvorhaben nicht möglich ist.

Änderung des § 9 (Beschränkung des Auskunftsrechts)

- Der LfDI sieht seine Vorschläge zur Änderung des § 9 LDSG im Rahmen der Evaluierung nicht berücksichtigt.

Haltung der Landesregierung

Aus Sicht der Landesregierung besteht kein zwingender Grund, die Regelung des § 9 Absatz 2 LDSG zu ändern. Auf die Begründung in der Evaluierung des Landesdatenschutzgesetzes wird verwiesen.

Änderung des § 14 (Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken)

- Der LfDI sieht in § 14 die Betroffenenrechte als zu weit eingeschränkt an.

Haltung der Landesregierung

§ 14 ist nicht Gegenstand der Novellierung. Das Archivrecht fällt in die Zuständigkeit des Wissenschaftsministeriums

Änderung des § 25 (Aufgaben und Befugnisse)

- Der LfDI bemängelt, dass seine diesbezüglichen Änderungsvorschläge im Rahmen der Evaluierung des LDSG nicht berücksichtigt wurden.

Haltung der Landesregierung

Die Vorschläge des LfDI wurden nicht aufgegriffen. Für die Begründung wird auf den Evaluierungsbericht verwiesen.

- Die KLV ergreifen eine Initiative zur Änderung der Gemeindeordnung mit dem Ziel, KI für die Erstellung von Gemeinderatsprotokollen zu nutzen. Dies subsidiär, falls § 3a dies nicht bereits ermöglicht.

Haltung der Landesregierung

Zunächst ist festzuhalten, dass sich die von den KLV aufgeworfene Frage, ob § 3a als ausreichend zur Regelung des Themenkomplexes „Erstellung des Gemeinderatsprotokolls durch eine KI“ angesehen wird, lediglich auf die datenschutzrechtlichen Aspekte der Thematik beziehen kann, nicht jedoch auf die kommunalverfassungsrechtlichen Regelungsinhalte.

Eine Änderung der GemO ist weder Gegenstand des vorliegenden Gesetzgebungsverfahrens, noch erscheint eine solche angezeigt. Denn die bestehenden Regelungen, hier insbesondere § 38 GemO, dürften ausreichend sein.

Die Erstellung der Niederschrift fällt in den Zuständigkeitsbereich des Bürgermeisters. Er bestimmt im Rahmen seines Organisationsrechts den Schriftführer und kann diesem auch Vorgaben zur Art und Weise der Protokollierung machen. Dies dürfte auch den Einsatz von Künstlicher Intelligenz mit umfassen. Eine ausdrückliche Zustimmung des Gemeinderats zum unterstützenden Einsatz von Künstlicher Intelligenz bei der Erstellung der Niederschrift erscheint deshalb nicht zwingend erforderlich. Auch ein Widerspruchsrecht – weder des Gremiums Gemeinderat, noch einzelner Gemeinderatsmitglieder – besteht insoweit nicht. Zur Vermeidung von Diskussionen oder Streitigkeiten dürfte es aber gleichwohl sinnvoll sein, den Gemeinderat vorher einzubinden.

b) Zur Änderung des EGovG BW

Zu § 17a – Grundsätzliche Anmerkungen

- Die KLV können sich für die Experimentierklausel auch eine weitergehende Formulierung vorstellen, die sich an § 155 Absatz 4 Satz 1 AO orientiert, der wie folgt lautet: „Die Finanzbehörden können Steuerfestsetzungen sowie Anrechnungen von Steuerabzugsbeträgen und Vorauszahlungen auf der Grundlage der ihnen vorliegenden Informationen und der Angaben des Steuerpflichtigen ausschließlich automationsgestützt vornehmen, berichtigen, zurücknehmen, widerrufen, aufheben oder ändern, soweit kein Anlass dazu besteht, den Einzelfall durch Amtsträger zu bearbeiten.“

Haltung der Landesregierung

Eine Orientierung der Erprobungsvoraussetzungen an der Formulierung des § 155 Absatz 4 Satz 1 AO ist nicht sachgerecht, da die Abgabenordnung als Spezialvorschrift für das Steuerrecht nur einen kleinen Teil der breiten Tätigkeit der Behörden im Land abdeckt. Eine Orientierung an den bewährten Vorgaben des Verwaltungsverfahrensrechts ist vor diesem Hintergrund sinnvoller. Zudem steht die benannte Regelung nicht für sich, sondern ist beispielweise auch im Kontext des § 88 Absatz 5 AO zu sehen, der Vorgaben für ein Risikomanagementsystem macht. Diese sind in der Erprobungsklausel bewusst nicht enthalten.

- Der LfDI meint, er könne nicht ohne Weiteres erkennen, dass der Regelungsentwurf gemäß Artikel 22 Absatz 2 Buchstabe b DSGVO „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten“ würde. Hinweise auf aus seiner Sicht weitere erforderliche Maßnahmen werden nicht gegeben.

Haltung der Landesregierung

Die angemessenen Schutzmaßnahmen ergeben sich neben der Interessenabwägung nach § 17a Absatz 2 Satz 2 EGovG BW auch 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 LVwVfG, zum Erfordernis der Bekanntgabe gemäß § 41 LVwVfG sowie zu den Rechtsbehelfsmöglichkeiten. Dabei berücksichtigen insbesondere §§ 35a und 24 Absatz 1 Satz 3 LVwVfG die spezifischen Risiken der automatisierten Verarbeitung.

- Der LfDI führt weiter an, dass der datenschutzrechtliche Anwendungsbereich und Regelungsgehalt des neuen § 17a EGovG BW unklar sei. Die geplanten Regelungen in §§ 15a bis 15c des Entwurfs des Änderungsgesetzes zum E-Government-Gesetzes Baden-Württemberg normierten die Datenverarbeitung im Dienstleistungsportal des Landes, die Rechtsgrundlagen der Datenverarbeitung in einem Onlinedienst und datenschutzrechtliche Verantwortlichkeiten, wobei alle drei Normen auf das Landesdatenschutzgesetz, insbesondere § 3 Absatz 1 LDSG, verwiesen. Eine zusätzliche Rechtsgrundlage für den KI-Einsatz neben den Regelungen im LDSG im E-Government-Gesetzes Baden-Württemberg erschließe sich ihm nicht.

Haltung der Landesregierung

Die zusätzlichen Regelungen im § 17a EGovG BW sind erforderlich, um den in § 35a LVwVfG geforderten Rechtsvorschriftvorbehalt für die Schaffung einer verwaltungsverfahrensrechtlichen Rechtsgrundlage in einer Rechtsvorschrift zu erfüllen. Die Regelungen des Landesdatenschutzgesetzes zum KI-Einsatz sind dafür nicht ausreichend, da diese lediglich die datenschutzrechtlichen Regelungserfordernisse abdecken. Zudem ergibt sich keine Überschneidung mit den geplanten Regelungen des §§ 15a bis 15c EGovG BW-E, da diese keine Regelungen für den Erlass von Verwaltungsakten enthalten, sondern die Datenverarbeitung im Dienstleistungsportal und den Onlinediensten zum Thema haben. Diese Vorgänge sind dem Verfahren zum Erlass eines Verwaltungsaktes (Sachverhaltsfeststellung, Rechtsanwendung und Bescheidformulierung) zeitlich vorgeschaltet und betreffen lediglich den Anstoß des Verfahrens.

- Der BBW sieht die Möglichkeit kritisch, Verwaltungsakte ausschließlich durch KI-Systeme ohne Plausibilitätskontrolle durch eine verantwortliche, natürliche Person zu erlassen. Er sieht dabei erhebliche Risiken wegen fehlender Berücksichtigung individueller Besonderheiten und vermutet eine Schwächung der rechtsstaatlichen Verankerung staatlichen Handelns sowie eine Beeinträchtigung des Vertrauens in die Verwaltung.

Haltung der Landesregierung

Nach dem Monitor öffentlicher Dienst 2025 des DBB Beamtenbund und Tarifunion fehlen dem öffentlichen Dienst in Deutschland 570.000 Beschäftigte. Die negativen Folgen der fehlenden Beschäftigten können abgemildert werden, indem Mitarbeiterinnen und Mitarbeiter von routinemäßigen Entscheidungen durch

Automation befreit werden. Auch kann der automatisierte Erlass von Verwaltungsakten das Vertrauen der Bürgerinnen und Bürger in einheitliche Entscheidungen stärken. So können insbesondere Verwaltungsakte im Bereich von Massenverfahren automatisiert erlassen werden. Dies ist etwa im Bereich von Registereintragungen bei unbemannten Fluggeräten, Kraftfahrzeugen, Batterien, Elektro- oder Elektronikgeräten bereits spezialgesetzlich geregelt (z. B. in § 66a des Luftverkehrsgesetzes, § 6g des Straßenverkehrsgesetzes, § 22 des Batteriegesetzes, § 38a des Elektro- und Elektronikgerätegesetzes). Daneben existieren auch landesrechtliche Regelungen (§ 10a des Rundfunkbeitragsstaatsvertrags, § 32a des baden-württembergischen Finanzausgleichsgesetzes). Die Erprobungsregelung ermöglicht den Einsatz auch außerhalb dieser spezialgesetzlich erfolgten Normierungen.

Der Einsatz der KI in vollautomatisierten Verfahren ist nach den Vorgaben des § 35a des Landesverwaltungsverfahrensgesetzes auf Fälle ohne Ermessungsspielraum und ohne Beurteilungsspielraum beschränkt, so dass eine Berücksichtigung individueller Besonderheiten regelmäßig nicht erforderlich sein dürfte. Zudem ist mit den in § 17a Absatz 2 EGovG BW-E verankerten Regelbeispielen eine an bewährten Regelungen orientierte rechtsstaatliche Grundlage für den Einsatz automatisierter Erlassmöglichkeiten von Verwaltungsakten vorhanden. Eine verpflichtende und umfassende Plausibilitätsprüfung der vollautomatisiert erlassenen Verwaltungsakte durch eine natürliche Person würde auch dem Erprobungsansatz widersprechen; durch die Vorgaben der KI-VO der EU sind zudem wesentlichen Risiken, die im Zusammengang mit KI stehen, abschließend europarechtlich normiert worden.

- Der Anwaltsverband Baden-Württemberg betont die Bedeutung der Anhörung und des Rechtes auf rechtliches Gehör. Zudem ist aus seiner Sicht aufgrund des Rechtes auf ein faires Verfahren ein Einsatz algorithmischer Systeme als Entscheider ausgeschlossen. Auch sei auf die Möglichkeit des Widerspruchsverfahrens als Rechtschutzmaßnahme hinzuweisen.

Haltung der Landesregierung

Das Anhörungsrecht nach § 28 LVwVfG erfährt durch den Gesetzentwurf keine Änderung, sondern ist wichtiger Bestandteil der angemessenen Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person nach Artikel 22 Absatz 2 Buchstabe b DSGVO. Ebenso ist die Überprüfungsmöglichkeit in einem Widerspruchsverfahren, welches nicht vollständig automatisiert abläuft, ein wichtiges Regelbeispiel (vgl. § 17a Absatz 2 Satz 2

Nummer 2 des Entwurfs), welches dafür sorgt, dass die Interessenabwägung einen Einsatz von KI-Technik ermöglicht. Somit wird das Widerspruchsverfahren in seiner Bedeutung gestärkt. Die Ansicht eines allgemeinen Ausschlusses von KI-Technik für Entscheidungsvorgänge wird nicht geteilt. Vielmehr wird darauf hingewiesen, dass dies in der Praxis bereits aufgrund spezieller Regelungen erfolgt.

- Die ARGE-HPR hält einen ausschließlichen durch KI-Technik durchgeführten automatisierten Erlass von Verwaltungsakten für verfrüht an. Sie sieht im Erprobungszeitraum eine lückenlose Kontrolle durch fachkundige Sachbearbeitungen als erforderlich an. Auch solle eine Stelle eingerichtet werden, um möglicherweise fehlerhafte Bearbeitung durch KI-Technik zu melden und überprüfen lassen zu können.

Haltung der Landesregierung

Ob und wie die jeweiligen Behörden die Durchführung der Erprobung ausgestalten, soll nicht durch einzelne starre Vorgaben festgelegt werden. Es ist zu erwarten, dass zur Vermeidung einer erhöhten Anzahl von Widersprüchen gegen mittels KI-Technik erlassene Verwaltungsakte die jeweilige Behörde bei Bedarf ihre Abhilfemöglichkeiten entsprechend anpasst, um zusätzliche Aufwände im weiteren Rechtsschutzverfahren zu vermeiden. Die Einrichtung einer zentralen Stelle zur Meldung und Überprüfung von mittels KI-Technik erlassenen Verwaltungsakten ist folglich nicht erforderlich. Die üblichen Strukturen der Rechts- und Fachaufsicht sind für die Begleitung des Erprobungsprozesses ausreichend.

- Die Universität Freiburg sieht die Zulassung einer behördenbezogenen Erprobung kritisch, da sie für bereichsspezifische Zulassungen den Normgeber gefordert sieht. Außerdem sieht sie das Regelbeispiel in Absatz 2 Satz 2 Nummer 2 insoweit als rechtsstaatlich bedenklich an, als auf eine menschliche Kontrolle der Ausgangsentscheidung schon wegen der Überprüfung im Widerspruchsverfahren verzichtet werde. Schließlich sieht sie den Übergang in die reguläre Anwendungspraxis durch Rechtsverordnung als nicht möglich an, da diese Entscheidung nach der Wesentlichkeitstheorie durch den Gesetzgeber zu treffen sei.

Haltung der Landesregierung

Dem Gesetzgeber steht es frei, eine allgemeine Erprobungszulassung des KI-Einsatzes zu beschließen; ein Normenvorrang des § 35a Landesverwaltungsverfahrensgesetzes vor anderen Gesetzen besteht nicht. Dies gilt

auch für eine Zulassung für die reguläre Anwendungspraxis durch Rechtsverordnung. Die Vorgaben des Artikels 61 Absatz 1 des Landesverfassung zum Verordnungserlass werden durch die Formulierung des Absatzes 5 eingehalten.

Wie bereits oben zur Stellungnahme des BBW zu § 17 a EGovG BW ausgeführt, bestehen keine grundsätzlichen rechtsstaatlichen Bedenken, wenn eine Entscheidung ohne Beteiligung einer verantwortlichen natürlichen Person ergeht.

Zu § 17a Absatz 2 Satz 2 Nummer 1

- Die KLV merken an, dass die in § 17a Absatz 2 Satz 2 Nummer 1 vorgesehen Einwilligung nicht in Schriftform, sondern in Textform zu erteilen sein sollte.

Haltung der Landesregierung

Eine Schriftformanordnung ist im Gesetzentwurf nicht enthalten, so dass der Erteilung in Textform, die aus Beweiszwecken sinnvoll sein dürfte, nichts entgegensteht.

- Der LfDI merkt an, dass bei einer Einwilligung der betroffenen Person gemäß Art. 6 Absatz 1 Buchstabe a DSGVO nicht zugleich von einem überwiegenden Interesse der verantwortlichen Stelle ausgegangen werden könne. Eine Einwilligung müsse nach Artikel 22 Absatz 2 Buchstabe c DSGVO ausdrücklich erteilt werden und von diesem Erfordernis einer ausdrücklichen Erklärung könne nicht ohne weiteres durch mitgliedstaatliches Recht unter Berufung auf Artikel 22 Absatz 2 Buchstabe b DSGVO abgewichen werden.

Haltung der Landesregierung

Aufgrund der von § 17a Absatz 2 Satz 2 Nummer 1 EGovG BW geforderten ausdrücklichen Einwilligung der Betroffenen ist den Anforderungen des Artikel 22 Absatz 2 Buchstabe c DSGVO an eine automatisierte Entscheidung im Einzelfall Genüge getan. Gleichzeitig liegen auch die Voraussetzungen des Artikel 22 Absatz 2 Buchstabe b DSGVO vor, wenn die automatisierte Entscheidung nach § 17a Absatz 2 Satz 1 EGovG BW in Verbindung mit dem LVwVfG zulässig ist, weil diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten. Der DSGVO lässt sich nicht entnehmen, dass nicht mehrere Varianten des Artikel 22 Absatz 2 DSGVO gleichzeitig vorliegen können.

Zu § 17a Absatz 3

- Der LfDI weist darauf hin, dass unklar bleibe, welche Unterlagen gemäß der DSGVO (bspw. Datenschutz-Folgenabschätzung) und der KI-VO (bspw. Grundrechts-Folgenabschätzung) verantwortliche Stellen mit der Anzeige des Vorhabens vorlegen müssten, um eine präventive Prüfung von der obersten Fachaufsichtsbehörde und dem für das Verwaltungsverfahrensrecht zuständigen Innenministerium zu ermöglichen.

Haltung der Landesregierung

Regelmäßig wird eine Datenschutz-Folgenabschätzung für eine Erprobung erforderlich sein. Die Anzeigepflicht betrifft aber Fälle mit und ohne Einsatz von KI, so dass im letzteren Falle mangels Anwendbarkeit der KI-VO keine Pflicht zur Grundrechts-Folgenabschätzung bestehen würde. Damit ist es eine Frage des Einzelfalles, welche Unterlagen im konkreten Fall erstellt werden müssen. Diese Unterlagen müssen zumeist auch nur vor Aufnahme des Verfahrens, nicht aber bereits zum Zeitpunkt der Anzeigepflicht – ein Monat vor Aufnahme des Verfahrens – vorliegen. Eine vorherige Vorlagepflicht von Unterlagen könnte daher die Verfahrensaufnahme verzögern, weshalb davon Abstand genommen wurde, abstrakt die Vorlagepflicht von Unterlagen zu normieren.

Auch dient die Anzeigepflicht neben der Möglichkeit zur präventiven Kontrolle vor allem auch der Information der obersten Fachaufsichtsbehörde bzw. Rechtsaufsichtbehörde und dem Innenministerium, damit diese ggf. auf ähnliche Verfahren hinweisen können und rechtsklar festgehalten ist, wann die Fristen nach Absatz 5 zu laufen beginnen. Dafür bedarf es aber regelmäßig gar keiner Vorlage von Unterlagen wie einer Datenschutz-Folgenabschätzung.

Zu § 17a Absatz 4

- Dem LfDI erscheint es fraglich, ob eine Erprobungszeit von 2 bis 5 Jahren verhältnismäßig sei, ohne dass die Datenverarbeitung zeitnah in einer Rechtsverordnung geregelt werde.

- Die Rechtsanwaltskammer Stuttgart fordert eine zwingende Einbeziehung der Rechtsanwaltskammern in den Evaluierungsprozess, damit die Interessen der Rechtsanwältinnen und Rechtsanwälte sowie von deren Mandaten frühzeitig vertreten werden und deren Perspektive als Betroffene in den Blick genommen wird.

- Der Anwaltsverband Baden-Württemberg fordert, dass die Evaluierungsberichte dem Landtag vorzulegen sind, um diesem Korrekturen am vorliegenden Gesetz zu ermöglichen. Zudem sollte der Landtag auch unterrichtet werden, welche KI-Versionen jeweils eingesetzt werden.

Haltung der Landesregierung

Die Erprobungszeit nach § 17a Absatz 4 Satz 2 wurde aufgrund der Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Zuge der frühzeitigen Beteiligung bereits von drei auf zwei Jahre verkürzt. Eine weitere Verkürzung würde die Möglichkeit zur Erprobung unverhältnismäßig stark einschränken. Außerdem handelt es sich bei den weiteren Fristen um Maximalfristen; es ist damit zu rechnen, dass eine Regelung in der Rechtsverordnung nach Vorlage der Erprobungsberichte nicht erst nach zwei Jahren erfolgen wird, da nur so die Möglichkeit besteht, dass eine Vielzahl von Behörden den KI-Einsatz auf einer einheitlichen rechtlichen Grundlage ohne die besonderen Anforderungen an einen Erprobungszeitraum durchführen können.

Eine gesetzliche Absicherung der Einbeziehung der Rechtsanwaltskammern in die Evaluierung der jeweiligen Behörde ist nicht sachgerecht, da eine einseitige und starre Vorgabe andere wichtige Interessen unberücksichtigt lässt. Über mögliche Beteiligungen an der Erarbeitung des jeweiligen Evaluierungsberichtes entscheidet jede Behörde eigenständig. Die Landesregierung wird die Rechtsanwaltskammern im Zuge der Anhörung zu einer Rechtsverordnung nach § 17a Absatz 5 EGovG BW beteiligen, um deren Sichtweise einbeziehen und gegebenenfalls berücksichtigen zu können.

Durch die im vorliegenden Gesetzentwurf vorgesehene Verordnungsermächtigung der Landesregierung ist eine gesetzliche verankerte Übermittlung der Evaluierungsberichte an den Landtag nicht erforderlich, da die Zulassung für die reguläre Anwendungspraxis durch Rechtsverordnung der Landesregierung erfolgt. Die Vorgaben des Artikels 61 Absatz 1 des Landesverfassung zum Verordnungserlass werden durch die Formulierung des Absatzes 5 eingehalten. Im Übrigen steht es dem Landtag frei, die gesetzlichen Grundlagen für die Zulassung zu ändern oder diese selbst zu schaffen.

Ergänzender Vorschlag

- ZENDAS hält eine normenklare Rechtsgrundlage für den Abruf der Identifikationsnummer zur Zulassung zum Hochschulstudium für erforderlich. § 6 Absatz 2 IDNrG sei dafür keine ausreichende Ermächtigungsgrundlage. ZENDAS schlägt vor zu prüfen, ob dies im Rahmen dieses Gesetzgebungsverfahrens erfolgen könne.

Haltung der Landesregierung

Im Zusammenhang mit Register-Nummer 25 nach Anlage zu § 1 IDNrG („bei den allgemeinbildenden und beruflichen Schulen, Schulbehörden, Bildungseinrichtungen nach § 2 des Hochschulstatistikgesetzes systematisch geführte personenbezogene Datenbestände zu Bildungsteilnehmenden“) werden die fachspezifischen Umsetzungsfragen durch eine Arbeitsgruppe innerhalb der Kultusministerkonferenz behandelt und damit außerhalb dieses Gesetzgebungsverfahrens aufgelöst. Eventuell erforderliche gesetzliche Anpassungen können erst nach Beendigung dieser Arbeit erfolgen.

c) Zur Änderung des LIFG

- Der LfDI hält die Kombination von informationsbezogenen und stellenbezogenen Bereichsausnahmen in einer Norm für systemwidrig. Zusätzlich führe die Verwendung von unbestimmten Rechtsbegriffen und der weite Anwendungsbereich zu Schwierigkeiten bei der Rechtsanwendung und zu einem erhöhten bürokratischen Aufwand. Die vorgesehene Erweiterung der Bereichsausnahme zum Schutz der Wissenschaftsfreiheit hält der LfDI für nicht erforderlich; der VGH BW habe in seiner Entscheidung vom 25.10.2023 (10 S 125/22) gerade keine verfassungsrechtlichen Bedenken an der bisherigen Regelung geäußert. Jedenfalls sollte der Zugang erst im Falle einer „Beeinträchtigung“ der Kunst- und Wissenschaftsfreiheit und nicht bereits bei einer „Betroffenheit“ derselben ausgeschlossen sein. Die Aufnahme einer Regelung zum Schutz der Informationen im Bereich der Kirchen, Religions- und Weltanschauungsgemeinschaften als Konsequenz aus der Rechtsprechung des VGH BW (10 S 916/22) befürwortet der LfDI hingegen; eine entsprechende Regelung sollte aber in § 6 LIFG und nicht in § 2 LIFG verortet werden. Zudem sei der Begriff der „Angelegenheiten“ nicht normenklar und werde zu Auslegungsschwierigkeiten führen.

- Die Universität Tübingen sowie das KIT schlagen vor, die bisherige stellenbezogene Bereichsausnahmeregelung zugunsten der Kunst- und

Wissenschaftsfreiheit beizubehalten und um weitere Stellen, insbesondere um die „zuständige Behörde gemäß § 8 Absatz 1 Tierschutzgesetz“ zu erweitern.

Haltung der Landesregierung

Eine Systemwidrigkeit kann nicht erkannt werden; auch in anderen landesrechtlichen Regelungen werden sowohl stellen- als auch informationsbezogene Bereichsausnahmen in einer Vorschrift geregelt, vgl. etwa § 5 Hamburgisches Transparenzgesetz sowie § 81 Hessisches Datenschutz- und Informationsfreiheitsgesetz. Systematisch soll der gesamte Bereich der Kunst- und Wissenschaftsfreiheit sowie der Bereich der Kirchen, Religions- und Weltanschauungsgemeinschaften ausgenommen werden, mithin handelt es sich dem Wesen nach um eine Bereichsausnahme. Daher wäre eher die Verortung in den Ablehnungsgründen der §§ 4-6 LIFG systemfremd; zudem fügen sich die Ausnahmen zum Schutz der Kunst- und Wissenschaftsfreiheit sowie des religionsgemeinschaftlichen Selbstbestimmungsrechts dort auch inhaltlich nicht ein, da es sich weder um besondere öffentliche Belange (§ 4 LIFG), um personenbezogene Daten (§ 5 LIFG) noch um geistiges Eigentum oder Betriebs- und Geschäftsgeheimnisse (§ 6 LIFG) handelt. Schließlich würde eine Verortung in den §§ 4-6 LIFG konsequenterweise die Notwendigkeit einer Drittbeteiligung nach § 8 LIFG auslösen – zumindest, wenn die Informationen von einer privaten Stelle stammen. Dies würde das Verfahren unnötig verkomplizieren. Sollte die informationspflichtige Stelle alleine nicht beurteilen können, ob die ihr vorliegenden Informationen unter die Bereichsausnahme nach § 2 Absatz 3 Nummer 5 bzw. Nummer 6 LIFG fallen, steht es ihr frei – den allgemeinen Grundsätzen des Verwaltungsverfahrens nach § 24 LVwVfG entsprechend – zur Sachverhaltsaufklärung die übermittelnde Stelle dennoch einzubeziehen.

Die vorgesehene Erweiterung der Bereichsausnahme zum Schutz der Wissenschaftsfreiheit ist verfassungsrechtlich geboten: In dem der Entscheidung des VGH BW (10 S 125/22) zugrundeliegenden Einzelfall stellte der Tierschutz einen legitimen Eingriffsgrund dar, da diesem über Artikel 20a GG ebenfalls Verfassungsrang zukommt. Daher hat der VGH BW auf eine Vorlage an das Bundesverfassungsgericht oder den Verfassungsgerichtshof verzichtet. Ist in einer anderen Fallkonstellation jedoch kein Eingriffsgrund mit Verfassungsrang gegeben, käme allenfalls ein Rückgriff auf die Wissenschaftsfreiheit selbst als verfassungsunmittelbarer Ablehnungsgrund in Frage. Einem Rückgriff auf Ablehnungsgründe direkt aus der Verfassung steht jedoch die Regelungssystematik des LIFG entgegen (vgl. VGH BW vom 08.11.2023 – 10 S 916/22). Demnach kann

ergänzend zu den im LIFG normierten Ausschlussgründen nicht unter Verweis auf verfassungsmäßige Rechte auf ungeschriebene Versagungsgründe zurückgegriffen werden, da das LIFG ein abgeschlossenes System von Bereichsausnahmen (§ 2 Absatz 2 und 3 LIFG) und Ausschlussgründen (§§ 4 bis 6 LIFG) enthalte.

Die im Rahmen der neuen Regelung des § 2 Absatz 3 Nummer 5 LIFG gewählte Terminologie der „Betroffenheit“ wurde auch schon in der bisherigen gesetzlichen Regelung des § 2 Absatz 3 Nummer 2 LIFG so verwendet: „[…] soweit Forschung, Kunst, Lehre, Leistungsbeurteilungen und Prüfungen betroffen sind […]“. Würde man stattdessen eine „Beeinträchtigung“ der Kunst- oder Wissenschaftsfreiheit voraussetzen, würde dies zu einer Absenkung des bisherigen Schutzniveaus führen, was gerade nicht bezweckt ist.

Der in der neuen Regelung des § 2 Absatz 3 Nummer 6 LIFG verwendete Begriff der „Angelegenheiten“ ist ausreichend normenklar. Die Begrifflichkeit selbst stammt aus Artikel 137 Absatz 3 Satz 1 WRV. 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. Sie sind hierfür darlegungs- und beweispflichtig. Die „Angelegenheiten“ der Kirchen, Religions- und Weltanschauungsgemeinschaften umfassen dabei Tätigkeiten und Aufgabenbereiche wie etwa Lehre und Kultus, Verfassung und Organisation der Religionsgemeinschaft, Ausbildung von Geistlichen, Definition der Rechte und Pflichten von Mitgliedern, Vermögensverwaltung und wirtschaftliche Tätigkeiten, Erlass und Veröffentlichung des eigenen Rechts sowie etwa karitative Aktivitäten (vgl. m.w.N.: Dürig/Herzog/Scholz/Korioth WRV Artikel 137 Randnummern 26-43).

Der Vorschlag, anstelle der Aufnahme einer informationsbezogenen Bereichsausnahmeregelung zugunsten der Kunst- und Wissenschaftsfreiheit die bisherige stellenbezogene Bereichsausnahmeregelung beizubehalten und um weitere Stellen zu erweitern, wird nicht aufgegriffen. Intention der Neuregelung in Form einer informationsbezogenen Bereichsausnahme zugunsten der Kunst- und Wissenschaftsfreiheit ist es gerade, entsprechende Informationen unabhängig davon zu schützen, bei welcher Stelle sie vorliegen.

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. Die GPA wird neben dem Rechnungshof in die Vorschrift aufgenommen. Nach § 113 Absatz 1 Satz 2 der Gemeindeordnung (GemO) handelt die GPA im Auftrag der Rechtsaufsichtsbehörde unter eigener Verantwortung. In Bezug auf diese Unabhängigkeit ist ihre Prüftätigkeit der des Rechnungshofs vergleichbar

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

Zu Absatz 3

Das KI-Modell wird in der KI-VO 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. Dies schließt es ein, ihre Einhaltung zu kontrollieren.

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 kann den Bürgerinnen und Bürgern und der Wirtschaft durch Steigerung der Effizienz zugutekommen und ist für die Zukunft der digitalen 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. Es bleibt aber zu betonen, dass der Anonymisierung jeweils ein legitimer Grund nach der DSGVO in Verbindung mit dem LDSG zugrunde liegen muss; dieser kann beispielsweise in der Forschung für einen bestimmten Zweck oder dem Training von KI für eine bestimmte Aufgabe liegen. Sind besondere Kategorien personenbezogener Daten betroffen, bedarf es einer Legitimation nach Artikel 9 Absatz 2 DSGVO oder einer speziellen Rechtsgrundlage.

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. Die Struktur der Vorschrift orientiert sich 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 von Rechtsansprüchen oder Verteidigung gegen Rechtsansprüche Dritter eingefügt (vgl. Absatz 2 Nummer 3). Damit sind gerichtliche und außergerichtliche Verfahren eingeschlossen. Des Weiteren wurde 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 an Stellen in anderen 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 andere Bestimmung ist in Absatz 4 für Datenübermittlungen auf Ersuchen aufgenommen, die nur für Ersuchen einer inländischen Stelle gelten.

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. Ein Bedürfnis für gemeinsame Dateien kann bestehen, wenn verschiedene öffentliche Stellen gemeinsam in einer Datei arbeiten. Dies kann eine erhebliche Arbeitserleichterung darstellen.

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 (z. B. Komm.ONE). 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 vertraglichen 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, ggf. auch in abstrakter Form, 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 zur Aufgabenerfüllung 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. In Bezug auf besondere Kategorien personenbezogener Daten bedarf es zusätzlich

einer Legitimation nach Artikel 9 Absatz 2 DSGVO oder einer speziellen Rechtsgrundlage.

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. Entscheidend für die Verwendung personenbezogener Klardaten für das Training ist also, dass die beabsichtigte Art und Qualität der Ergebnisse, die durch das KI-System erzeugt werden, nicht mit anonymen oder pseudonymen Daten herbeigeführt werden kann.

Für das Training mit besonderen Kategorien personenbezogener Daten wird regelmäßig die Pseudonymisierung der Daten erforderlich sein. Vorrangig ist auch hierfür das Training mit anonymen Daten.

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 Frage- und Informationsrecht mit dem aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundrecht auf informationelle Selbstbestimmung in Einklang zu bringen. Denn der Informationsanspruch der 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)

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.

n 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 wie bisher 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. Neben der Verpflichtung der öffentlichen Stelle nach Absatz 3 zur Datenminimierung vor der Weitergabe ist der Empfänger von der übermittelnden öffentlichen Stelle zu verpflichten. Dementsprechend muss der Empfänger die Daten, sofern dies nicht bereits erfolgt ist, 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 Nachweiseüber die Einhaltung der Verpflichtungen 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. In Absatz 2 Satz 2 ist ein Bezug auf Satz 1 eingefügt. Es darf auch für diese Verarbeitung kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

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 zur Minimierung der Datenverarbeitung zu treffen sind. Weitere Anforderungen an die Authentifizierung können sich auch aus Vorschriften zur Datensicherheit ergeben. 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. In diesem Fall unterbleibt die Verarbeitung. Auf das Widerspruchsrecht ist hinzuweisen.

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

Regelungsbedarf besteht aus den folgenden Gründen:

- Die Beschränkung des Videoschutzes auf den Schutz bestimmter Objekte und Personen verengt den Anwendungsbereich zu stark. Videoüberwachung sollte generell zur Erfüllung öffentlicher Aufgaben herangezogen werden können, wenn dies im Einzelfall erforderlich ist.

- 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 soll als besonders wichtiges öffentliches Interesse herausgestellt werden.

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

- Zum Schutz von Leib oder Leben von Personen sowie 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 können.

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 neu)

Zu Satz 1

In § 18 Absatz 1 Satz 1 wird die Beschränkung auf den Schutz bestimmter Objekte und Personen aufgehoben. Gemäß Artikel 6 Absatz 1 Buchst. e DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie für die Erfüllung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Umfasst sind Aufgaben, die in der Zuständigkeit der jeweiligen öffentlichen Stelle liegen. Maßgebend sind die spezifischen Bestimmungen der Aufgabennorm. Die Videoüberwachung muss für die Erfüllung der öffentlichen Aufgabe erforderlich sein; sie braucht aber nicht die eigentliche Aufgabenerfüllung darzustellen. Sofern die Videoüberwachung die Aufgabenerfüllung unterstützen kann, kann ihr Einsatz zulässig sein. Zu betonen ist aber, dass weiterhin die Erforderlichkeit im Einzelfall gegeben sein muss, also eine konkrete oder abstrakte Gefahrenlage vorliegen muss, was die regelmäßige Anwendung ausschließt. Sofern optisch-elektronische Systeme regelmäßig eingesetzt werden sollen, bedarf es einer spezialgesetzlichen Grundlage.

Der Hauptanwendungsfall wird weiterhin sein, Gefahren für Personen und Objekte im Verantwortungsbereich der öffentlichen Stelle in Ausübung ihrer Schutzpflicht abzuwenden. Öffentlichen Stellen obliegt nach der gefestigten Rechtsprechung des Bundesverfassungsgerichts die Schutzpflicht als rechtliches Gebot, Maßnahmen zum Schutz von Rechtsgütern Dritter zu treffen (vgl. z. B. BVerG Beschluss des Ersten Senats vom 24. März 2021 im Zusammenhang mit Klimaschutz, 1 BvR 2656/18, 1 BvR 78/20, 1 BvR 96/20, 1 BvR 288/20). Die Schutzpflicht des Staates ist fester Bestandteil der Rechtsprechung des Bundesverfassungsgerichts. Sie folgt aus den Grundrechten, im Kontext der Videoüberwachung maßgeblich zum Schutz von Leben, Gesundheit, Freiheit oder Eigentum von Personen.

Hierdurch wird beispielsweise die Möglichkeit eröffnet, gegen illegale Müllablagerungen vorzugehen, wenn von diesen erhebliche Gefahren ausgehen, zu deren Beseitigung öffentliche Stellen im Sinne des § 2 Absatz 1 verpflichtet sind (z. B. Gesundheitsgefahren durch gefährliche Stoffe, Ratten, gefährliche Lagerung etc.). Ebenso könnte die Videoüberwachung an Umsteigeknoten des öffentlichen Personennahverkehrs zur Verfügung stehen, soweit dort eine Schutzpflicht öffentlicher Stellen besteht. Dies kann vor allem in Bezug auf die dortigen baulichen Anlagen sowie zum Schutz von sich dort aufhaltenden Personen der Fall sein. In Bezug auf öffentliche Verkehrsmittel und deren Einstiegsbereich ist § 18 LDSG nur anwendbar, wenn die Verkehrsmittel von öffentlichen Stellen betrieben werden, die dem LDSG unterfallen.

Vergleichbare Regelungen finden sich in anderen Landesgesetzen, beispielsweise in Rheinland-Pfalz (§ 21), Berlin (§ 20) oder Hamburg (§ 9) sowie im Bundesdatenschutzgesetz (§ 4).

Vorrangig bleiben fachgesetzliche Regelungen. Diese bleiben nach dem Wesentlichkeitsgrundsatz erforderlich, wenn die Videoüberwachung besonders eingriffsintensiv ist.

Wegen des als Ausprägung des allgemeinen Persönlichkeitsrechts verfassungsrechtlich verbürgten Grundrechts auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes muss die Anwendung der Vorschrift nach dem Verhältnismäßigkeitsprinzip erfolgen. Es ist jeweils zu prüfen, ob die Maßnahme der Videoüberwachung, geeignet, erforderlich und angemessen ist. Dies kommt in der Vorschrift hinreichend zum Ausdruck, indem auf den Einzelfall und die Erforderlichkeit abgestellt wird, außerdem eine Abwägung mit den schutzwürdigen Interessen der betroffenen Personen erfolgen muss.

Zu beachten ist die Abgrenzung zur Videoüberwachung nach dem PolG. Das LDSG beruht auf der DSGVO, die nach Artikel 2 Absatz 2 Buchst. d keine Anwendung findet auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Der Schutz der öffentlichen Sicherheit und Ordnung wird grundsätzlich durch die Polizei gewährleistet. Den Ordnungs- und Sicherheitsbehörden steht zur Kriminalitätsbekämpfung die Videoüberwachung nach dem PolG zur Verfügung. Videoüberwachung nach dem LDSG zielt in Abgrenzung zum Polizeigesetz nicht darauf, Straftaten präventiv und repressiv zu bekämpfen, sondern darauf, zugewiesene Aufgaben außerhalb der Aufgaben nach dem PolG oder Gefahren für Personen und Objekte in Ausübung ihrer Schutzpflicht abzuwenden. Dementsprechend gilt das LDSG gemäß § 2 Absatz 1 Satz 2 Nummer 3 nicht für die Verarbeitung personenbezogener Daten durch die Polizei (§ 104 PolG).

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 Nummer 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. Für die weiteren Informationen, z. B. über den Zweck der Videoüberwachung und die Speicherdauer, muss erkennbar sein, wo diese verfügbar sind. Die Informationspflicht kann beispielsweise durch Anbringung eines QR-Codes mit Bereitstellung der Information an der angegebenen URL oder

der Angabe einer Webseite erfüllt werden. Piktogramme mit der Möglichkeit, die erforderlichen Hinweise aufzunehmen, sind verfügbar. Es sollte auch möglich sein, die Informationen in Textform zu erhalten.

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)

Moderne Videoüberwachung kann mit Hilfe von KI-Systemen effizienter gestaltet werden. Dies könnte auch dazu beitragen, den Eingriff abzumildern, indem nur die für den Überwachungszweck relevanten Verhaltensweisen oder die zu beseitigenden Zustände erfasst werden. Die Zulässigkeit beurteilt sich entsprechend den 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.

Zu Absatz 6 Nummer 1

In Nummer 1 wird Videoüberwachung unter Nutzung von KI-Systemen ermöglicht, soweit dies erforderlich ist, um Leib oder Leben von Personen zu schützen. Ein Anwendungsbeispiel könnte die KI-basierte Videoüberwachung in öffentlichen Schwimmbädern zur Vermeidung von Ertrinkungsunfällen sein.

Zu Absatz 6 Nummer 2

Des Weiteren kann Videoüberwachung unter Nutzung von KI-Systemen 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.

Neben § 3a wird hiermit 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.

Auch hier wird mit der Zulassung im Einzelfall das Bestehen einer Gefahrenlage vorausgesetzt, wobei das Bestehen einer konkreten oder 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. Möglich wäre es z. B., die Videoüberwachung durchzuführen, wenn nicht mit der Anwesenheit von Personen zu rechnen ist.

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 § 31 Satz 1 SGB X (ähnlich auch § 155 Absatz 4 Satz 1 der Abgabenordnung), wonach ein Verwaltungsakt vollständig durch automatische Einrichtungen erlassen werden kann, wenn „kein Anlass besteht, den Einzelfall durch Amtsträger zu bearbeiten“. Auf die dazu ergangene Rechtsprechung kann zur Konkretisierung grundsätzlich zurückgegriffen werden. Da im Bereich des allgemeinen Verfahrensrechts noch unterschiedlichere Fallkonstellationen als im Rahmen des SGB X und der Abgabenordnung in Betracht kommen, erfolgt eine weitere Konkretisierung dadurch, dass vorausgesetzt wird, dass „die Angaben derjenigen, für die der Verwaltungsakt bestimmt ist oder die von ihm betroffen werden, keine vom Regelfall abweichenden Hinweise enthalten.“

Eine § 31 Satz 2 SGB X entsprechende Regelung zur Berücksichtigung von für den Einzelfall bedeutsamen tatsächlichen Angaben des Beteiligten ist bereits in § 24 Absatz 1 Satz 3 LVwVfG enthalten.

Zu Absatz 3

Mit der Anzeigepflicht nach Absatz 3 mindestens einen Monat vor Aufnahme des Verfahrens bei der obersten Fachaufsichtsbehörde bzw. zuständigen Rechtsaufsichtsbehörde 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.

Sofern eine Behörde für ihre Tätigkeit keiner obersten Fachaufsichtsbehörde untersteht (wie beispielsweise die Berufskammern oder die Gemeinden im Bereich der freiwilligen Aufgaben oder Pflichtaufgaben ohne Weisung), ist die zuständige Rechtsaufsichtsbehörde stattdessen entsprechend zu informieren.

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.

Sofern eine Behörde für ihre Tätigkeit keiner obersten Fachaufsichtsbehörde untersteht (wie beispielsweise die Berufskammern oder die Gemeinden im Bereich der freiwilligen Aufgaben oder Pflichtaufgaben ohne Weisung), ist die zuständige Rechtsaufsichtsbehörde stattdessen entsprechend zu informieren.

Bestandteil des Evaluierungsberichtes ist regelmäßig die Datenschutz-Folgeabschätzung nach der DSGVO bzw. die Grundrechts-Folgeabschätzung nach der KI-VO, sofern diese aufgrund des technischen Ansatzes der Erprobung erstellt werden mussten.

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 in Bezug auf Leistungsbeurteilungen und Prüfungen beibehalten. Dies ist aus Gründen der Rechtssicherheit erforderlich, da diesbezügliche Informationen nicht in jedem Falle unter die neue Bereichsausnahmeregelung in Nummer 5 fallen würden.

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.

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 47/84) 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.

Baden-Württemberg
Normenkontrollrat

Stellungnahme des Normenkontrollrates Baden-Württemberg gem. Nr. 4.1 VwV NKR BW

14.05.2025

Gesetz zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze

NKR-Nummer 60/2025, Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg

Der Normenkontrollrat (NKR) Baden-Württemberg hat sich mit dem Entwurf des oben genannten Regelungsvorhabens befasst.

I. Im Einzelnen

Durch das Artikelgesetz werden geändert das Landesdatenschutzgesetz (LDSG), das E-Government-Gesetz Baden-Württemberg, das Gesetz zur Ausführung des Personenstandsgesetzes, das Landesinformationsfreiheitsgesetz (LIFG), das Landesmediengesetz und die Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten.

1.

Landesdatenschutzgesetz (LDSG)

Mit der Änderung des LDSG werden die im Evaluierungsbericht zum Landesdatenschutzgesetz vom 8. Oktober 2024 (Landtagsdrucksache 17/7596) festgestellten Änderungsbedarfe umgesetzt, insbesondere:

- Regelungen für den Einsatz Künstlicher Intelligenz (KI) bei der Verarbeitung personenbezogener Daten (§ 3a).
- Erweiterung der Möglichkeiten der „Datenverarbeitung zu anderen Zwecken“ (§ 5).
- Gesetzliche Grundlage für Auftragsdatenverarbeitung für öffentliche Stellen durch staatliche Behörden (§ 7a).
- Die Verarbeitung personenbezogener Daten zu Zwecken der parlamentarischen Kontrolle wird rechtlich gesondert legitimiert (§ 12a).
- Erweiterte Befugnisse für die Forschung öffentlicher Stellen (§ 13)
- Rechtsgrundlage zur Verarbeitung personenbezogener Daten für die Öffentlichkeitsarbeit (§ 17).
- Videoüberwachung wird zum Schutz von sicherheitsrelevanten Einrichtungen, Dienstgebäuden, Dienstfahrzeugen, Kulturgütern und öffentlichen Verkehrsmitteln abstrakt-generell als verhältnismäßiges Mittel zugelassen. Flankierend wird die Speicherfrist auf zwei Monate erhöht (bisher vier Wochen) und die Informationspflichten der öffentlichen Stellen zugunsten der betroffenen Personen erweitert (§ 18).

- Rechtsgrundlage zur Videoüberwachung einschließlich der KI-Nutzung in nicht öffentlich zugänglichen Räumen (§ 18a).

- Rechtsgrundlage zum Einsatz sonstiger technischer Mittel mit KI-Unterstützung zur Überwachung von Bauwerken und Infrastruktur (§ 18b).

2.

E-Government-Gesetz Baden-Württemberg

Verwaltungsakte, bei denen weder ein Ermessen noch ein Beurteilungsspielraum besteht, können automatisiert und durch Nutzung von KI erlassen werden. Regelungen zur Erprobung und Evaluation werden flankierend getroffen.

3.

Gesetz zur Ausführung des Personenstandsgesetzes

Regelung des automatisierten Zugriffs der Fachaufsicht auf die elektronischen Sammelakten der Standesämter.

4.

Landesinfomationsfreiheitsgesetz (LIFG)

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

5.

Landesmediengesetz

Anpassung an bundesgesetzliche Vorschriften und an den Fünften Medienstaatsvertrag.

6.

Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten

- Als zuständige Verwaltungsbehörde für die Bußgeldvorschrift des § 28 Absatz 1 Nummer 12 Gesetz über den Datenschutz u. den Schutz der Privatsphäre in der Telekommunikation u. bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG) wird der Landesbeauftragte für den Datenschutz u. die Informationsfreiheit (LfDI) bestimmt.

- Die Zuständigkeit für die Ordnungswidrigkeit nach § 33 Absatz 1 Digitale-Dienste-Gesetz (DDG) wird der Landesanstalt für Kommunikation übertragen (bisher Regierungspräsidium Karlsruhe)

II. Votum

Der NKR begrüßt es, dass das LDSG einer Evaluierung unterzogen wurde und die darin festgestellten Änderungsbedarfe umgesetzt werden sollen. Auch im Rahmen des Rechtsregimes der unmittelbar geltenden Datenschutz-Grundverordnung (DSGVO) sind Spielräume der Rechtsgestaltung und Spezifizierung vorhanden. Er begrüßt, dass der Landesgesetzgeber diese Spielräume nutzt und kein „Gold Plating“ mehr betreiben möchte (§ 2 Absatz 3 Satz 1 LDSG).

Folgende Aspekte hält der NKR insbesondere für erwähnenswert:

1.

Die Begriffsbestimmungen in § 2a LDSG mögen rechtsverweisungstechnisch korrekt sein; für den Normadressaten oder die Normadressatin sind sie jedoch nicht nutzerfreundlich. Dieser oder diese muss im Zweifelsfall neun andere europarechtliche Vorschriften sichten.

2.

Der NKR begrüßt es, dass in § 7a Absatz 1 LDSG nunmehr ausdrücklich klargestellt wird, dass auch eine Behörde im Auftrag einer anderen öffentlichen Stelle eine Auftragsdatenverarbeitung im Sinne des Artikels 28 DSGVO erbringen kann.

Er ist jedoch nicht überzeugt davon, dass hierfür eine Rechtsverordnung der Landesregierung für die Nutzungsbedingungen erforderlich ist (§ 7a Absatz 2 LDSG), nachdem der Inhalt eines Auftragsdatenverarbeitungsvertrages in Artikel 28 DSGVO geregelt ist.

3.

In § 8 LDSG (Beschränkung der Informationspflicht) soll ein Absatz 2 aufgenommen werden, der die öffentlichen Stellen verpflichtet, *„geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der (…) genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“* zu ergreifen.

Das Ressort führt dazu in der Gesetzesbegründung aus, dass eine auf Artikel 23 Absatz 2 DSGVO beruhende zwingende Regelung bislang fehlte und die entsprechenden Regelungen nunmehr in Anlehnung an §§ 32, 33 Bundesdatenschutzgesetz (BDSG) getroffen werden. Dies überzeugt den NKR nicht. Die Bereitstellung öffentlicher Informationen bei unterbliebener individueller Information, die noch dazu gesteigerten Anforderungen an Sprache, Zugänglichkeit etc. unterliegen, erachtet der NKR als unnötige bürokratische und auslegungsbedürftige Informationspflicht für öffentliche Stellen. Wie das Ressort in der Gesetzesbegründung selbst ausführt, besteht ohnehin eine Pflicht zur Nachholung der Information, sobald der vorübergehende Hinderungsgrund entfallen ist („soweit und solange“ in § 8 Absatz 1 LDSG). Der NKR ist der Ansicht, dass es damit – wie schon bisher - sein Bewenden haben kann.

4.

Der NKR begrüßt es, dass das Recht auf Berichtigung und Löschung von mit KI-Systemen und KI-Modellen verarbeiteten personenbezogenen Daten beschränkt wird (§§ 9a, 10 Absatz 4 LDSG). Damit können unverhältnismäßige Aufwände vermieden werden.

5.

Der NKR begrüßt es, dass in § 11a LDSG eine Ermächtigungsgrundlage geschaffen wird für die Weiterverarbeitung von personenbezogenen Daten durch öffentliche Stellen zum Zwecke der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von KI-Systemen und KI-Modellen.

Er appelliert aber an die Landesregierung, die Anforderungen an Zweckbindung und Rechtfertigung im Gleichklang mit der KI-Verordnung zu regeln und nicht darüber hinaus zu gehen.

6.

Der NKR begrüßt es, dass die Zwecke der Verarbeitung personenbezogener Daten der besonderen Kategorien im Dienst- u. Arbeitsverhältnis erweitert wurden um Anliegen der Gesundheitsvorsorge, Arbeitsmedizin, Arbeitsfähigkeit (§ 15 Absatz 2 Satz 2 LDSG).

Der NKR regt hinsichtlich der in § 15 Absatz 9 LDSG neu geschaffenen Informationspflicht an zu prüfen, ob diese „*ergänzend zu den Informationspflichten nach der KI-VO und der DSGVO*“, wie es die Gesetzesbegründung ausführt, erforderlich sind.

7.

Der NKR begrüßt es, dass mit der Änderung des LDSG die Videoüberwachung von sicherheitsrelevanten Einrichtungen, Dienstgebäuden, Dienstfahrzeugen, Kulturgütern und öffentlichen Verkehrsmitteln erleichtert wird (§ 18 LDSG). Die aufwändige Vorrangprüfung anderer Mittel entfällt damit künftig in diesen Bereichen. Allerdings regelt das Ressort zugleich eine Erweiterung der Informationspflichten zugunsten der betroffenen Personen. Der NKR sieht hierfür keine Erforderlichkeit und ist der Auffassung, dass getroffene verhältnismäßige Erleichterungen nicht mit neuen Erschwernissen „bezahlt“ werden sollten.

8.
Der NKR begrüßt es des Weiteren, dass die Rechtsgrundlagen geschaffen werden, in bestimmten Fällen Verwaltungsakte vollständig automatisiert einschließlich der Nutzung von KI erlassen zu können (§ 17 a E-Government-Gesetz Baden-Württemberg). Dies kann langfristig zu einer erheblichen Verwaltungsvereinfachung führen.

Der NKR ermuntert das Ressort, auch weiterhin und außerhalb einer förmlichen Evaluierung Anregungen aus der Praxis aufzugreifen, die geeignet sind, rechtmäßige Vereinfachungen im Datenschutzrecht und in der datenschutzrechtlichen Praxis herbeizuführen.

Des Weiteren regt der NKR an, – soweit erforderlich - Regelungen vorzusehen, die einen verwaltungsarmen Abgleich mit dem Registermodernisierungsgesetz ohne weiteres erlauben.

gez. Dr. Dieter Salomon
Vorsitzender

gez. Adrian Probst
Berichterstatter