



Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg | Postfach 10 29 32 | 70025 Stuttgart

Innenministerium
Willy-Brandt-Str. 41
70173 Stuttgart

Nur per E-Mail an:

Nachrichtlich an:

Name	Dr. Wacke
Leitender Beamter	
Telefon	+49 711 615541
E-Mail	poststelle@lfdi.bwl.de
Geschäftszeichen	LfDILB-0557 0-19/1 (bei Antwort bitte angeben)
Datum	15.10.2025

Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze

Ihr Schreiben vom 23.09.2025

Ihr Zeichen. IM2-0557-54/8/3

Sehr geehrter ,
sehr geehrte ,
sehr geehrte Damen und Herren,

für die Gelegenheit zur Stellungnahme zum vorgelegten Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze danken wir sehr.

Vorab nehmen wir auf unsere Stellungnahme gegenüber dem Innenministerium vom 10. Juni 2025 zu einem früheren Stand des Entwurfs Bezug und halten an unseren dort geltend gemachten Äußerungen fest, soweit nicht durch die nunmehr vorgelegte Fassung Abhilfe geschaffen wurde.

Zum dem nunmehr vorgelegten Gesetzentwurf nehmen wir wie folgt Stellung:

Zu Artikel 1 – Änderung des Landesdatenschutzgesetzes (LDSG)

Vorbemerkungen:

Im Folgenden bezeichnet die Abkürzung „LDSG-E“ die Fassung des Gesetzes, die sich ergeben würde, wenn der Gesetzentwurf in der vorgelegten Form umgesetzt würde. Die Bezeichnung „LDSG“ steht dagegen für das Landesdatenschutzgesetz in seiner bisherigen Fassung. Wir nehmen im Folgenden zumindest partiell auch insoweit Stellung, als wir einen Anderungsbedarf an der bisherigen Fassung des Landesdatenschutzgesetzes erkennen, dem der Entwurf bislang nicht nachkommt.

Soweit wir im Folgenden auf unsere Stellungnahme von 2020 Bezug nehmen, ist damit unser Schreiben zur Evaluierung des Landesdatenschutzgesetzes vom 6. November 2020 gemeint. Soweit wir auf unsere Stellungnahme aus dem Jahr 2024 Bezug nehmen, bezieht sich dies auf unser Schreiben „Stellungnahme zur Evaluierung des Landesdatenschutzgesetzes“ vom 13. Februar 2024, Az.: 0557.0-1/1/3.

Die Bezeichnung „Abschlussbericht des Innenministeriums zur Evaluierung des Landesdatenschutzgesetzes“ bezieht sich auf den Bericht Stand Juli 2024.

Zu § 2 LDSG:

Zur beabsichtigten Änderung von § 2 Absatz 1 Satz LDSG

In Absatz 1 Satz 2 sollen gemäß dem Entwurf nach dem Wort „dieses“ die Wörter „oder ein anderes“ eingefügt werden.

Der Vorrang anderer Gesetze ergibt sich jedoch schon aus § 2 Absatz 3. Die Einfügung ist mithin entbehrlich und führt eher zu Missverständnissen, inwieweit ohne eine gegenüber § 2 Absatz 3 spezielle Regelung des Vorrangs das Landesdatenschutzgesetz doch Vorrang haben könnte. Wir empfehlen daher, von der Einfügung der Wörter „oder ein anderes Gesetz“ abzusehen.

Zum bestehenden § 2 Absatz 3 LDSG

Auf die Kritik zu Auslegungsschwierigkeiten (insbesondere bei der Formulierung „Ermittlung des Sachverhalts“) in unseren früheren Stellungnahmen von 2020 und 2024 nehmen wir Bezug. Wir empfehlen, die nach dem Abschlussbericht des Innenministeriums zur Evaluation des Landesdatenschutzgesetzes vorgesehene Anpassung von § 73 Absatz 1 des Landesverwaltungsverfahrensgesetzes an die Bundesregelung mit diesem Gesetzentwurf vorzunehmen und darüber hinaus - wie zuletzt in unserer Stellungnahme vom 13. Februar 2024 ausgeführt - auch das LDSG anzupassen, um derartige Auslegungsschwierigkeiten in Bezug auf das Verwaltungsverfahrensgesetz zu vermeiden.

Zu § 2 Abs. 5 LDSG-E – Anwendung von Teilen des LDSG auf justizielle Tätigkeit

Soweit nach dem Entwurf das Landesdatenschutzgesetz partiell Anwendung finden soll „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“, konnte die Regelung leerlaufen, wenn für die justizielle Tätigkeit die Bundes-Vorschriften der Prozessordnungen vorgehen und diese abschließend sind. Das Prozessrecht besteht zu großen Teilen aus Regelungen zur Verarbeitung personenbezogener Daten (z. B. über die Beweiserhebung, Wahrheitsfindung allgemein, Begründung und Offenlegung von Entscheidungen etc.). Weshalb der insoweit spezialgesetzlich geregelte Datenschutz einer durch den Landesgesetzgeber ausfüllbaren Öffnung für den Bereich KI-gestützter Datenverarbeitung zugänglich sein soll, bedürfte einer gegenüber dem Entwurf der Gesetzesbegründung deutlich weitergehenden Argumentation.

Mit Blick auf die Gesetzgebungskompetenz dürfte nicht § 1 Absatz 1 Satz 1 Nummer 2 Buchstabe b BDSG, sondern § 1 Absatz 2 BDSG entscheidend sein, wonach spezialgesetzliche Regelungen vorgehen. Das sind grundsätzlich die Prozessordnungen mit Blick auf die Rechtsgrundlagen zum Zweck der Verfahrenserledigung. Die fortschreitende Digitalisierung und technische Entwicklungen ändern an diesem Befund nichts. Denn auch in Bezug hierauf dürfte der Bundesgesetzgeber seine Kompetenzen abschließend wahrgenommen haben und nimmt sie weiter wahr. Beispiele sind etwa die Regelungen zur eAkte und der elektronischen Einreichung und Verarbeitung von Schriftsätzen oder die Durchführung von mündlichen Verhandlungen per Videokonferenz. Insgesamt ist die Diskussion insoweit im Fluss (vgl. die

Gemeinsame Erklärung der Justizministerinnen und Justizminister des Bundes und der Länder zum Einsatz von Künstlicher Intelligenz in der Justiz im Rahmen der Frühjahrs-Justizministerkonferenz 2025 in Sachsen, abrufbar unter: <https://www.justiz.sachsen.de/smj/download/Beschluesse96JuMiKoFruehjahr.pdf>).

Fraglich ist darüber hinaus, ob und wie weit die Erprobung von Systemen der Künstlichen Intelligenz der justiziellen Tätigkeit zuzurechnen ist. Während der EuGH in seinem Urteil vom 24.3.2022 – C-245/20 (X ua/Autoriteit Persoonsgegevens) von der weiten Auslegung des Begriffs „justizielle Tätigkeit“ bei der vorübergehenden Bereitstellung von Unterlagen aus einem Gerichtsverfahren gegenüber Journalisten ausging und damit (auch) unter Beachtung von Art. 55 Abs. 3 DS-GVO Gerichte im Rahmen ihrer „justiziellen Tätigkeit“ von der Aufsichts- und Kontrollkompetenz der Datenschutzbehörden nach Art. 55 Abs. 1 DS-GVO ausnahm, durfte die Erprobung von KI-Anwendungen nach Sinn und Zweck nicht von dieser Ausnahme erfasst sein.

Die Erprobung von KI-Anwendungen lässt keine Beeinträchtigung der richterlichen Unabhängigkeit befürchten. Die Entwurfsbegründung weist zu Recht darauf hin, dass die mit Hilfe von KI-Systemen und KI-Modellen insbesondere im Rahmen von elektronischen Aktenführungssystemen, Datenbanken und digitalen Kommunikationssystemen verarbeiteten personenbezogenen Daten besonders schutzwürdig sind. Dieser Wertung trägt auch die KI-VO Rechnung, die die Erprobung von KI-Systemen für den Einsatz im Rahmen der justiziellen Tätigkeit in Artikel 6, Anhang III Nr. 6 und 8, Artikel 57, 59, 60 KI-VO besonderen Vorgaben zuführt. Soweit KI-Systeme bei der Erprobung personenbezogene Daten verarbeiten, ist gemäß Art. 57 Abs. 10 KI-VO die Datenschutzbehörde einzubeziehen.

Selbst wenn also die teilweise Erweiterung des LDSG auf den justiziellen Bereich eine verfassungsrechtlich zulässige Maßnahme darstellen sollte, unterliegt die Erprobung von KI-Systemen der Aufsichts- und Kontrollkompetenz der Datenschutzbehörden nach Art. 55 Abs. 1 DS-GVO.

Zu den in Bezug genommenen Regelungen und die Begriffsbestimmungen in § 2a verweisen wir auf unsere dortigen jeweiligen Ausführungen. Für uns nicht ohne weiteres erkennbar ist, wieso auf § 4 Absatz 2 LDSG-E Bezug genommen werden soll, in dem u. a. eine Befugnis zur Herstellung synthetischer Daten geregelt werden soll. An welchen Anwendungsfällen außerhalb der Verwaltungstätigkeit der Gerichte ist hier gedacht? Die Begründung verhält sich hierzu

bislang nicht. Unklar ist schließlich, warum ausdrücklich „Abschnitt 5“ für nicht anwendbar erklärt wird. Dass außerhalb der Verwaltungsangelegenheiten Abschnitt 5 nicht gilt, ergibt sich schon aus Satz 1. Die explizite Erwähnung von Abschnitt 5 in Satz 2 (2. Halbsatz) lässt daher die Frage aufkeimen, ob außer den in Satz 2 (1. Halbsatz) erwähnten Normen des LDSG vielleicht doch auch noch andere Regelungen des LDSG außerhalb von Abschnitt 5 zur Anwendung kommen sollen.

Zu § 2a LDSG-E:

Zu § 2a Absatz 1 LDSG-E

Die Geltung der Begrifflichkeiten aus der DS-GVO ergibt sich aus § 1 LDSG. Die Einführung ist mithin entbehrlich.

Zu § 2a Absatz 3 LDSG-E

Wir begrüßen die Klarstellung in § 2a Absatz 3, wonach „KI-Modelle für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen“ eingeschlossen sind. Dies weicht von Artikel 3 Nr. 63 KI-VO insofern ab, als dass dort „KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden,“ von der Regelung ausgenommen sind.

Aus Absatz 3 und der dazugehörigen Begründung geht hervor, dass der Begriff „KI-Modell“, der gemäß der KI-VO KI-Modelle mit allgemeinem Verwendungszweck umfasst, um KI-Modelle mit spezifischem Verwendungszweck erweitert werden soll. Hierbei wird auf den Erwagungsgrund 97 Satz 6 bis 8 zur KI-VO verwiesen. In Satz 1 von des Erwagungsgrundes 97 wird jedoch die Notwendigkeit einer klaren Abgrenzung zwischen KI-Modellen mit allgemeinem Verwendungszweck und KI-Systemen im Sinne der Rechtssicherheit betont. Das Beispiel der Nutzerschnittstelle in Erwagungsgrund 97 verstehen wir so, dass durch die Nutzerschnittstelle der Zweck festgelegt wird, wodurch kein allgemeiner Verwendungszweck mehr gegeben ist.

Nach unserer Auffassung sollte eine KI, die spezifisch dazu dient, beispielsweise Baugenehmigungsanträge oder Gerichtsakten zu strukturieren (siehe Begründung), den KI-

Systemen zugeordnet werden. Eine Erweiterung der Definition von KI-Modellen und damit eine Abweichung von der bestehenden Definition in der KI-VO erscheint uns im Hinblick auf die Rechtsklarheit nicht sinnvoll und steht zudem im Widerspruch zur KI-VO.

Zu § 3 LDSG:

Zu § 3 Absatz 1:

Wir begrüßen die in Absatz 1 vorgenommene Klarstellung, die helfen kann, Missverständnisse zur bestehenden Verpflichtung, technische und organisatorische Maßnahmen zu treffen, zu vermeiden

Nach wie vor ist aber unklar, inwieweit es in der Norm um eine bloße Wiederholung oder um eine Modifizierung der Verpflichtung zur Durchführung technischer und organisatorischer Maßnahmen aus Artikel 24, 25 und 32 DS-GVO gehen soll (wie die Entwurfsbegründung nahelegt), wobei für eine Modifizierung eine entsprechende Öffnungsklausel in der Datenschutz-Grundverordnung nicht bestehen würde, oder inwieweit spezifische Maßnahmen im Sinne von Art. 6 Absatz 2 und 3 DS-GVO für die Verarbeitung personenbezogener Daten durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung normiert werden sollen, wobei die Regelungen allerdings nicht spezifisch genug wären. Infolge des Verweises in § 17 Absatz 3 LDSG-E soll die Norm offenbar zugleich eine Regelung „spezifischer Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ bei der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Absatz 2 Buchstabe g DS-GVO darstellen, wobei für die Verarbeitung dieser besonders schutzwürdigen Datenkategorien nur wenig speziellere Maßnahmen vorgesehen werden (s. dazu noch unten bei § 17). Überdies bildet die Norm teilweise die Pflichten aus dem Unionsrecht nur unvollständig ab, etwa in Bezug auf die Verarbeitung durch Auftragsverarbeiter.

Wir halten daher die Norm auch in der Fassung des Entwurfs nicht für den europarechtlichen Anforderungen genügend und empfehlen deswegen weiterhin - wie in unseren Stellungnahmen von 2018, 2020 und 2024 näher ausgeführt, eine umfassende, systematische Überarbeitung.

Soweit es in Absatz 1 Satz 2 (2. Halbsatz) heißt: „zu den erforderlichen Maßnahmen können insbesondere gehören“, käme das mutmaßlich Gemeinte möglicherweise besser zum Ausdruck, wenn formuliert wurde. „dabei ist mindestens zu prüfen, ob die folgenden Maßnahmen erforderlich sind“. Auf diese Weise würde immerhin das Verfahren zur Prüfung der erforderlichen Maßnahmen im Sinne von Artikel 6 Absatz 2 und 3 DS-GVO etwas spezifiziert und den öffentlichen Stellen ein rudimentäres Mindest-Prüfprogramm zur Verfügung gestellt. Immerhin findet sich eine entsprechende Formulierung in der Entwurfsbegründung; sie sollte aber Eingang in den Gesetzestext selbst finden.

Zu § 3 Absatz 1 Nummer 1 – neu – („Maßnahmen, die die nachtragliche Überprüfung und Feststellung gewahrleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind.“) weisen wir aufgrund unserer Erfahrungen vorsorglich darauf hin, dass hier nicht nur Maßnahmen zur Überprüfbarkeit bzw. Feststellbarkeit vorzusehen sind, sondern dass auch für die tatsächliche Durchführung regelmaßiger (wenigstens stichpunktartiger) Prüfroutinen und anlassbezogener Prüfungen zu sorgen ist. Das kommt auch in der Gesetzesbegründung zu § 17 nicht ausreichend zum Ausdruck, die insoweit geändert werden sollte (s. dazu unten). Auch bei § 3 Absatz 1 Nummer 1 würde sich ein entsprechender Hinweis in der Entwurfsbegründung für die Praxis empfehlen. Auch schrankt der Wortlaut von § 1 Absatz 1 Nummer 1 die Überprüfung auf die Verarbeitungsvorgänge Erfassen, Verändern und loschen ein. Richtigerweise sollte der Wortlaut – wie bislang die Formulierung zu § 17 des Entwurfs – die Überprüfung jeglicher Arten der Verarbeitung vorsehen.

Zu § 3 Absatz 2

Zu § 3 Absatz 2 verwiesen wir auf unsere Kritik aus unserer Stellungnahme vom Februar 2024 (S. 11).

Zu § 3a LDSG-E:

§ 3a LDSG-E neu setzt voraus, dass die Verarbeitung personenbezogener Daten in Fällen, in denen „KI [...] in besonderer Weise geeignet [ist], die Verwaltung dabei zu unterstützen, die gesetzlichen Aufgaben effizient, in der gebotenen Qualität und ressourcenschonend zu erfüllen“ (vgl. Begründung zu § 3a), grundsätzlich einer zweckkompatiblen Weiterverarbeitung personenbezogener Daten entspricht. Auf Artikel 59 Absatz 1 Buchstabe a Ziffer v der KI-VO wird verwiesen.

Es ist jedoch wichtig zu betonen, dass KI-Tools nicht ausschließlich als einfache Betriebsmittel betrachtet werden sollten. Ein wesentlicher Unterschied besteht beispielsweise darin, ob ein KI-System mit personenbezogenen Daten (aus der Verwaltung) (nach-)trainiert wird oder nicht, da sich die datenschutzrechtliche Bewertung in diesen Fällen erheblich unterscheidet. Eine pauschale Einordnung als einfaches Betriebsmittel ist daher nicht sachgerecht; vielmehr sollte jede Klasse von KI-Systemen im Einzelfall bewertet werden.

Die Nutzung von KI-Systemen zur Verarbeitung personenbezogener Daten kann mit einer zweckandernden Weiterverarbeitung personenbezogener Daten verbunden sein, weshalb die Anforderungen aus Artikel 6 Absatz 4 DS-GVO beachtet werden müssen. Gemäß Artikel 6 Absatz 4 in Verbindung mit Artikel 23 DS-GVO (siehe auch § 9a und § 10 Absatz 5 LdSG-E) sollten geeignete Maßnahmen ergriffen werden, um einen Ausgleich für die (zusätzlichen) Grundrechtseingriffe in die Rechte der betroffenen Personen zu schaffen. Dies wird in Artikel 59 der KI-VO adressiert. Ein pauschaler Erlaubnistanstbestand kann keinesfalls die im Einzelfall erforderliche Abwägung ersetzen, um zu klären, ob die Verarbeitung eine erforderliche und verhältnismäßige Maßnahme darstellt (Wesensgehaltsgarantie im Grundrechtsschutz) und welche technischen sowie organisatorischen Maßnahmen erforderlich sind. Zudem muss die Rechtsnorm sicherstellen, dass nur das mildeste Mittel zur Verarbeitung eingesetzt wird. Die Generalklausel des § 3a LdSG-E kann nur, wenn überhaupt, für Verarbeitungen mit geringer Eingriffsintensität Anwendung finden; alle anderen Verarbeitungen sind mit Rechtsunsicherheiten verbunden. Letztlich bietet die Norm im Vergleich zu § 4 LdSG keinen Vorteil für die verantwortlichen Stellen.

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 müssen, das heißt in einer kontrollierten Umgebung und in der Regel mit Beteiligung des LfDI. Das Reallabor sollte den Anforderungen aus Artikel 59 Absatz 1 Buchstabe c) bis j) der KI-VO entsprechen, um geeignete Maßnahmen zur Minderung der Grundrechtseingriffe in die Rechte der betroffenen Personen zu schaffen. Auf diese Weise würde den Anforderungen aus Artikel 6 Absatz 4 in Verbindung mit Artikel 23 DS-GVO Rechnung getragen. Nach erfolgreichem Abschluss der Tests im Reallabor sollte die Nutzung der KI kein hohes Risiko mehr darstellen. Eine Art Freigabe (für bestimmte Klassen) von KI-Systemen könnte dann durch einen delegierten Rechtsakt oder eine Verwaltungsvorschrift erfolgen. Sollte die Nutzung der KI jedoch weiterhin mit einem hohen Risiko verbunden sein, wäre ein spezifisches parlamentarisches Gesetz erforderlich.

Bei der Begründung zu § 3a LDSG-E ist der zweite Absatz („KI soll nämlich der Verwaltung...“) entbehrlich. Er enthält vielfach kaum bewiesene pauschale Annahmen, die teilweise schwer verständlich (z. B. inwiefern genau durch Anwendung von KI in der Verwaltung Gemeinwohlziele befördert werden können und warum die Anwendung von KI durch öffentliche Stellen für den Wirtschaftsstandort Baden-Württemberg unverzichtbar sei), teilweise missverständlich sind (mit Blick auf den Energieverbrauch des Einsatzes von Systemen künstlicher Intelligenz erscheint z. B. fraglich, ob dieser als „ressourcenschonend“ bezeichnet werden kann).

Zur Systematik von §§ 4-6 LDSG(-E)

Die bisherige Systematik der §§ 4-6 LDSG ist – wie bereits in unserer Stellungnahme vom 13. Februar 2024, S. 14 ausgeführt – für die Praxis nicht leicht verständlich und sollte revidiert werden. Das Innenministerium hat diese Ansicht im Abschlussbericht zur Evaluation des LDSG (S. 34) geteilt und angekündigt, im Rahmen einer Novellierung zu prüfen, wie die Systematik besser abgebildet werden kann. Der Gesetzentwurf hat hierzu bislang nur wenig (im Wesentlichen bei der Überarbeitung von § 6 LDSG-E) Neuerungen gebracht. Eine insgesamt verbesserte Systematik bliebe wünschenswert.

Zu § 4 Absatz 2 LDSG-E:

Zu § 4 Absatz 2 Satz 1 LDSG-E

In unserer letzten Stellungnahme hatten wir Bedenken mit Blick auf den Bestimmtheitsgrundsatz geäußert. Namentlich war u.E. unklar, was der Gesetzgeber mit Synthetisierung meint und inwieweit sich dies von einer Anonymisierung unterscheidet. Darüber hinaus hegten wir Bedenken, da der Zweck der zu erlaubenden Verarbeitung nicht aus dem Wortlaut der Regelung hervorging.

Vor diesem Hintergrund begrüßen wir sehr, dass im nunmehr vorliegenden Entwurf sowohl der Begriff der Synthetisierung in der Gesetzesbegründung erläutert und von dem Vorgang der Anonymisierung abgegrenzt wird, als auch der Wortlaut des § 4 Abs. 2 LDSG-E nunmehr einen Verarbeitungszweck benennt. Während der Synthetisierungsbegriff dadurch nunmehr für uns nachvollziehbar wurde (wenngleich die Aufnahme einer Definition im Gesetzestext selbst



rechtstechnisch vorzugswürdig wäre und der Praxis die Anwendung erheblich erleichtern würde), konnte die Ergänzung des Zwecks „Datenminimierung“ unsere Bedenken jedoch nicht ausraumen. Die Norm bleibt damit noch immer inhaltlich unbegrenzt (Näheres zu den Gründen s. u.), was unseres Erachtens in sowohl mit Blick auf die Normenklarheit, die Voraussetzungen einer Rechtsgrundlage nach Artikel 6 Absatz 3 DS-GVO, als auch den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz unzulässig ist. Wir empfehlen deswegen, die Erlaubnis zur Herstellung von anonymen und synthetischen Daten an die Zwecke der Forschung und der KI-Entwicklung zu binden und in den entsprechenden Vorschriften (§ 13 LDSG und § 11a LDSG-E) in Form eines Stufenkonzepts zu ergänzen: Kann der Forschungs-/Trainingszweck mit anonymen/ synthetischen Daten erreicht werden, so ist zunächst zu anonymisieren/synthetisieren. Kann der Forschungs-/Trainingszweck nicht mit anonymen/ synthetischen Daten erreicht werden, dürfen (unter den weiter geregelten Voraussetzungen) personenbezogene Daten verwendet werden. Für § 11a LDSG-E könnte dies beispielsweise wie folgt aussehen:

„(1) 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 personenbezogene Daten anonymisiert werden, wenn der Zweck des KI-Systems oder KI-Modells auf andere Weise nicht effektiv erreicht werden kann und schutzwürdige Belange der betroffenen Personen nicht entgegenstehen.

(2) 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 und schutzwürdige Belange der betroffenen Personen nicht entgegenstehen.“

Hintergrund der Bedenken ist, dass der nunmehr im Wortlaut genannte Zweck der Datenminimierung kein tauglicher ist und letztlich eine Globalbefugnis geschaffen wird, Daten zu jedem erdenklichen Zweck zu anonymisieren/synthetisieren.

Der im Wortlaut genannte Zweck der Datenminimierung ist kein tauglicher Verarbeitungszweck, da er ohnehin gemäß Artikel 5 Absatz 1 Buchstabe c DS-GVO für jeglichen Verarbeitungsprozess gilt. In der Folge kann er kein eigenständiges legitimes Ziel eines Verarbeitungsvorgangs sein. Vielmehr wäre der Zweck der Anonymisierung oder Synthetisierung die Ermöglichung von (datensparsamer) Forschung oder KI-Entwicklung/Training. Eben diese Zwecke sind jedoch im Gesetzeswortlaut nicht und in der Begründung nur als Regelbeispiel genannt („vor allem für die Forschung [...] sowie Entwicklung und das Training von KI werden anonyme - und möglichst synthetische Daten benötigt“). Folglich sollen Anonymisierung und Synthetisierung auch zur Erreichung anderer Ziele zulässig sein. Ohne Begrenzung der Verarbeitungserlaubnis auf einen Sachzweck bleibt die derzeit vorgesehenen Verarbeitungserlaubnis inhaltlich unbegrenzt. Dies führt - unabhängig vom konkreten rechtsdogmatischen Anknüpfungspunkts - jedenfalls dazu, dass der Gesetzgeber keine Abwägung zwischen den angestrebten Zwecken und dem Grundrechtseingriff vornehmen kann. Und es könnten sich Handlungsspielräume für die Verwaltung ergeben, die der Gesetzgeber - unabhängig vom Datenschutzrecht - womöglich nicht erlauben möchte, insbesondere das bereits in unserer letzten Stellungnahme bezeichnete Beispiel eines womöglich zulässigen Verkaufs hoheitlicher anonymisierter oder synthetisierter Daten, bspw. an Softwareunternehmen. Denn sind die Daten tatsächlich anonymisiert, so wurde wegen des Entfalls des Personenbezugs dieser Daten einem solchen Handeln kein Datenschutzrecht entgegenstehen

Im Übrigen weisen wir darauf hin, dass sich hier auch ein Wertungswiderspruch zum Umgang mit Statistikdaten ergibt: Für diese gelten eine Reihe besonders strenger Vorgaben. Hier sind jedoch keinerlei besonderen Schutzmaßnahmen für den Anonymisierungs-/Synthetisierungsprozess genannt.

Zusätzlich sollte je nach Sensibilität der Daten - insbesondere bei Daten nach Artikel 9 DS-GVO - eine Datenschutzfolgenabschätzung und unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ein Verfahren zur regelmäßigen Überprüfung der Anonymität der Daten verpflichtend vorgeschrieben werden. Denn eine echte Anonymisierung ist unter Umständen schwer zu erreichen und kann unter Berücksichtigung des technischen Fortschritts überholt werden, beispielsweise weil ein automatisierter Abgleich von Daten immer schneller und feingranularer möglich wird.

Der Vollständigkeit halber weisen wir darauf hin, dass § 4 Absatz 2 LDSG keine Rechtsgrundlage zur Anonymisierung oder Synthetisierung von besonderen Kategorien personenbezogener Daten im Sinne von Artikel 9 DS-GVO darstellt. Besondere Kategorien personenbezogener Daten, beispielsweise Gesundheitsdaten, dürften somit nur dann anonymisiert oder synthetisiert werden, wenn zusätzlich eine Befreiung vom Verarbeitungsverbot aus Artikel 9 Absatz 1 DS-GVO vorliegt, also etwa zumindest die Voraussetzungen des § 17 LDSG-E erfüllt sind (s. dazu noch unten).

Zu § 5 LDSG:

Zu § 5 Absatz 1 Nummer 1

Das mit der Ergänzung des § 5 Absatz 1 Nummer 1 verfolgte Ziel des Gesetzgebers ist anerkennenswert. Es bestehen allerdings Zweifel, ob die Ergänzung geeignet ist, Zweckänderungen zugunsten des Gemeinwohls zu konkretisieren.

Denn nach Art. 23 Abs. 2 Buchstabe a DS-GVO ist es Sache des Gesetzgebers, Zwecke und Ziele der Weiterverarbeitung näher festzulegen. Die Neufassung unter Aufnahme des „öffentlichen Interesses“ ist zwar enger, legt aber nach wie vor nicht die konkreten Zwecke und Ziele der Verarbeitung fest, zu deren Gunsten eine Zweckänderung zulässig sein soll. Daher bestehen auch in Bezug auf die durch den Entwurf geänderte Fassung weiterhin erhebliche Zweifel an der Europarechtskonformität.

Zu § 5 Absatz 1 Nummer 5

Wir begrüßen die Änderung des Wortlauts gegenüber dem unserer Stellungnahme vom 10. Juni 2025 zugrunde liegenden Entwurf von „verweigern“ hin zu „nicht erteilen“. Die bereits mitgeteilten erheblichen Zweifel werden dadurch jedoch nicht ausgeräumt.

Was „im Interesse der betroffenen Person“ liegt, wird die Person typischerweise selbst am besten entscheiden können. Eine staatliche Bevormundung darf insoweit grundsätzlich nicht stattfinden, jedenfalls solange davon auszugehen ist, dass diese (oder ggf. eine vertretungsberechtigte Person) ihren Willen bilden und artikulieren könnte. Der von der

Begründung herangezogene Artikel 23 Absatz 1 Buchstabe i DS-GVO formuliert auch enger, dass die Datenverarbeitung den „Schutz“ der betroffenen Person sicherstellen muss.

Des Weiteren ist eine fingierte Einwilligung durch die betroffene Person der Systematik der Datenschutz-Grundverordnung fremd (dort wird vielmehr eine *unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung verlangt*), sodass auch aus diesem Grund Zweifel an der Europarechtskonformität der Regelung bestehen. In den vom Entwurf umfassten Fällen sollte daher richtigerweise eine Einwilligung der betroffenen Person zur zweckändernden Verarbeitung eingeholt werden; ihrer gesetzlichen Ersetzung bedarf es weder, noch wäre dies europarechtlich zulässig

Zu § 6 LDSG:

In systematischer Hinsicht begrüßen wir grundsätzlich die Neufassung des § 6 LDSG Im Hinblick auf die Überschrift scheint es jedoch zu einem Redaktionsverssehen gekommen zu sein. Denn in der Begründung heißt es, dass „insbesondere [...] in der Überschrift klargestellt [wird], dass nur die Übermittlung personenbezogener Daten zu anderen Zwecken geregelt wird“. In der Überschrift wurde nun jedoch gegenüber dem unserer Stellungnahme vom 10. Juni 2025 zugrunde liegenden Entwurf gerade der Zusatz § 6 – Übermittlung personenbezogener Daten zu anderen Zwecken“ entfernt, sodass nunmehr gerade nicht aus der Überschrift hervorgeht, dass die Norm nur die zweckändernde Übermittlung adressiert.

Der Vollständigkeit halber teilen wir noch mit, dass wir davon ausgehen, dass bei besonderen Kategorien personenbezogener Daten zusätzlich eine Befreiung vom Verarbeitungsverbot aus Artikel 9 DS-GVO vorliegen muss

Zu § 6 Absatz 1

Den Bedarf der Änderung des Wortlauts von „Übermittlung [...] an öffentliche Stellen“ hin zu „Übermittlung [...] an Stellen innerhalb des öffentlichen Bereichs“ können wir anhand der Begründung nachvollziehen, nachdem dort erläutert wird, dass mit dem „öffentlichen Bereich“ öffentliche Stellen des Bundes und der Länder gemeint seien. Anders als in § 25 BDSG, wo nur die Rede von der Übermittlung an öffentliche Stellen die Rede ist, aber der

Begriff „öffentliche Stelle“ nicht auf Stellen des Bundes beschränkt ist, ist in der Legaldefinition in § 2 Absatz 1 der Begriff „öffentliche Stelle“ auf „Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts“ beschränkt.

Nachteilig an der gewählten Lösung ist, dass sich die Definition des „öffentlichen Bereichs“ nicht aus dem Gesetz selbst ergibt. Wenn daher die Legaldefinition in § 2 Absatz 1 LDSG – möglicherweise aus Gründen der Gesetzgebungskompetenz des Landes – nicht geändert werden soll, wäre zu erwägen, ob eine Definition des Begriffs „öffentlicher Bereich“ im Sinne der derzeit in der Begründung enthaltenen Formulierung aufgenommen werden kann.

Zu § 6 Absatz 2 Nummer 3

Wir begrüßen die Klarstellung in § 6 Absatz 2 Nummer 3 LDSG-E gegenüber der Formulierung des unserer Stellungnahme vom 10. Juni 2025 zugrundeliegenden Entwurfs im Hinblick auf die Stelle, um deren Ansprüche es geht und im Hinblick darauf, dass alle (Arten von) Rechtsansprüche gemeint sind, nicht nur zivilrechtliche. In folgender Hinsicht erschien uns eine Klarstellung - jedenfalls in der Begründung - jedoch nach wie vor äußerst hilfreich.

Die Formulierung lässt offen, wie die Prüfung des „Erforderlichkeit“ der Übermittlung zu den genannten Zwecken auszugestalten ist. Insofern ist die Frage, ob – insbesondere bei einer Übermittlung an eine rechtsberatende Person – nur zu prüfen ist, ob sie für den jeweiligen Mandatszweck erforderlich ist, oder ob sich die Prüfung der Erforderlichkeit auch auf die Frage der Notwendigkeit der Einschaltung eines Rechtsanwalts bzw. der gerichtlichen Geltendmachung erstrecken soll, inwieweit also auch Erfolgsaussicht oder Sinnhaftigkeit der Inanspruchnahme anwaltlicher Vertretung bzw. der gerichtlichen Geltendmachung zu prüfen sind. Wir gehen davon aus, dass insoweit der öffentlichen Stelle ein Einschätzungsspielraum verbleiben muss und deswegen alleine aus einer späteren Erfolglosigkeit der anwaltlichen Tätigkeit nicht zwingend auf die datenschutzrechtliche Unzulässigkeit der Einschaltung anwaltlicher Bemühungen geschlossen werden kann.

Ebenfalls Missverständnisse vermeiden konnte eine Klarstellung darüber, inwieweit mit der Beschreibung „Geltendmachung, Ausubung oder Verteidigung von Rechtsansprüchen der übermittelnden Stelle“ bloße Rechtsberatung umfasst ist, die nicht in eine konkrete Handlung zur Geltendmachung, Ausubung oder Verteidigung eines Rechtsanspruchs mündet oder

münden soll. Die derzeitigen Ausführungen in der Gesetzesbegründung wiederholen lediglich den Gesetzeswortlaut, erläutern seinen Inhalt jedoch nicht näher („[...] lediglich nunmehr die Alternative der Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen der übermittelnden Stelle eingefügt [...]“)

Insgesamt solle unseres Erachtens bei der Klarung dieser Fragen berücksichtigt werden, dass einerseits die öffentliche Stelle grundsätzlich zur Wahrung ihrer Ansprüche und Rechte sowie zur Verteidigung gegen erhobene Ansprüche legitimiert sein muss, dass aber andererseits auch die Übermittlung zum Zwecke der Rechtsberatung bzw. Rechtsverfolgung einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt und daher ausreichend veranlasst sein muss.

Schließlich weisen wir noch darauf hin, dass eine Klarung wünschenswert wäre, ob mit der Umschreibung „Verteidigung von Rechtsansprüchen“ auch (oder vielleicht gerade nur) die Verteidigung gegen von anderer Seite geltend gemachte Rechtsansprüche gemeint sein soll.

Zu § 6 Absatz 4

Wir begrüßen, dass das Innenministerium die Bedenken aus unserer Stellungnahme vom 13. Februar 2024 in Bezug auf die bisherige Regelung in § 6 Absatz 2 LDSG aufgreift, wie sich insbesondere aus der Entwurfsbegründung ergibt. Der Sache nach sagt die Regelung, wie wir sie jetzt verstehen, dass die abrufende Stelle die Verantwortung für die Rechtsmaßigkeit der Erhebung trägt und die übermittelnde Stelle diejenige für die Übermittlung. Dabei hat die übermittelnde Stelle die Voraussetzungen der Rechtmäßigkeit der Erhebung im Falle eines Abrufs oder eines Ersuchens (also beispielsweise die Erforderlichkeit der Erhebung zur Aufgabenerfüllung der anfordernden Stelle im Fall von § 4 Absatz 1 LDSG) nur dann zu prüfen, wenn es dafür Anlass gibt. Zu prüfen ist allerdings, inwieweit dies auch bei einem Abrufen oder Ersuchen durch eine Stelle, die zu Zwecken der JI-Richtlinie tätig wird, gelten kann. Hierzu müsste es wohl einer entsprechenden Zuweisung der Verantwortung auch in entsprechenden Umsetzungsnormen zur JI-Richtlinie geben. Nicht sicher erscheint uns, ob die so verstandene gesetzgeberische Intention auch für Anwendende klar genug zum Ausdruck kommt. Möglicherweise würde klarer an das Doppeltürmodell angeknüpft, wenn in der Formulierung statt an „die Rechtmäßigkeit des Abrufs oder des Ersuchens“ anknüpfen wurde an die „Rechtmäßigkeit der Erhebung, soweit deren Voraussetzungen zugleich Rechtmäßigkeitsvoraussetzungen der Übermittlung sind“.

Darüber hinaus ist für uns unklar, ob die Regelung in Absatz 4 des Entwurfs für jegliche (oder nur für mit einer Zweckänderung einhergehende?) Übermittlung gelten soll. Dies sollte bei der Bereinigung des oben zu § 6 LDSG-E aufgeführten Widerspruchs zwischen der neuen Überschrift und der Entwurfsbegründung mitbedacht und geklärt werden.

Zu § 6 Absatz 5

Der Entwurf zu § 6 Absatz 5 LDSG ist zu unbestimmt. Mit der vorgeschlagenen Formulierung würde mittels Generalklausel das Anlegen gemeinsamer Dateien erlaubt, wenn eine Einzelfallübermittlung durch eine andere Regelung erlaubt ist. Die Abwägungsentscheidung über die Erlaubnis des Gesetzgebers zu einer Einzelfallübermittlung unterscheidet sich jedoch maßgeblich von der Abwägungsentscheidung der Erlaubnis einer gemeinsamen automatisierten Datei Gemeinsame Dateien, sprich das Zusammentragen von Informationen verschiedener Stellen, werden regelmäßig einen Grundrechtseingriff darstellen, der ausdrücklich vom Gesetzgeber erlaubt werden muss, da die Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung höher ist. In der Generalklausel kann nur schwerlich eine Abwägung der Zweck-Mittel-Relation erfolgen, da der Zweck der jeweiligen gemeinsamen Datei sich aus einer anderen Regelung ergäbe, der ihrerseits jedoch nur eine Einzelfallabwägung zugrunde liegt. Zwar wird dies in Teilen dadurch aufgefangen, dass die Regelung selbst die Einschränkung enthält, dass „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“. Allerdings geht aus der Gesetzesbegründung überhaupt nicht hervor, weshalb es eine Generalklausel für gemeinsame Dateien überhaupt - außerhalb spezieller Regelungen – bedarf.

Zu § 7a LDSG:

Die Regelung ist grundsätzlich zu begrüßen. Sie entspricht in ihrer Intention der Anregung des LfDI und kann die Begründung von Auftragsverarbeitungsverhältnissen erleichtern und damit die Rechtmäßigkeit der Verwaltung besser sicherstellen

Allerdings fragt sich, inwieweit bei Absatz 1 hier tatsächlich noch von einem „Auftragsverarbeitungsvertrag“ die Rede sein sollte und nicht eher von einem

„Auftragsverarbeitungsverhältnis“, nachdem die Regelungen ja nicht mehr im eigentlichen Sinne vertraglichen Ursprungs sind.

Wir können auch nicht erkennen, ob die Voraussetzung „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,“ hinreichend klar normiert ist. An welche Konstellation außerhalb der BITBW, der LBank und der Komm.One ist hier gedacht? Wenn nur die in der Begründung aufgeführten Konstellationen erfasst werden sollte, könnte diese zur Vermeidung von Auslegungsschwierigkeiten konkret benannt werden. In Bezug auf die Komm.One fragt sich ferner, inwieweit das kommunale Selbstverwaltungsrecht eine solche Regelung des Vertragsverhältnisses über eine Rechtsverordnung überhaupt zulassen würde.

Die Regelungen in Absatz 1 und 2 stellen bislang auch nicht sicher, dass alle von Artikel 28 DS-GVO vorausgesetzten Bedingungen erfüllt werden (z. B. die Festlegung von technisch-organisatorischen Maßnahmen, Mitwirkung bei Datenpannen, Verhalten bei Beendigung etc.).

Unklar ist, inwieweit sich Absatz 2 und 3 nur auf den in Absatz 1 geregelten Fall beziehen sollen, oder ob sie vollkommen eigenständige Tatbestände darstellen sollen.

Zu Absatz 3 ist klarstellend anzumerken, dass hier das Verbot eines In-Sich-Geschäfts (§ 181 BGB) zu beachten ist. Die vorgesetzte Behörde kann also dann nicht im Wege der Stellvertretung nach Absatz 3 ein Auftragsverarbeitungsverhältnis begründen, wenn und soweit sie selbst Auftragsverarbeiterin sein soll, denn ansonsten wäre sie gar nicht effektiv im Sinne von Artikel 28 Absatz 3 DS-GVO gebunden.

Zu § 8 LDSG-E:

Wir begrüßen die Einfügung eines neuen Absatz 2, verweisen aber auf den bereits mit unseren Stellungnahmen vom 6. November 2020 und vom 13. Februar 2024 dargelegten Konkretisierungsbedarf

Zu § 9 LDSG-E:

Zu § 9 LDSG verweisen wir auf unsere Ausführungen in unseren Stellungnahmen vom 6. November 2020 und vom 13. Februar 2024, die leider bislang keinen Eingang in den Entwurf gefunden haben.

Zu § 9a LDSG:

Die Ausnahme von Artikel 16 DS-GVO wird ausweislich der Entwurfsbegründung auf Artikel 23 Absatz 1 Buchstabe e DS-GVO gestützt. Danach ist Voraussetzung für eine Beschränkung von Betroffenenrechten u. a., dass diese eine in einer demokratischen Gesellschaft notwendige und verhältnismaßige Maßnahme darstellt, die den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats sicherstellt. Nach der Entwurfsbegründung wird zu dem mit der Vorschrift verfolgten Ziel ausgeführt, dass die Anwendung von KI in der öffentlichen Verwaltung unverzichtbar sei, um effizient, in der gebotenen Qualität und ressourcenschonend die gesetzlichen Aufgaben zu erfüllen. Wenn das Ziel der effizienten, ressourcenschonenden (s. dazu allerdings schon oben unsere Anmerkung zu § 3a LDSG-E) und den gebotenen Qualitätsanforderungen entsprechenden Aufgabenerfüllung der öffentlichen Verwaltung mit der Vorschrift verfolgt wird, ist in Erfüllung der Anforderungen von Artikel 23 Absatz 1 DS-GVO sicherzustellen, dass der Ausschluss eine hierzu notwendige und verhältnismäßige Maßnahme darstellt. Daher sind dementsprechende Anforderungen in den Gesetzesentwurf aufzunehmen.

Hierfür sollte beispielsweise nach Satz 3 folgendes 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.“

Zu § 10 Absatz 4 LDSG-E:

Der Gesetzgeber erkennt richtigerweise, dass Filter dem Schutz der Rechte Betroffener dienen können.

Ein Filter stellt jedoch keine Löschung, sondern lediglich eine temporäre Maßnahme dar. Wenn die Löschung praktisch nicht umsetzbar ist, kann die KI nicht eingesetzt werden. Dies wird besonders problematisch im Hinblick auf die Speicherbegrenzung personenbezogener Daten. Die Speicherung personenbezogener Daten in einer KI ohne klare Aufbewahrungsfrist, das heißt im Extremfall eine unbeschränkte Speicherung, ist mit den Anforderungen der Datenschutz-Grundverordnung nicht vereinbar. Eine verlängerte Speicherung der Daten im Vergleich zu einer Verarbeitung ohne KI ist nur dann gerechtfertigt, wenn ein erhebliches öffentliches Interesse an der Verarbeitung besteht. Dies kann jedoch nur im Einzelfall oder für bestimmte Klassen von KI-Systemen rechtlich geprüft werden. Unseres Erachtens sollte die Prüfung nicht auf „extrem teuer und zeitaufwändig reduziert werden, wie in der Gesetzesbegründung angedeutet wird. Daher sollte die Beschränkung des Rechts auf Löschung durch separate Regelung erfolgen.“

Zudem verweisen wir auf unsere Ausführungen zu § 9a LDSG

Zu § 11a LDSG-E:

Ein pauschaler Erlaubnistanstbestand kann keinesfalls die im Einzelfall erforderliche Abwägung ersetzen, ob die Verarbeitung eine erforderliche und verhältnismäßige Maßnahme darstellt (Wesensgehaltsgarantie im Grundrechtsschutz) und ob ggf. technische und organisatorische Maßnahmen erforderlich sind. Trotz Vorliegen einer Rechtsgrundlage muss sichergestellt werden, dass nur das mildeste Mittel (eingriffsgeringste) zur Verarbeitung personenbezogener Daten eingesetzt wird.

Die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen sollten, sofern eine nicht nur geringe Eingriffsintensität in die Rechte und Freiheiten betroffener Personen vorliegt, ausschließlich innerhalb eines Reallabors erfolgen (vgl. Artikel 59 Absatz 1 Buchstabe c bis j der KI-VO). Auf diese Weise können die nach Artikel 6 Absatz 4 in Verbindung mit Artikel 23 DS-GVO erforderlichen Maßnahmen umgesetzt werden.

Die Gesetzesbegründung zu § 11a LDSG verweist allgemein auf die Einhaltung der rechtlichen Anforderungen aus dem Datenschutz. Dies sollte jedoch regelmäßig durch ein Gesetz geregelt werden. Beispielsweise kann die Verlagerung der Zulässigkeitsprüfung auf die verantwortliche Stelle zu erheblicher Rechtsunsicherheit führen.

Die differenzierte Darstellung der Begriffe „Anonymisierung“, „Pseudonymisierung“ und „direkte Verarbeitung“ in der Gesetzesbegründung heißen wir gut.

Zu § 12a LDSG-E

Die Notwendigkeit einer klarstellenden Regelung für die Verarbeitung personenbezogener Daten zu Zwecken der parlamentarischen Kontrolle hat sich im Rahmen des Evaluierungsverfahrens zum Landesdatenschutzgesetz an mehreren Stellen gezeigt. Insofern begrüßen wir grundsätzlich die Ergänzung des Landesdatenschutzgesetzes um die Regelung zur Verarbeitung personenbezogener Daten zu Zwecken der parlamentarischen Kontrolle. Allerdings bitten wir um Prufung, inwieweit es tatsächlich einer umfassenden Befugnis zur Verarbeitung seitens der Landesregierung bedarf. Nach unserer bisherigen Einschätzung dürften der Landesregierung für die Erhebung der Informationen grundsätzlich ausreichende Möglichkeiten im Wege der Aufsicht über die Verwaltung zur Verfügung stehen. Hier erscheint uns eine Abgrenzung erforderlich, inwieweit die Verarbeitung dem jeweiligen Aufsichtsrecht folgen soll (was u. E. ausreichend sein dürfte) oder inwieweit hier eine Erweiterung der Erhebungsbefugnisse durch die Regelungen erfolgen soll. Regelungsbedürftig erscheint uns v. a. die Übermittlung an den Landtag; zur Zweckänderung verweisen wir auf unsere Stellungnahme vom 13. Februar 2024, S. 19.

Eine Klarstellung ist auch deswegen erforderlich, weil die Regelung ausschließlich die Verarbeitung durch „die Landesregierung“ betrifft. Verantwortliche Stelle bei der Ausübung von Aufsichtsrechten ist dagegen regelmäßig das einzelne zuständige Ministerium als oberste Landesbehörde.

Zu § 13 LDSG:

Zu § 13 Absatz 1 LDSG in der bisherigen Fassung, soweit er nach dem Entwurf erhalten bleiben soll.

Die Regelung des § 13 Absatz 1 LDSG ist so konzipiert, dass sie eine Rechtsgrundlage für öffentliche Stellen zur Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten für Forschungszwecke und für statistische Zwecke darstellen soll. Dabei soll die Regelung sowohl als Befreiung vom Verbot aus Artikel 9 Absatz

1 DS-GVO (Ausnahme nach Artikel 9 Absatz 2 Buchst. j DSGVO) als auch als Rechtsgrund im Sinne von Artikel 6 Absatz 1 DS-GVO fungieren.

Soweit sich die Regelung eines Rechtsgrundes im Sinne von Artikel 6 Absatz 1 DS-GVO auf Artikel 6 Absatz 1 Buchstabe e DS-GVO stützen soll, führt dies zur Frage, in welchen Fällen Forschung und Statistik jeweils zur Aufgabe der öffentlichen Stellen des Landes gehören. Insoweit bedarf es grundsätzlich einer konkreten gesetzlichen Aufgabenzuweisung. Klar ist beispielsweise, dass den Hochschulen Aufgaben zur unabhängigen Forschung zugewiesen sind; eine entsprechende gesetzliche Aufgabenzuweisung findet sich u. a. in § 2 Absatz 1 des Landeshochschulgesetzes (LHG). Eine ähnliche Aufgabenzuweisung enthält § 4 Absatz 1 Satz 2 des Universitätsklinikgesetzes zugunsten der Universitätskliniken.

Soweit allerdings eine solche gesetzliche Aufgabenzuweisung nicht besteht, fragt sich, in welchem Umfang öffentlichen Stellen trotzdem die Aufgabe der Forschung im Sinne von Artikel 6 Absatz 1 Buchstabe e DS-GVO zukommen soll. Die Formulierung von § 13 Absatz 1 LDSG ließe sich dahingehend verstehen, dass jede öffentliche Stelle legitimiert werden soll, zu jedem Forschungsthema personenbezogene Daten zu verarbeiten, und zwar unabhängig davon, ob dieses Thema etwas mit ihren sonstigen gesetzlichen Aufgaben zu tun hat oder nicht. Das ist im Falle potentieller Eingriffe in das Grundrecht auf informationelle Selbstbestimmung problematisch und lässt sich nur in Grenzen durch das Grundrecht auf Forschungsfreiheit rechtfertigen, weil dieses im Allgemeinen (vom Sonderstatus bestimmter Entitäten, namentlich der Hochschulen abgesehen) dem Staat als Hoheitsträger nicht zukommt.

Von daher bedürfte es, wenn durch § 13 LDSG tatsächlich als Aufgabenzuweisung im Sinne von Artikel 6 Absatz 1 Buchstabe e DS-GVO verstanden werden soll, einer ausdrücklichen Regelung, welchen staatlichen Stellen zu welchen Themen die Aufgabe der (unabhängigen) Forschung zukommen soll. Eine solche Entscheidung lässt sich aber § 13 LDSG bislang nicht entnehmen.

Alternativ könnte der Gesetzgeber klarstellen, dass § 13 LDSG nicht als Aufgabenzuweisung zu verstehen ist, sondern nur die Modalitäten der Verarbeitung zu Forschungszwecken regelt, soweit die öffentliche Stelle Forschungsaufgaben übernimmt (die ihnen durch ein anderes Gesetz zugewiesen sind). In diese Richtung deutlicher formuliert ist z. B. Artikel 25 des Bayerischen Datenschutzgesetzes, § 13 des Bremer Ausführungsgesetzes zur Datenschutz-

Grundverordnung, § 27 des Datenschutz-Ausführungsgesetzes von Sachsen-Anhalt, § 24 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (wenn man den dortigen Absatz 1 seinem Wortlaut entsprechend nur auf die Befreiung von Artikel 9 Absatz 1 DS-GVO bezieht), § 22 des Landesdatenschutzgesetzes Rheinland-Pfalz und § 28 des Thüringischen Datenschutzgesetzes.

Für öffentliche Stellen ohne konkrete gesetzliche Zuweisung eigener Forschungsaufgaben bliebe dann noch im Landesdatenschutzgesetz zu regeln, unter welchen Voraussetzungen sie bei ihr vorhandene Daten anderen forschenden Stellen übermitteln darf. Wir würden es begrüßen, wenn der Gesetzgeber diese klare Differenzierung (Eigenforschung nur im Falle gesonderter gesetzlicher Aufgabenzuweisung, dann aber nach Maßgaben der Modalitäten des Landesdatenschutzgesetzes; Übermittlung zu Forschungszwecken durch öffentliche Stellen unabhängig von einer gesonderten Aufgabenzuweisung) abbilden würde

Zu den vorgesehenen Änderungen in § 13 Absatz 1 LDSG-E

Soweit in Absatz 1 nach dem Wort „verarbeiten“ eingefügt werden soll „und vorhandene Daten der genannten Art weiterverarbeiten“, erschließt sich uns der Sinn der Gesetzesänderung nicht, und zwar auch nicht durch die Entwurfsbegründung. Wir empfehlen, von dieser Änderung Abstand zu nehmen.

Verarbeiten ist ein Oberbegriff, der das Weiterverarbeiten bereits erhobener Daten einschließt. Durch die gesonderte Erwähnung der Weiterverarbeitung wird die Gefahr begründet, dass an anderer Stellen des Gesetzes, an denen die Weiterverarbeitung nicht gesondert erwähnt wird, in Form eines Umkehrschlusses gefolgert wird, dass eine Weiterverarbeitung nach der Erhebung ohne gesonderte Erwähnung nicht erlaubt sei.

Soweit mit der Formulierung gemeint sein sollte, dass damit eine Zweckänderung legitimiert werden soll, wenn Daten bislang zu anderen Zwecken erhoben worden sind, ist auf den zweiten Halbsatz von Artikel 5 Absatz 1 Buchstabe b DS-GVO zu verweisen, dem zufolge eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Dies stellt bereits eine Regelung des Europarechts im Sinne von Artikel 6 Absatz 4 DS-GVO dar, die eine Zweckänderung erlaubt, so dass es insoweit keiner weiteren mitgliedsstaatlichen Regelung bedarf.

Gegen die übrigen Änderungen von Absatz 1 haben wir keine Bedenken. Begrüßt wird die gegenüber den Forschungsklauseln anderer Länder sowie § 27 BDSG anschlussfähigere explizite Aufnahme der Erforderlichkeit statt der bisherigen Formulierung „wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können“.

Überarbeitungsbedürftig erscheint uns allerdings der letzte Absatz der Begründung zu den Änderungen von Absatz 1; dort wird ausgeführt:

„Absatz 1 erlaubt auch die Forschung mit Kooperationspartnern in gemeinsamer Verantwortung. Die Übermittlung an Dritte für deren eigene Forschungsvorhaben ist in Absatz 4 geregelt.“

Die Ausführungen lassen das Missverständnis zu, dass die Überlassung von Daten einer öffentlichen Stelle an Kooperationspartner im Rahmen einer gemeinsamen Verantwortung keine Übermittlung darstelle, solange die öffentliche Stelle selbst an dem Forschungsvorhaben beteiligt sei. Dies wäre indes unrichtig, jede (zielgerichtete) Offenlegung an Dritte stellt eine Übermittlung dar, so dass die dafür notwendigen Anforderungen erfüllt sein müssen.

Zu § 13 Absatz 2 LDSG-E:

Zu der Frage der Erhebung von öffentlich zugänglichen personenbezogenen Daten zu Forschungszwecken haben wir bereits in unserer Stellungnahme vom 13. Februar 2024 (S. 34 ff.) Stellung genommen. Insoweit ist zunächst festzuhalten, dass vielfach ohne Anhörung nicht feststellbar sein wird, inwieweit entgegenstehende schutzwürdige Interessen der betroffenen Person bestehen. Aus diesem Grund scheint der praktische Nutzen der Norm fraglich. Ausnahmen könnten allenfalls dann anerkannt werden, wenn offensichtlich ist, dass die betroffene Person mit der Veröffentlichung einverstanden ist und dass keine der Verarbeitung zu Forschungszwecken entgegenstehenden Interessen bestehen. Auf die Erhebung in dieser Fallkonstellation sollte die Vorschrift beschränkt werden. Darüber hinaus hielten wir bereits in der o. a. Stellungnahme die gesetzliche Einführung andere Garantien für die Rechte und Freiheiten der betroffenen Personen – wie z. B. die Vorab-Prüfung durch eine unabhängige Stelle – für geboten, um die notwendige Abmilderung des Eingriffs durch Verfahrensvorsorge sicherzustellen. Auch eine besondere gesetzliche Sicherstellung von Transparenzanforderungen und die tatsächliche Möglichkeit zur Ausübung von

Betroffenenrechten einschließlich eines voraussetzungslosen Widerspruchsrechts könnten unseres Erachtens zu Abmilderung beitragen. Zusätzlich wären bei Einräumung des Rechts auf Verknüpfung mit weiteren Daten weitere Risiken zu bedenken und Vorsorge zu treffen.

Diesen Anforderungen wird der vorgeschlagene Regelungsentwurf nicht gerecht, so dass er in seiner jetzigen Fassung als unverhältnismäßig in Grundrechte eingreifend abzulehnen ist.

Zu § 13 Absatz 3 LDSG-E.

Soweit in Satz 3 vorgeschrieben wird, dass „zur Wahrung der Interessen der betroffenen Personen weitere angemessene und spezifische Maßnahmen entsprechend § 3 Absatz 1 zu treffen“ seien, ist dem Bestimmtheitsgrundsatz nicht vollständig Genüge getan, vgl. Anforderungen der Datenschutzgrundverordnung (insbesondere Artikel 89 Absatz 1, 6 Absatz 2 und 3 DS-GVO). Der pauschale Verweis, dass (irgendwelche) Maßnahmen nach § 3 Absatz 1 zu treffen ist insoweit unzureichend. Hinzu kommt, was genau damit gemeint ist, dass die Maßnahmen nur „entsprechend“ § 3 Absatz 1 erfolgen sollen (was impliziert, dass § 3 nicht direkt anwendbar sei und offenlässt, inwieweit die „entsprechende“ Geltung gehen soll). Zudem ist unklar, inwieweit angesichts des ausdrücklichen Hinweises auf § 3 Absatz 1 auch § 17 LDSG für die Verarbeitung besonderer Kategorien personenbezogener Daten gelten soll. Insofern weisen wir darauf hin, dass bei Verarbeitung besonderer Kategorien personenbezogener Daten, für die Artikel 9 Absatz 2 Buchstabe j DS-GVO vorschreibt, dass das nationale Recht selbst angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsieht, und deren Ergreifung nicht den Verantwortlichen überlässt.

Für besondere Kategorien personenbezogener Daten darf die Regelung auch nicht in einem Wertungswiderspruch zu anderen Regelungen stehen, die spezifische Maßnahmen insoweit vorsehen. So sieht beispielsweise § 6 Absatz 1 des Gesundheitsdatennutzungsgesetzes (GDNG) vor, dass die Daten bei Eigenforschung durch Gesundheitseinrichtungen stets mindestens zu pseudonymisieren sind, ein Rechte- und Rollenkonzept zu erstellen und Weiterverarbeitungen protokolliert werden. Auch die derzeit im Entwurf befindliche Neuregelung im Landeskrankenhausgesetz sieht weitere Schutzmaßnahmen hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten vor, hinter denen die allgemeine Regelung im Landesdatenschutzgesetz nicht zurückbleiben sollte. Hier ist im Interesse der Vermeidung von unnötigen Verständnisschwierigkeiten der Praxis vielmehr eine

Harmonisierung der Forschungsklauseln vorzunehmen. Es ist nicht einzusehen, warum für Gesundheitsdaten, die durch das Universitätsklinikum verarbeitet werden, insoweit andere Vorgaben gelten sollen, als wenn sie durch die Universität verarbeitet werden. Im Falle des Universitätsklinikums bliebe im Übrigen fraglich, – da sowohl Krankenhaus bzw. datenverarbeitende Gesundheitseinrichtung im Sinne von § 2 Nummer 7 GDNG als auch öffentliche Stelle des Landes – welche Regelung hier den Vorrang haben soll.

Dabei sollten die Regelungen auch hinsichtlich der Frage harmonisiert werden, inwieweit zwischen verschiedenen Arten der besonderen Kategorien personenbezogener Daten differenziert werden muss. Zu Recht geht der Entwurf einer Novellierung des Landeskrankenhausgesetzes insoweit davon aus, dass die Verarbeitung genetischer Daten zu Forschungszwecken wegen der besonderen Sensibilität dieser Daten (die nach dem Gendiagnostikgesetz grundsätzlich nur auf Basis einer Einwilligung verarbeitet werden dürfen) besondere Anforderungen voraussetzen muss. Diese Anforderungen an die einwilligungsfreie Verarbeitung von genetischen Daten, wie sie im Entwurf der Änderung des Landeskrankenhausgesetzes vorgesehen sind, müssen auch für öffentliche Stellen des Landes gelten, um hier einen Wertungswiderspruch zu vermeiden.

Unabhängig davon, ob die personenbezogenen Daten besondere Kategorien darstellen, ist bei der Verarbeitung personenbezogener Daten zur Forschungs- oder Statistikzwecke wichtig sicherzustellen, dass die zu diesen Zwecken erhobenen Daten und die durch ihre Verarbeitung erzielten weiteren Erkenntnisse nur zu den Erhebungszwecken weiterverarbeitet werden dürfen. Dies heben einige Landesdatenschutzgesetze – unseres Erachtens zu Recht – hervor (vgl. etwa Artikel 25 Nummer 1 des Bayerischen Datenschutzgesetzes). Eine Verarbeitung insbesondere zu anderen Zwecken der Verwaltung muss durch entsprechende trennende Maßnahmen einschließlich eines darauf ausgerichteten Rechte- und Rollenkonzepts, idealerweise auch durch die Regelung eines Forschungsgeheimnisses, effektiv verhindert werden.

Zu § 13 Absatz 5 LDSG-E:

Wir begrüßen das Bestreben, die Übermittlung personenbezogener Daten zu Statistik- und Forschungszwecken an nicht-öffentliche Stellen gesetzlich gesondert zu regeln. Auch eine gesonderte Regelung der Übermittlung an öffentliche Stellen ist überdies jedoch geboten.

Allerdings ist die entworfene Regelung der Übermittlung zur Wahrung der Interessen und Freiheiten der betroffenen Personen nicht ausreichend. Der pauschale Verweis, dass (irgendwelche) Maßnahmen nach dem entsprechend geltenden Absatz 3 (i.V.m. § 3 Absatz 1) zu ergreifen seien, bzw. die empfangende Stelle sich dazu verpflichtet, (irgendwelche) „Maßnahmen entsprechend § 3 Absatz 1 zu treffen“, ist insoweit unzureichend.

Die Regelung muss zunächst klar zum Ausdruck bringen, dass grundsätzlich nur anonymisierte Daten zu Forschungszwecken herausgegeben werden dürfen. Nur soweit für die Verwirklichung des Forschungszwecks unbedingt erforderlich, kann auch eine Übermittlung pseudonymisierter Daten in Betracht kommen. In Bezug auf den Vorgang der Anonymisierung und ggf. der Pseudonymisierung sollte zusätzlich – da dies regelmäßig komplexe datenschutzrechtliche Fragestellungen sind – vorgeschrieben werden, dass die oder der behördliche Datenschutzbeauftragte so zu beteiligen ist, dass sie bzw. er die Erfüllung der Anonymisierungs- und Pseudonymisierungsvorgaben und die weiteren Voraussetzungen für die Rechtmäßigkeit einer Übermittlung effektiv beurteilen kann, so auch der Begründungstext. Selbstverständlich musste eine etwaige Verpflichtung zur Erstellung einer Datenschutz-Folgenabschätzung unberührt bleiben, was jedenfalls im Begründungstext zum Ausdruck gebracht wird.

Eine Übermittlung ohne Einwilligung zu Statistik- und Forschungszwecken setzt darüber hinaus die Erfüllung von besonderen Transparenzanforderungen voraus, zu denen eine klare Regelung getroffen werden sollte. Auch empfehlen wir dringend, um die Akzeptanz der Überlassung von Daten zu Forschungszwecken zu erhöhen und zum Ausdruck zu bringen, dass auch bei der Überlassung personenbezogener Daten zu Forschungs- und Statistikzwecken der Mensch im Vordergrund steht, ein voraussetzungsloses Widerspruchsrecht einzuräumen, dass die betroffenen Personen aufwandsarm ausüben können und über das sie angemessen zumindest in allgemeiner Form informiert werden sollten. Dies wird – zu Recht – auch im Entwurf der Novellierung des Krankenhausgesetzes vorgesehen. Eine Abweichung hiervon erschiene zumindest bei besonderen Kategorien personenbezogener Daten wertungswidersprüchlich.

Richtigerweise setzt der Entwurf gesteigerte Handlungspflichten für die übermittelnde öffentliche Stelle voraus. Hierzu gehört, dass die empfangende Stelle sich gegenüber der übermittelnden Stelle vorab verpflichten müsse, „ebenfalls Maßnahmen entsprechend Absatz 3 i.V.m. § 3 Absatz 1 zu treffen sowie die Daten zu anonymisieren, sobald der Personenbezug



für das Forschungsvorhaben nicht mehr erforderlich ist.“ Diese Regelung erscheint jedoch aus mehreren Gründen überarbeitungsbedürftig:

1. Die Regelung ist hinsichtlich der vom Empfänger zu übernehmenden Verpflichtungen nicht ausreichend. Beispielsweise:
 - a. Zwar wird die Geheimhaltung als solche benannt, eine Klarstellung des Adressatenkreises einer solchen Geheimhaltung bleibt allerdings - so etwa in der Gesetzesbegründung - aus. Explizit müssen der Empfänger und seine Beschäftigten sowie Auftragsverarbeiter zumindest zur Geheimhaltung der personenbezogenen Daten verpflichtet sein (vgl. § 3 Absatz 2 LDSG),
 - b. Der Empfänger muss dazu verpflichtet sein, die übermittelnden Daten ausschließlich zu den Zwecken zu verarbeiten, zu denen ihm die Daten übermittelt werden. Hierzu hat er angemessene organisatorische und technische Maßnahmen (z. B. ein schlüssiges Rechte- und Rollenkonzept) umzusetzen.
 - c. Der Empfänger muss zu einer Löschung der Daten nach Erreichung des Forschungszwecks verpflichtet sein.
 - d. Außerdem hat er sich zu verpflichten, die Daten zu anonymisieren, sobald dies im Rahmen des Forschungszwecks möglich ist, und zuvor die Daten nur pseudonym zu verarbeiten und durch angemessene technische und organisatorische Maßnahmen verhindern, dass ein Personenbezug hergestellt wird.
 - e. Zu begrüßen ist, dass der Empfänger die erhaltenen personenbezogenen Daten auch nicht anderen Verantwortlichen übermitteln darf. Es fehlt allerdings die Konkretisierung, dass der Empfänger dafür Sorge tragen muss, dass auch seine Auftragsverarbeiter die Verpflichtungen einhalten.
 - f. Der Empfänger muss verpflichtet sein, etwaige Verletzungen des Schutzes personenbezogener Daten in seiner Verantwortung der übermittelnden Stelle unverzüglich mitzuteilen. Diese hat sie wiederum in entsprechender Anwendung



der Regelungen in Artikel 33 und 34 der sie zuständigen Aufsichtsbehörde zu melden und sicherzustellen, dass unter den dort genannten Bedingungen auch die betroffene Person unterrichtet wird.

Diese Verpflichtungen unter Buchstabe f sind insbesondere deswegen wichtig, weil der Empfänger bei pseudonymisierten Daten die betroffenen Personen möglicherweise nicht ohne weiteres identifizieren und sie daher nicht benachrichtigen kann, und der LfDI Baden-Württemberg in solchen Fällen Anlass haben kann, die Rechtmäßigkeit der Übermittlung zu prüfen und seine Befugnisse in Bezug auf den Empfänger auszuüben (s. dazu noch sogleich unter 3.).

2. Die Regelung ist hinsichtlich der von der übermittelnden Stelle durchzufuhrenden Prüfungen nicht ausreichend: Die übermittelnde Stelle muss zumindest prüfen, inwieweit die empfangende Stelle nicht nur Gewähr für die Einhaltung ihrer Verpflichtungen bietet, sondern auch inwieweit die von ihr übernommenen Verpflichtungen durchsetzbar sowie dem Umfang nach angemessen sind,
3. Die Regelung ist hinsichtlich der Rechtsfolgen der durch den Empfänger einzugehenden Verpflichtungen nicht ausreichend. Unklar ist, wer die Einhaltung der Verpflichtungen prüft und zu wessen Gunsten sie eingegangen werden. Die Verpflichtung muss aber durchsetzbar und sanktionierbar sein, und zwar auch dann, wenn der Empfänger der Daten nicht oder nicht mehr unter der Aufsicht des LfDI Baden-Württemberg steht. Andernfalls wären sie ein bloßer bürokratischer Papiertiger.

Insofern ist zu bestimmen, dass

- a) die Verpflichtungen auch zugunsten der betroffenen Personen wirken müssen,
- b) dass die Befugnisse des LfDI BW zur Ausübung von Untersuchungs- und Abhilfemaßnahmen sich auch auf die Einhaltung der vertraglichen Verpflichtungen erstreckt, sofern der Empfänger seiner Aufsicht unterliegt,



- c) sofern der Empfänger nicht (oder nicht mehr) der Aufsicht des LfDI BW unterliegt,
dass
 - a. der LfDI BW die vertraglichen Rechte der übermittelnden Stelle neben dieser ausüben kann und die übermittelnde Stelle eine Pflicht zur Unterstützung des LfDI BW in Bezug auf die Durchsetzung der vertraglichen Pflichten trifft,
 - b. sich der Empfänger auch gegenüber der für ihn zuständigen Datenschutz-Aufsichtsbehörde verpflichtet, deren gesetzliche Untersuchungsmaßnahmen in Bezug auf die Einhaltung der Verpflichtungen zu befolgen.
 - c. der Empfänger sich wirksam verpflichtet, angemessene Vertragsstrafen für jeden Fall der Zu widerhandlung an den LfD BW zu zahlen.

Unabhängig davon müssen die Regelungen aus dem Kapitel V der Datenschutzgrundverordnung für Übermittlungen auch bei der Übermittlung zur Forschungs- und Statistikzwecken eingehalten werden.

Wir weisen darauf hin, dass wir auch bei der Novellierung des Landeskrankenhausgesetzes angemerkt haben, dass die Pflichten der Stelle, die personenbezogene Daten zu Forschungszwecken übermittelt werden, auch durch die Aufsichtsbehörde durchsetzbar sein müssen, und zwar auch dann, wenn der Empfänger selbst (beispielsweise weil er seinen Sitz außerhalb von Baden-Württemberg hat oder ihn nach Erhalt der Daten aus Baden-Württemberg hinaus verlegt) nicht der Aufsicht des LfDI BW unterliegt. Insoweit ist der uns bekannte Entwurf des Landeskrankenhausgesetzes unseren Hinweisen leider bislang nicht ausreichend gefolgt. Wir bitten dringend darum, dies in beiden Gesetzen – sowohl im Landesdatenschutzgesetz als auch im Landeskrankenhausgesetz – nachzuholen. Zum besseren Verständnis und zum Zwecke, hier eine Harmonisierung zu erreichen, fügen wir unsere Stellungnahme vom 02.06.2025 – Az.: LfDIAbt3-0554.9-269/2 – zum Entwurf der Novellierung des Landeskrankenhausgesetzes erneut bei.

Ergänzend weisen wir darauf hin, dass zumindest bei besonderen Kategorien personenbezogener Daten geprüft werden sollte, ob die Schaffung eines Straftatbestandes

nach dem Vorbild des § 9 GDNG sinnvoll und geboten ist. Der Straftatbestand des § 9 GDNG besteht nur bei Verarbeitung von Gesundheitsdaten zu Forschungszwecken; ein vergleichbarer Schutzbedarf durfte aber auch bei anderen besonderen Kategorien personenbezogener Daten bestehen.

Zu § 14 LDSG(-E):

Wir halten an unserer in unseren Stellungnahmen vom 6. November 2020 und vom 13. Februar 2024 geäußerten Auffassung fest, dass durch § 14 LDSG zu weitgehend in Betroffenenrechte eingegriffen wird. Insbesondere darf bloßer Verwaltungsaufwand i. S. v. § 14 Absatz 2 LDSG das Auskunftsrecht nicht schmälern. Insoweit ist auch ein Sonderrecht für die archivarische Verarbeitung nicht anzuerkennen. Und insbesondere auch eine Beschränkung des Berichtigungsrechts muss voraussetzen, dass dessen Geltendmachung auch im Einzelfall die Verwirklichung der im Archivzwecke unmöglich machen würde.

Wir weisen ferner darauf hin, dass § 14 Absatz 5 LDSG unklar ist, soweit in der ersten Variante die Löschung erst zulässig sein soll, „nachdem die Unterlagen dem öffentlichen Archiv angeboten und von diesem nicht als archivwürdig übernommen worden sind.“ Insoweit ist darauf hinzuweisen, dass auch im neuen Landesarchivgesetz vom 22. Juli 2025 der Begriff „archivwürdig“ nicht auftaucht. Der gesetzliche Terminus, auf den abzustellen sein dürfte, ist insoweit vielmehr die Feststellung bleibenden Werts. Dieser sollte daher auch im LDSG verwendet werden.

Zudem ist die Negativ-Voraussetzung („und von diesem nicht als archivwürdig übernommen worden sind“) nicht richtig formuliert, denn um diese zu erfüllen, müsste unbegrenzt abgewartet werden, ob das Archiv nicht doch noch den bleibenden Wert feststellt (so dass die Variante leerliefe und letztlich immer die in Variante 2 genannte Bewertungsfrist abzuwarten wäre). Nach dem geltenden Recht soll es aber möglich sein, dass das Archiv bereits vor Ablauf der Bewertungsfrist und sogar vor Ablauf der Aufbewahrungsfrist positiv feststellt, dass Unterlagen kein bleibender Wert zukommt. In diesen Fällen muss die sofortige Löschung nach Ablauf der Aufbewahrungsfrist zulässig (und verpflichtend) sein.

Zu § 15 LDSG-E:

Zu § 15 Absatz 2 Satz 2 LDSG-E

Zwar haben wir uns in unserer Stellungnahme zur Evaluation des LDSG vom 13. Februar 2024 dahingehend geäußert, dass eine Erweiterung des § 15 Absatz 2 LDSG durchaus zu überlegen sei, und einen Vergleich zu § 22 Absatz 1 Nummer 1 Buchstabe b BDSG gezogen. Wir weisen allerdings darauf hin, dass die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in ihrer Stellungnahme zur Evaluierung des Bundesdatenschutzgesetzes vom 2. März 2021 die Auffassung vertreten hat, dass § 22 Absatz 1 Nummer 1 Buchstabe b BDSG zu unbestimmt sei. Die Datenverarbeitung u.a. auf den Gebieten der Gesundheitsvorsorge und für die Beurteilung der Arbeitsfähigkeit von Beschäftigten könne nicht durch eine zentrale Generalklausel im BDSG legitimiert werden. Hier sei ausschließlich das jeweilige bereichsspezifische Fachrecht heranziehen und ggf. zu schaffen, welches sodann Art, Zweck und Umfang der Datenverarbeitung explizit zu regeln habe (s. https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf, S. 6, vgl. auch Petri, in: Simitis/Hornung/Spiecker gen. Dohmann, Datenschutzrecht, 2. Aufl. 2025, § 22 BDSG Rn. 27). Vor diesem Hintergrund halten wir die Übernahme einer Ermächtigungsgrundlage für die Verarbeitung personenbezogener Daten, die ähnlich weit wie § 22 Absatz 1 Nummer 1 Buchstabe b DS-GVO formuliert ist, zwar für überlegens-, aber letztlich nicht für empfehlenswert. Die Fürsorgepflicht des Dienstherrn als solche kann, anders als in der Gesetzesbegründung angegeben, keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sein, die Befugnis zur Datenverarbeitung muss durch spezielle Normen konkretisiert werden. Eine Ergänzung wie der beabsichtigte § 15 Absatz 2 Satz 2 LDSG sollte daher voraussetzen, dass die Datenverarbeitungen zu Zwecken der Gesundheitsvorsorge, der Arbeitsmedizin oder der Beurteilung der Arbeitsfähigkeit der Beschäftigten speziell geregelt ist.

Bei der Ergänzung, dass die Daten nur von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, empfehlen wir eine Orientierung an dem Wortlaut von Artikel 9 Absatz 3 DS-GVO. Problematisch ist insbesondere, dass die jetzige Formulierung so interpretiert werden kann, dass die Daten unter der Verantwortung von Personen, die „einer entsprechenden Geheimhaltungspflicht unterliegen“ auch durch Personen verarbeitet werden können, die keiner Schweigepflicht unterliegen und nicht zur Geheimhaltung verpflichtet

worden sind. Dies wäre nicht mit Artikel 9 Absatz 3 DS-GVO vereinbar. Hiernach dürfen die in Artikel 9 Absatz 1 DS-GVO genannten personenbezogenen Daten entweder durch Fachpersonal, das einem Berufsgeheimnis unterliegt, oder unter dessen Verantwortung oder von einer anderen Person, die ebenfalls einer Geheimhaltungspflicht unterliegt, verarbeitet werden. Die nach Erwägungsgrund 8 zur Datenschutz-Grundverordnung bei einer Übernahme ins nationale Recht notwendige Präzisierung der Datenschutz-Grundverordnung kann dadurch erreicht werden, dass das zur Verschwiegenheit verpflichtete Fachpersonal wie vorgeschlagen als „ärztliches Personal“ konkretisiert wird.

In § 15 Absatz 2 Satz 2 LDSG-E soll nunmehr formuliert werden. „Besondere Kategorien personenbezogener Daten dürfen auch verarbeitet werden, soweit ...“. Abweichend hiervon hieß es in dem Entwurf, der unserer Stellungnahme vom 10. Juni 2025 zugrunde lag, noch. „Satz 1 gilt entsprechend, soweit ...“. Die Änderung hätte allerdings zur Folge, dass dem Wortlaut nach die in § 15 Absatz 2 Satz 1 LDSG vorgesehene Interessenabwägung nicht erforderlich wäre. Wir weisen indes darauf hin, dass die von Artikel 9 Absatz 2 Buchstabe h DS-GVO vorausgesetzte Erforderlichkeit der Datenverarbeitung auf jeden Fall eine Interessenabwägung verlangt. Dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung nicht überwiegt, ist daher auch bei Datenverarbeitungen für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin oder der Beurteilung der Arbeitsfähigkeit der Beschäftigten Voraussetzung.

Zu § 15 Absatz 6 LDSG-E

Die aktuelle Formulierung von § 15 Absatz 6 LDSG verstehen wir so, dass die Verarbeitung der biometrischen Daten zu Authentifizierungs- und Autorisierungszwecken neben der Erforderlichkeit zum Erreichen des gewünschten Zwecks (der wohl noch immer in der Erfüllung der dienstlichen Aufgaben liegen muss) als zusätzliche Garantie im Sinne von Artikel 9 Absatz 2 Buchstabe b DS-GVO voraussetzen soll, dass die Beschäftigten zustimmen oder eine Dienstvereinbarung die Datenverarbeitung regelt (s. auch LT-Drs. 3930/16, S. 103). Auch insoweit gilt freilich, dass die Verarbeitung der besonderen Kategorien zum verfolgten dienstlichen Zweck auch angemessen sein muss.

Wir weisen darauf hin, dass eine Dienstvereinbarung selbst keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten begründen oder das Schutzniveau der DS-GVO absenken kann. Sie kann lediglich die Voraussetzungen für eine bereits nach Artikel 6 Absatz 1

Unterabsatz 1 Buchstabe e DS-GVO i.V.m. § 15 Absatz 1 und 2 LDSG zulässige Datenverarbeitung konkretisieren. Dies wird in EuGH, Urteil vom 19.12.2024 - C-65/23, klargestellt. Die Zulässigkeit der Datenverarbeitung richtet sich nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e DS-GVO i.V.m. § 15 Abs. 6 LDSG als Aufgabenzuweisung. Eine nähere Regelung der Datenverarbeitung in einer Betriebs- oder Dienstvereinbarung kann jedoch einen zusätzlichen Schutz der Rechte der betroffenen Beschäftigten bringen (vgl. Artikel 88 DS-GVO). Dies hat zunächst keine Auswirkungen auf die Ausgestaltung der Vorschrift, konnte sich aber als Klarstellung zur Auslegung in der Gesetzesbegründung anbieten.

Zudem bestehen weiterhin Unklarheiten hinsichtlich des Anwendungsbereichs von § 15 Absatz 6 LDSG. So könnte § 15 Absatz 6 LDSG dahingehend verstanden werden, dass alleine die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken besonderen Anforderungen unterliegt und im Übrigen die Verarbeitung biometrischer Daten im Beschäftigungsverhältnis zu anderen Zwecken ohne weitere Einschränkungen nach § 15 Absatz 1 und 2 LDSG zulässig wäre. Dies ist aber aus historischer und systematischer Sicht unzutreffend, vielmehr muss § 15 Absatz 6 so verstanden werden, dass die Verarbeitung biometrischer Daten grundsätzlich unzulässig, alleine aber zu Authentifizierungs- und Autorisierungszwecken unter den strengen Vorgaben des Absatz 6 zulässig ist (vgl. zum Ganzen Schweizer, Jacobi, Landesdatenschutzgesetz Baden-Württemberg, § 15 Nr. 2.6). Eine entsprechende Klarstellung wäre wünschenswert.

Wir halten darüber hinaus die spezifische Regelung von Maßnahmen zum Schutz der sensiblen biometrischen Daten, die zu den hier genannten Zwecken verarbeitet werden, für erforderlich. Hierzu sollte nicht nur bestimmt werden, dass die Daten ausschließlich für die genannten Zwecke verarbeitet und nicht Dritten zur Verfügung gestellt dürfen, sondern auch, dass die Daten zusätzlich so gespeichert werden müssen, dass aus ihnen die körperlichen Merkmale der betroffenen Person nicht rekonstruierbar sind (d. h. anhand der Daten kann zwar die Identität einer Person mit der berechtigten Person festgestellt werden, aber aus ihnen lassen sich nicht die körperlichen Merkmale der Person aktiv erschließen) und dass die Daten selbst nicht auslesbar sind. Diesen Vorgaben sind nicht nur unter dem Gesichtspunkt des Schutzes der Daten der Beschäftigten geboten, sondern sind auch unter IT-Sicherheitsgesichtspunkten zielführend. Wenn die Daten nämlich auslesbar wären, könnten Angreifer im Falle des Auslesens sich etwa durch Brute-Force-Angriffe die Authentifizierung bzw. Autorisierung erschleichen. In der Praxis werden die Vorgaben dazu führen, dass die Daten stets in einem Hardware-Sicherheitsmodul oder in sonstiger sicherer Hardware zu



speichern sein werden (was in der Entwurfsbegründung entsprechend ausgeführt werden konnte).

Zu § 15 Absatz 9 LDSG-E

Der Einsatz von KI im Beschäftigungsverhältnis benötigt eine datenschutzrechtliche Grundlage, die nicht in dem neuen § 15 Absatz 9 LDSG liegt. Eine Rechtsgrundlage könnte § 15 Absatz 1 LDSG sein, wenn dessen Voraussetzungen gegeben sind (insbesondere keine zumutbare datenschutzfreundlichere Alternative vorhanden ist und die Interessen der verwendenden Stelle am Einsatz der KI überwiegen). Hinsichtlich des Einsatzes von KI-Systemen bestehen bereits Informationspflichten nach Artikel 13 und 14 DS-GVO und für KI-Systeme im Sinne von Artikel 6 KI-VO und Artikel 50 KI-VO in Zukunft nach Artikel 26 Absatz 7 und 11 sowie aus Artikel 50 KI-VO. Damit durfte § 15 Absatz 9 LDSG nur einen begrenzten Mehrwert haben, konkret in Konstellationen, in denen bei einem KI-Einsatz die Voraussetzungen von Artikel 13 Absatz 2 Buchstabe f DS-GVO, Artikel 14 Absatz 2 Buchstabe g DS-GVO und Artikel 26 und 50 KI-Verordnung nicht vorliegen und auch der Zweck der Datenverarbeitung an sich ohne Erwähnung des KI-Einsatzes beschrieben werden kann. Nichtsdestotrotz ist die Aufnahme der Vorschrift eine begrüßenswerte Klarstellung, insbesondere hinsichtlich des Einsatzes wenig risikanter KI, die Entscheidungen nicht beeinflusst. Wir würden darüber hinaus vorschlagen, wenn in Absatz 9 auch Informationen über den involvierten Algorithmus und die Logik der Funktionsweise der KI verlangt werden. Dies würde einen über besagte Klarstellung hinausgehenden Mehrwert für betroffene Personen darstellen. Zudem könnte so der Anregung des Normenkontrollrats Rechnung getragen werden, zu prüfen, ob die Informationspflicht „ergänzend zu den Informationspflichten nach der KI-VO und der DSGVO“, wie es die Gesetzesbegründung ausführt, erforderlich ist.

Zu § 16 LDSG-E:

Wie in unserer Stellungnahme vom 13. Februar 2024 ausgeführt, ist für die Regelung in § 16 LDSG, insbesondere für Beschränkungen der Betroffenenrechte, keine Öffnungsklausel in der DS-GVO ersichtlich. Wie das Innenministerium in seinem Abschlussbericht zur Evaluierung des LDSG (S 103) zutreffend schildert, ist der Gesetzgeber beim Erlass der Norm davon ausgegangen, dass staatliche Verfahren zur Verleihung von Auszeichnungen und Ehrungen

gemäß Artikel 2 Absatz 2 Buchst. a DSGVO nicht unter die DSGVO fallen. Das ist unseres Erachtens auch angesichts der neueren Rechtsprechung des EuGH etwa zum Anwendungsbereich der Datenschutz-Grundverordnung auch auf die Verarbeitung personenbezogener Daten durch Parlamente nicht (jedenfalls nicht mehr) haltbar.

Es ist auch nicht richtig, die Betroffenenrechte in Bezug auf die Verarbeitung teils sehr sensibler Daten wie beispielsweise solche über strafrechtliche Verurteilungen auszuschließen. Dies stellt insbesondere eine erhebliche Beeinträchtigung der gebotenen Transparenz dar.

Zudem wird die Vergabe von Ehrungen und Auszeichnungen derzeit durch untergesetzliche Regelungen (etwa Bekanntmachungen des Ministerpräsidenten und Ausführungsbestimmungen hierzu, s. <https://stm.baden-wuerttemberg.de/de/themen/orden-und-ehrenzeichen>) normiert, wobei eine Vielzahl von Behörden potenziell die personenbezogenen Daten für die Entscheidungen über die Ehrungen und Auszeichnungen oder Vorschläge hierzu sollen verarbeiten können. Hier bedarf es mit Blick auf die Eingriffe in das informationelle Selbstbestimmungsrecht der betroffenen Kandidatinnen und Kandidaten dringend gesetzlicher Regelungen und Aufgabenzuweisungen. Die Norm des § 16 LDSG, die weder konkrete Aufgabenzuweisungen enthält noch sonst ausreichende Vorgaben für die Verarbeitung personenbezogener Daten (insbesondere noch nicht einmal den Grundsatz der Erforderlichkeit/Datenminimierung zum Ausdruck bringt) ist hierfür nicht hinreichend.

Wir empfehlen daher dringend, die Regelung des § 16 LDSG insgesamt aufzuheben und die Regelungen zur Verarbeitung personenbezogener Daten zu den dort genannten Zwecken einem eigenen Gesetz vorzubehalten. Denn die Materie, welche Behörde zu welchem Zweck welche personenbezogenen Daten soll verarbeiten dürfen, ist durchaus komplex und nicht ohne weiteres in einer Generalklausel zu ermöglichen (z. B.: Welche Behörde darf vorschlagen, welche entscheidet? Welche Informationen darf die vorschlagende, welche die entscheidende Behörde erheben? Welche Rückmeldung bekommt die vorschlagende Behörde? Wie lange sind die Informationen zu speichern? Welche Veröffentlichungsbefugnisse gibt es?).

Auch für die Verarbeitung eines Widerspruchs, wie jetzt im Entwurf vorgesehen, bedürfte es normenklarer gesetzlicher Regelungen und einer Verpflichtung zur Information hierüber.

Zu § 17 LDSG-E:

Wir begrüßen, dass die Generalklausel zur Verarbeitung besonderer Kategorien personenbezogener Daten nunmehr für sich steht und sich damit ihre Auffindbarkeit erhöht. In der Vergangenheit hatte ihre Stellung als Absatz 2 unter der Regelung von Zuverlässigkeitstests und weit entfernt von den anderen Generalklauseln der §§ 4 - 6 LDSG ihre Auffindbarkeit erheblich erschwert. Auch begrüßen wir die Aufnahme eines Mindeststandards an technischen und organisatorischen Schutzmaßnahmen durch den Verweis auf § 3 Nummer 1 - 3 und die ausführlicheren Erläuterungen zur Regelung in der Gesetzesbegründung, auch wenn insoweit noch fraglich bleibt, inwieweit die Maßnahmen spezifisch genug im Sinne von Artikel 9 Absatz DS-GVO sind. Insbesondere begrüßen wir, dass in der Gesetzesbegründung ausdrücklich formuliert wird, dass Protokollierungsmaßnahmen für jegliche Verarbeitung getroffen werden müssen. Wie bereits zu § 3 Absatz 1 Nummer 1 – neu – ausgeführt, stellt allein die Vornahme von Protokollierungsmaßnahmen noch keine ausreichende technisch-organisatorische Schutzmaßnahme dar. Insoweit ist auch die Entwurfsbegründung zu § 17 bislang noch unvollständig. Vielmehr sind nach § 3 Absatz 1 Nummer 1 nicht nur Maßnahmen zur Überprüfbarkeit bzw. Feststellbarkeit vorzusehen sind, ob und von wem (wann) bestimmte Verarbeitungsvorgänge veranlasst wurden, sondern es muss auch für die tatsächliche Durchführung regelmäßiger (wenigstens stichpunktartiger) Prüfroutinen und anlassbezogener Prüfungen gesorgt werden. Wir bitten darum, dies auch in der Gesetzesbegründung zu § 17 entsprechend zum Ausdruck zu bringen (s. dazu auch schon oben bei § 3).

Auch ist aus unserer Sicht zusätzlich zumindest noch vorzusehen, dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten auch die Maßnahmen aus § 3 Nummer 5 (Verschlüsselung), 6 (dauerhafte Sicherstellung der Schutzziele), 7 (Verfahren zur regelmäßigen Überprüfung der Maßnahmen) und 8 (Verfahren zum Schutz bei Zweckänderung) – jeweils nach der Nummerierung des vorgelegten Entwurfs – sowie die von uns empfohlene zusätzlich zu regelnde Schutzmaßnahme (der Abschottung) obligatorisch umgesetzt werden. Denn insgesamt sind die Vorgaben aus Artikel 9 Absatz 2 Buchstabe g DS-GVO zu erfüllen (die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich).

Grundsätzlich regen wir jedoch mit Blick auf die Systematik des LDSG an, die Regelung vollständig in den „Allgemeinen Teil“ zu verlegen, namentlich als § 3 oder § 4, da ihr Anwendungsbereich dann eindeutig zutreffend verstanden würde. Denn - wie oben bereits kurz geschildert - die Voraussetzung von § 17 LDSG-E müssen zusätzlich zu anderen Generalklauseln erfüllt werden, wenn auf deren Grundlage personenbezogene Daten besonderer Kategorien, also Daten im Sinne des Artikel 9 Absatz 1 DS-GVO, verarbeitet werden sollen.

Zu § 17a Absatz 2 LDSG-E

Angesichts der großen Bandbreite von Maßnahmen ganz unterschiedlicher Eingriffsintensität, die durch die bislang zu offene Formulierung des § 17a Absatz 2 Satz 1 ermöglicht würden - über die beispielhaft genannten Schulungs- und Sensibilisierungsmaßnahmen hinaus wären z.B. auch Datenabgleiche zur Zuverlässigkeitüberprüfung denkbar – verwundert es, dass insoweit – anders als für Zuverlässigkeitüberprüfungen nach § 17a Absatz 1 LDSG-E – keine Einwilligung (oder Zustimmung oder Widerspruchsmöglichkeit) der betroffenen Person vorgesehen ist.

Zudem bleibt das Verhältnis von § 17a Absatz 2 Satz 1 und Absatz 1 LDSG-E, deren Tatbestände sich überschneiden können, unklar. Wonach bemisst sich die Zulässigkeit der Zuverlässigkeitüberprüfung eines „Dritten“ (s. dazu noch sogleich), der Zugang zu Serverräumen zu Wartungszwecken erhalten soll? Man könnte insoweit sowohl § 17a Absatz 1 als auch § 17a Absatz 2 Satz 1 LDSG-E als die speziellere Vorschrift ansehen.

Eine Verarbeitung nach § 17a Absatz 2 Satz 2 LDSG-E darf nur stattfinden, wenn auch die Voraussetzungen von Satz 1 vorliegen, namentlich die dortigen Umstände (Zugang zu sicherheits- oder sicherheitstechnisch relevanten Datenverarbeitungsanlagen oder -geräten) und Zweckbestimmungen („zur Gewährleistung der Informationssicherheit, der Cybersicherheit oder des Funktionierens kritischer Infrastruktur erforderlich“).

Zudem sollten auch hier – sowohl aus Gründen der Informationssicherheit als auch aus Gründen des Schutzes des Rechts auf informationelle Selbstbestimmung – spezifische Vorgaben zu den Schutzmaßnahmen getroffen werden. Hierzu gehört, dass die Daten ausschließlich für die genannten Zwecke verarbeitet und nicht Dritten zur Verfügung gestellt dürfen, die Daten müssen zusätzlich so gespeichert werden, dass aus ihnen die körperlichen

Merkmale der betroffenen Person nicht rekonstruierbar sind und dass die Daten selbst nicht auslesbar sind (vgl. hierzu und zur Begründung schon unsere Ausführungen oben zu § 15 Absatz 6 LDSG-E).

Zu § 17b LDSG-E:

Eine Spezialregelung zur Offentlichkeitsarbeit ist grundsätzlich zu begrüßen und konnte geeignet sein, Rechtsunsicherheit, inwieweit personenbezogene Daten im Interesse der Offentlichkeitsarbeit einer Behörde auf gesetzlicher Grundlage, also ohne Einwilligung, verarbeitet werden dürfen, zu beseitigen. Indessen ist zweifelhaft, ob die zu weit geratene Regelung in § 17a LDSG-E geeignet ist, diese Ziele zu erfüllen, insbesondere die angestrebte Rechtssicherheit zu erreichen. Auch mit Blick auf Artikel 6 Absatz 3 Satz 1 DS-GVO und den Bestimmtheitsgrundsatz bestehen erhebliche Bedenken.

§ 17b Satz 1 LDSG-E enthält die Voraussetzung, dass Bürger_innen in „angemessener Weise“ informiert werden. Weder aus der Formulierung des § 17b Satz 1 LDSG, noch aus der Begründung ergibt sich, an welche Kriterien hier anzuknüpfen ist und an welche Art der Information gedacht ist. Dass die Zwecke auch „werblich“ sein dürfen, ist missverständlich und sollte gestrichen werden. Wie in der Entwurfsbegründung zu Recht ausgeführt, geht der Auftrag der Öffentlichkeitsarbeit dahin, die Öffentlichkeit mit „objektiv gehaltenen Informationen“ zu versorgen (vgl. u.a. BVerfGE, Urteil vom 16. Dezember 2014 - 2 BvE 2/14, (zuletzt) BVerfGE, Urteil vom 27. Februar 2028 - 2 BvE 1/16). „Werbung“ stünde dem diametral entgegen.

Auch bei der Mittelauswahl ist die Verwaltung nach dem Rechtsstaatsprinzip, Artikel 20 Absatz 3 GG, an Recht und Gesetz gebunden. Unklar ist auch, um welche Art von personenbezogenen Daten es gehen soll (soll beispielsweise auch ermöglicht werden, Interessensgebiete von Personen, Surfverhalten im Internet, bestimmte soziale Verhältnisse oder anderes mehr von Amts wegen erfasst und weiter verarbeitet werden dürfen, um die angesprochenen Informationen „zielgruppengenau“ verteilen zu können?), um wessen personenbezogene Daten es gehen soll (sollen beispielsweise auch solche von Beschäftigten verarbeitet, etwa veröffentlicht werden dürfen, ggf. inwieweit, und wie verhält sich die Regelung insoweit zu § 15? Sollen auch personenbezogene Daten von Nutzerinnen und Nutzern staatlicher Einrichtungen, von Schulerinnen und Schülern usw. verarbeitet werden

dürfen?) und wieso es nur um die Information von Bürgerinnen und Bürgern und nicht auch von anderen Personen oder Personengruppen (ohne deutsche Staatsbürgerschaft) gehen soll.

Der Gesetzesbegründung kann nicht entnommen werden, was unter „politischer Bildung“ und „Bürgerinformation“ zu verstehen ist. Mithin ist bereits unklar, zu welchen Zwecken personenbezogenen Daten überhaupt verarbeitet werden können.

§ 17b Satz 1 LDSG-E mit der zugehörigen Begründung suggeriert, dass nunmehr eine rechtssichere Grundlage für die Öffentlichkeitsarbeit, einschließlich der Nutzung sozialer Medien, besteht. Werden Daten der Bürger:innen über die Öffentlichkeitsarbeit hinaus etwa zur Analyse des Nutzerverhaltens ausgewertet, ist dies für die Öffentlichkeitsarbeit der Behörde nicht mehr erforderlich und unverhältnismäßig; entsprechende Datenverarbeitung ist rechtswidrig. Im Kontext der sozialen Medien sei auf die Komplexität und den Umfang der Erforderlichkeitsprüfung beim Einsatz durch öffentliche Stellen, die eingeschränkte Überprüfbarkeit und mangelnde Transparenz vieler Social Media Dienste, sowie auf die eingeschränkte Einflussnahmemöglichkeit auf Social Media Anbieter hingewiesen. Bei gemeinsamer Verantwortlichkeit (vgl. dazu u.a. EuGH C-210/16, C-683/21, C-604/22) erstreckt sich die Verantwortlichkeit auch auf die Datenverarbeitungen durch Plattformbetreiber und auf gemeinsame Erfüllung von Betroffenenrechten wie Auskunfts-, Lösch- oder Schadensersatzpflichten.

In der Entwurfsbegründung zu § 17b Satz 1 LDSG-E heißt es: „Hierbei wird 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.“ Diese Ausführungen sind unserer Auffassung nach schwer nachvollziehbar. Vernünftigerweise dürften Bürger_innen davon ausgehen, dass öffentliche Stellen keine personenbezogenen Daten außerhalb der gesetzlich zugewiesenen Aufgaben von ihnen verarbeiten, auch wenn sie öffentliche Dienste in Anspruch nehmen - wobei hier schon unklar ist, was darunter zu verstehen ist – oder sich über öffentliche Kanäle informieren.

Die Regelung in § 17b Satz 2 LDSG-E soll die Verarbeitung personenbezogener Daten im Rahmen des Veranstaltungsmanagements regeln. In der Tat besteht in der Praxis in diesem Kontext zuweilen eine Rechtsunsicherheit, inwieweit personenbezogene Daten ohne Einwilligung verarbeitet werden darf. Allerdings haben sich aus unserer Sicht in der Praxis

durchaus sachgerechte Fallkonstellationen etabliert, beispielsweise dafür, dass für die Versendung von Newslettern in der Regel auch Behörden auf die Einholung einer Einwilligung angewiesen sind. Dasselbe gilt unseres Erachtens grundsätzlich für das Erheben, Speichern (und ggf. Verwenden) von Kontaktdaten von Interessierten in Bezug auf Veranstaltungen. Eine Ausnahme kann insoweit nur anerkannt werden, soweit dienstliche Kontaktdaten von Personen der öffentlichen Verwaltung betroffen werden; deren Erhebung, Speicherung und Verwendung kann auch ohne Einwilligung gerechtfertigt werden, wenn es darum geht, dass diese Personen zu Veranstaltungen der öffentlichen Verwaltung eingeladen werden, soweit davon auszugehen ist, dass die Person an der Teilnahme an der Veranstaltung ein dienstliches Interesse haben könnte.

Gegen die Fertigung von Fotografien oder Videoaufnahmen von Besucherinnen und Besuchern einer Veranstaltung sowie deren Veröffentlichung ohne Einwilligung der Betroffenen haben wir durchgreifende Bedenken und verweisen insofern auf unsere Stellungnahme aus dem Jahr 2024. Eine Teilnahme an Informationsveranstaltungen der öffentlichen Hand muss diskriminierungsfrei auch ohne eine solche eingriffsintensive Maßnahme möglich sein, zumal wenn die öffentliche Hand solche Veranstaltungen im Rahmen eines Informationsauftrages organisiert und anbietet, und erst recht, wenn gar von einem korrespondierenden Informationsanspruch der Bürgerinnen und Bürger auszugehen ist. Das Erfordernis eines Widerspruchs birgt dagegen die Gefahr einer Diskriminierung. Auch zeigt die Möglichkeit zum Widerspruch, die angestrebte Datenverarbeitung (die bildlich-tonliche Erfassung und Veröffentlichung jeder teilnehmenden Person) gerade nicht im öffentlichen Interesse erforderlich ist. Um nicht zwingend erforderliche Datenverarbeitungen zu ermöglichen, sieht indes die Datenschutz-Grundverordnung das Institut der Einwilligung vor, deren Voraussetzungen - insbesondere die Abgabe einer entsprechenden Willenserklärung seitens der betroffenen Person - nicht unterlaufen werden dürfen. Allein das Ziel einer Vereinfachung des Verfahrens zugunsten der öffentlichen Verwaltung kann nicht herangezogen werden, um diesen weitgehenden Grundrechtseingriff zu rechtfertigen, eine Notwendigkeit können wir - wie ausgeführt - auch deswegen nicht erkennen, weil sich in der Praxis für diesen Regelungsbereich gut handhabbare Verfahrensweisen auch auf der Grundlage der bisherigen Regelung etabliert haben. Die nach dem Gesetzesentwurf heranzuziehenden Schranken von § 2 KUG und § 23 KUG können die Veröffentlichung von Bildern von Veranstaltungen nur rechtfertigen, wenn dies zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt. Nur dann liefert Artikel 85 Absatz 2 DS-GVO eine Öffnungsklausel, welche durch das KUG ausgefüllt werden kann. Für die Öffentlichkeitsarbeit besteht keine entsprechende Öffnungsklausel.

Soweit es entgegen unserer Empfehlung weiterhin bei der Widerspruchsregelung bleiben sollte, waren zumindest die Rechtsfolgen des Widerspruchsrechts klar zu regeln. Ebenso sollte in der Gesetzesbegründung klarstellend darauf hingewiesen werden, dass die Informationspflichten nach Artikel 13 und 14 DS-GVO bestehen. Dies bedeutet u.a., dass die betroffenen Personen zum Zeitpunkt der Erhebung zu informieren sind.

Zu § 18 LDSG-E:

Zur Überschrift

Die Einfugung des Begriffs „Videoschutz“ in der Überschrift des § 18 LDSG-E erschließt sich für uns nicht. Der Begriff wird an keiner anderen Stelle im Gesetz aufgegriffen und auch nicht definiert. Es ist sonst, auch im Paragraphen selber, immer die Rede von „Videoüberwachung“.

In Absatz 1 Satz 3 des Entwurfs findet sich zudem die Formulierung „*sofern die Videoüberwachung zum Schutz... erforderlich ist*“. Dies zeigt bereits, dass der Schutzaspekt nur einen Teilaspekt der Videoüberwachung ausmacht.

Die Benennung des Paragraphen nach diesem Teilaspekt, der zudem nicht näher definiert ist, ist irreführend.

Zu § 18 Absatz 1 Satz 2 LDSG-E

Satz 2 legt fest, dass es sich bei dem Schutz von Leben, Gesundheit und Freiheit von Personen um besonders wichtige öffentliche Interessen handelt.

Vor dem Hintergrund des Artikel 2 Absatz 2 des Grundgesetzes (GG) und Artikel 2 und 3 der Charta der Grundrechte der EU (GRCH) ist die Benennung dieser grundrechtlich gesicherten Schutzgüter als wichtige Schutzgüter zunächst nachvollziehbar.

Jedoch genießt auch der Schutz der personenbezogenen Daten nach Artikel 8 GRCh und die informationelle Selbstbestimmung nach Artikel 2 Absatz, Artikel 1 Absatz 1 GG Grundrechtsschutz.

Es muss daher immer eine Abwägung erfolgen, zwischen den beiden geschützten Grundrechten. Ein pauschales Überwiegen des einen Grundrechts kann nicht angenommen werden.

Zu § 18 Absatz 1 Satz 3 LDSG-E:

Allgemein zur Fiktion der Angemessen-/Verhältnismäßigkeit:

Der Absatz ist zu weit formuliert, sodass der Umfang der dadurch möglichen Videouberwachung nicht absehbar ist. Während in der Begründung zu Absatz 1 Satz 2 ausgeführt wird, dass eine Abwägung erfolgen muss (letzter Satz), würde hier die Abwägung vorweggenommen werden. Grundrechte der betroffenen Personen fänden keinen Platz mehr. Diese müssten pauschal zurücktreten. Die Begründung, dass „*die genannte Abwägung regelmäßig zugunsten einer Videoüberwachung als geeignetstes Mittel ausfallen*“ kann nicht nachvollzogen werden. Allein die Bewertung, dass dies „*regelmäßig*“ der Fall sei, zeigt bereits auf, dass eben nicht in jedem Fall davon ausgegangen werden kann, dass die Abwägung zugunsten des Einsatzes der Videoüberwachung ausfallen würde.

Es handelt sich bei der Videouberwachung um einen Eingriff in Artikel 8 GRCh, weshalb nach Artikel 52 Absatz 1 Satz 2 GRCh die Verhältnismäßigkeit gewahrt werden muss (vgl. EuGH, Urteil vom 1.8.2022 – C-184/20). Danach ist eine Gewichtung der legitimen Zwecke und der Rechte der betroffenen Personen „*auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen*“ geboten (Kühling/Buchner/Buchner/Petri DS-GVO Art. 6 Rn. 94).

Nicht berücksichtigt werden konnten bei einer solchen Fiktion zudem verschiedene weitere Abwägungspunkte wie z.B. Anzahl der betroffenen Personen oder „Art“ der betroffenen Personen (Kinder, Patienten einer anliegenden Praxis/Beratungsstelle etc.).

So wurde im Rahmen der Gesetzesbegründung 2018 zu Recht noch anerkannt, dass die Videouberwachung „*überwiegend Personen [erfasst], die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Dies stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen dar*“ (Drucksache 16 / 3930, S. 107).

Eine pauschale Fiktion dahingehend, dass die Abwägung immer zugunsten der Videoüberwachung ausfällt, ist daher abzulehnen und begegnet durchgreifenden verfassungsrechtlichen Bedenken. Für die verfassungsrechtliche Prufung der Verhältnismäßigkeit im engeren Sinne hat der Gesetzgeber gerade einen angemessenen Ausgleich zwischen der Schwere der Eingriffe in die Rechte potentiell betroffener Personen und der Pflicht des Staates zum Schutz der Grundrechte anderer zu treffen. Die Anforderungen an diesen Ausgleich sind mit dem aktuellen Regelungsentwurf nach unserer Bewertung nicht erfüllt.

Konkret zum Gesetzestext:

Der Gesetzestext ist unklar formuliert. Es ist z. B. nicht ersichtlich, auf welche der genannten Objekte sich das Merkmal „*sicherheitsrelevant[e]*“ bezieht. Im Gesetzestext steht dieser nur vor dem Begriff „*Einrichtungen*“. Die Gesetzesbegründung schreibt zusätzlich von „*sicherheitsrelevanten Dienstgebäuden*“. Ob auch bezüglich der „*Dienstfahrzeuge*“ der Begriff „*sicherheitsrelevant[e]*“ hinzugelesen werden muss, ist unklar.

Auch kann nicht nachvollzogen werden, wie durch die Videoüberwachung von Dienstfahrzeugen die Einsatzbereitschaft sichergestellt werden soll und was hierfür videoüberwacht werden kann/darf. Dies wird in der Praxis für Unklarheiten sorgen.

Bei der Überwachung von Kulturgütern i.S.d. § 2 Abs. 1 Nr. 10 Kulturschutzgesetz ist darauf zu achten, dass bspw bei der Überwachung von Gedenkstätten – ähnlich wie bei der Videoüberwachung von Gräbern – die Videoüberwachung kritisch zu bewerten sein kann, insbesondere vor dem Hintergrund, dass die Interessen der betroffenen Personen hier pauschal, ohne Abwägung im Einzelfall, im Rahmen der Abwägung unterliegen (vgl. hierzu 40. Tätigkeitsbericht, Datenschutz 2024, LfDI BW, S. 96ff, „Ruhe in Unfrieden“).

Zu § 18 Absatz 2 LDSG-E

Der bisherige Absatz 4 (Informationspflicht) soll gestrichen werden mit dem Verweis, dass Absatz 2 den Anforderungen an die Informationspflicht genügen würde

Die Informationspflicht ergibt sich bereits aus Artikel 13 DSGVO, sodass auf Absatz 4 insofern verzichtet werden kann. Die nach Absatz 2 zu machenden Angaben genügen jedoch nicht, um der Informationspflicht nach Artikel 13 DSGVO nachzukommen.

Eine Beschränkung der Transparenzpflichten ist mit dem vorrangigen europäischen Datenschutzrecht nicht vereinbar. Es ist auch nicht ersichtlich, aufgrund welcher Öffnungsklausel die Informationspflichten nach Artikel 13 DSGVO hier beschränkt werden sollen oder dass eine Ausnahme (Artikel 23 DSGVO i.V.m. § 8 LDSG) hier Anwendung fände. Die Datenerhebung bei der betroffenen Person erfolgt mit Erfassung der Daten, also zum Aufnahmepunkt, sodass regelmäßig Artikel 13 DSGVO einschlägig ist. Die betroffenen Personen müssen daher in diesen Fällen vor Betreten des erfassten Bereichs informiert werden.

Die Unterrichtung kann in Form eines Hinweisschildes, auf dem die nach Artikel 13 DSGVO erforderlichen Angaben hinterlegt sind, erfolgen. Allerdings ist die Praxis der ausschließlichen Verwendung von Hinweisschildern insoweit zu überdenken, als möglicherweise betroffene Personen nicht erreicht werden können, die den (optisch wahrnehmbaren) Inhalt eines Hinweisschildes nicht zur Kenntnis nehmen können, etwa wegen ihrer eingeschränkten Sehfähigkeit. Der Begriff „geeignete Maßnahmen“ muss daher europarechtskonform dahingehend ausgelegt werden, dass alle Informationen, über die nach Artikel 13 DSGVO informiert werden muss, der betroffenen Person mitzuteilen sind. Die Norm suggeriert derzeit jedoch, dass weniger (nur die benannten Angaben) mitzuteilen sind. Dies könnte irreführend für die öffentlichen Stellen sein.

Die Abrufmöglichkeit der Informationen nur mittels QR genügt zudem nicht. Es muss sichergestellt sein, dass auch ohne Smartphone die Möglichkeit zur Information besteht. Auf das Missbrauchspotenzial bei der Verwendung von QR Codes im öffentlichen Raum wird hingewiesen (vgl. das Phänomen des Quishing).

Wir weisen darauf hin, dass das in der Gesetzesbegründung erwähnte Muster DIN 33450 nur ein Kamerasymbol enthält und damit nicht die Informationspflichten erfüllt werden.

Zu § 18 Absatz 3 LDSG-E

Unklar ist, ob die Zweckänderung möglich sein soll, wenn die verantwortliche Stelle eigene Rechtsansprüche gelten machen will, oder ob dies auch zur Geltendmachung von Ansprüchen Dritter erfolgen soll, und wenn ja, unter welchen Voraussetzungen.

Zur beabsichtigten Aufhebung von § 18 Absatz 4 LDSG:

Die Informationspflicht wird nicht durch Absatz 2 erfüllt (siehe dazu schon oben). Wegen des Vorrangs der europarechtlichen Regelung wird sie zu erfüllen bleiben.

Zu § 18 Absatz 4 LDSG-E

Sind Videoaufnahmen für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig, ist der Verantwortliche verpflichtet, die Aufnahmen unverzüglich zu löschen, vgl. Artikel 17 Absatz 1 Buchstabe a DS-GVO (i. V. m. Artikel 5 Absatz 1 Buchstabe e DSGVO). Die zulässige Speicherdauer bei der Videoüberwachung durch nicht-öffentliche Stellen beträgt so i.d.R. maximal 72 Stunden (vgl. DSK Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, S. 22 f.). Davon abweichende Speicherdauern sind nur in Ausnahmefällen zulässig.

Die gemeindliche/öffentliche Videoüberwachung ist durchaus mit der Videoüberwachung durch nicht-öffentliche Stellen zu vergleichen; häufig überschneiden sich auch die mit der Videoüberwachung verfolgten Zwecke (Schutz vor Sachbeschädigung, Einbruch). Dabei stellt die Videoüberwachung durch öffentliche Stellen keine anderen Anforderungen an die Speicherdauer als diejenige durch nicht-öffentliche Stellen. Eine abweichende Regelung hinsichtlich der Speicherfrist für öffentliche Stellen ist deswegen nicht gerechtfertigt. Innegemeindliche Abläufe, die eine Sichtung der Bilder verzögern könnten, sind keine Rechtfertigung für eine längerfristige Speicherung von Bildern. Mit der Speicherdauer nimmt auch die Intensität des Eingriffes in die Rechte Gefilmter zu. Auch im nicht-öffentlichen Bereich kann die Auswertung von Videodaten komplex sein und auch dort gilt grundsätzlich, dass eine Speicherung nicht über 72h hinaus erfolgen kann.

Die Speicherung der Aufnahmen ist zudem als selbstständiger Verarbeitungsvorgang (Artikel 4 Nummer 2 DSGVO) rechtfertigungsbedürftig, d.h. die Speicherung selbst muss erforderlich,

angemessen und verhältnismaßig sein. Eine verlängerte Speicherung bis zu zwei Monaten ist daher im Einzelfall zu begründen. Beispielsweise ist an Feiertagen und in Urlaubszeiten eine Verlängerung von Speicherfristen möglich, wenn kein Geschäftsbetrieb erfolgt und Schäden nicht unmittelbar bemerkt werden können. Ggf. müssen im Einzelfall auch besondere Sachverhalte nachvollzogen werden, die sich über einen längeren Zeitraum erstrecken.

Eine verlangerte Speicherfrist kann indes nur für bestimmte Kameras in Sonderfällen gelten und nicht als Standard-Speicherdauer auf alle Kameras übertragen werden. Sie gilt - nach dem Grundsatz der Datenminimierung - außerdem nur für die Zeiten, an welchen beispielsweise eine Kontrolle der überwachten Bereiche nicht möglich ist, beispielsweise an Wochenenden oder in Ferien und Urlaubszeiten.

Bereits die derzeitige Regelung führt leider in der Tat oft zu Missverständnissen hinsichtlich der zulässigen Dauer der Speicherung. Aus der Praxis sind zudem keine Fälle bekannt, in welchen eine Speicherdauer von vier Wochen tatsächlich erforderlich gewesen wäre. Insoweit ist auch eine Ausweitung der Speicherdauer mangels praktischer Relevanz nicht erforderlich.

Zu § 18 Absatz 6 LDSG-E

Aus dem Gesetzeswortlaut und der dazugehörigen Gesetzesbegründung wird nicht klar, welche Sachverhalte konkret geregelt werden sollen. Nach der Gesetzesbegründung könnten sämtliche öffentlich zugängliche Flächen z.B. schon dann erfasst werden, wenn die Gefahr von Vandalismus besteht. Dies wurde dazu führen, dass die strengeren Voraussetzungen des Absatz 1 inhaltlich ausgehebelt werden. Der Gesetzeswortlaut selbst lässt entgegen Artikel 6 Absatz 3 Satz 2 DS-GVO keinen klaren Verarbeitungszweck erkennen, soweit eine „Videoüberwachung“ zum Zwecke des „Überwachens“ hierfür zulässig erklärt werden soll, erscheint das tautologisch.

Wir weisen zudem darauf hin, dass die Anforderungen des § 44 Absatz 3 Polizeigesetz nicht unterlaufen werden dürfen. Dies folgt u.a. aus der Streubreite des Mittels der Videoüberwachung und der Erfassung vieler unbeteiligter Personen, die keinen Anlass bieten, erfasst zu werden. Es ist äußerst fraglich, ob die Anforderungen des Bundesverfassungsgerichts an die Bestimmtheit und Normenklarheit gewahrt sind (vgl. 1 BvR 2368/06, Rn. 45 ff.).



Der Bedarf einer Regelung zur Erhaltung der Funktionsfähigkeit öffentlichen Eigentums kann unter bestimmten konkreten Umständen grundsätzlich nachvollzogen werden (z. B. Analyse der Straßenbeschaffenheit). Die vorliegende gesetzliche Regelung im Zusammenspiel mit der Gesetzesbegründung erscheint aus den oben dargelegten Gründen jedoch zu weitreichend.

Zu § 18a LDSG:

Die zu § 18 Absatz 6 gemachten Ausführungen gelten entsprechend.

Wir sehen bei der Videoüberwachung in nicht öffentlich zugänglichen Räumen einen höheren Schutzbedarf als bei öffentlich zugänglichen Räumen, da in öffentlich zugänglichen Bereichen typischerweise ohnehin damit zu rechnen ist, dass man beobachtet wird (wenngleich nicht unbedingt per Videoüberwachung) und die betroffenen Personen typischerweise ihr Verhalten ohnehin dem aufgrund der öffentlichen Zugänglichkeit bestehenden Beobachtungsdruck anpassen.

Wenn neben der „Überwachung des Erhaltungszustands und der Funktionsfähigkeit des Eigentums öffentlicher Stellen“ weitere Zwecke verfolgt werden, dann sollten sich diese transparent im Gesetzestext widerspiegeln.

Die Rechtsgrundlage sollte sich daher auf enge Anwendungsfälle beschränken und keinesfalls die Anforderungen unterschreiten, die nach der geltenden Rechtslage an die Videoüberwachung öffentlich zugänglicher Räume gestellt werden.

Sollten die Überwachungszwecke über § 18 Absatz 6 LDSG hinausgehen, regen wir daher dringlich an, diese noch festzulegen. So könnte die Videoüberwachung für den Fall explizit gestattet werden, dass eine öffentliche Einrichtung ihre Innenräume zu Zeiten überwachen will, zu denen mit der Anwesenheit berechtigter Personen in den überwachten Räumlichkeiten nicht zu rechnen ist, aber Anhaltspunkte für eine Gefahr im Sinne von § 18 Absatz 1 Nummer 1 oder 2 LDSG bestehen.

Zu § 18b LDSG:

Anhand des Gesetzestextes und der –begründung ist für uns nicht ersichtlich, welche Arten von Überwachungen hierdurch zu welchem Zweck und unter welchen Umständen geregelt werden sollen, und ob diese nicht bereits durch den neuen § 3a erfasst werden. Eine Überwachung als Selbstzweck (nach dem Wortlaut soll auch hier eine Überwachung zu Zwecken der Überwachung stattfinden) kann datenschutzrechtlich nicht nachvollzogen werden; eine hinreichende Zweckbestimmung im Sinne von Artikel 6 Absatz 3 Satz 2 liegt daher nicht vor. Auch der Verhältnismaßigkeitsgrundsatz ist in diesem Kontext zu berücksichtigen.

Zudem weisen wir darauf hin, dass Tonaufnahmen einen gravierenden Eingriff in die Persönlichkeitsrechte der betroffenen Personen darstellen (vgl. § 201 StGB).

Weiter bleibt auch unklar, wie in den Fällen des § 18b betroffene Personen nach Artikel 13 DSGVO informiert werden sollen.

Nach unserer Bewertung sind insgesamt die Anforderungen an die Bestimmtheit der Norm nicht erfüllt.

Zu § 25 LDSG:

Wir sehen nach wie vor dringenden Anpassungsbedarf an die europarechtlichen Vorgaben in Bezug auf § 25 Absatz 4 und 5 LDSG und verweisen insoweit auf unsere Stellungnahmen vom 6. November 2020 und 13. Februar 2024. Die dort vorgebrachten Argumente werden u. E. durch den Abschlussbericht des Innenministeriums zur Evaluierung des LDSG nicht ausreichend entkräftet.

Zu § 27a LDSG-E:

Der LfDI begrüßt die Ergänzung der Zuständigkeit des LfDI und die Klarstellung, dass der LfDI auch im Bereich Digitale Dienste Befugnisse nach Art. 58 DS-GVO hat. Diese Befugnisse spielen bisher in der Aufsichtspraxis des LfDI zur DS-GVO eine entscheidende Rolle und

werden nunmehr auch im Bereich Digitale Dienste zur effektiven Durchsetzung des Telekommunikations-Digitale Dienste-Gesetz maßgeblich beitragen.

Zu Artikel 2 – Änderung des E-Government-Gesetzes Baden-Württemberg (eGovG)

Zu § 17a eGovG:

Allgemeines/Verhältnis zu §§ 15a bis 15c eGovG-E

Unter Berücksichtigung des uns bereits am 28 Februar 2025 übersandten Entwurfs eines Änderungsgesetzes zum E-Government-Gesetzes Baden-Württemberg bleibt uns der datenschutzrechtliche Anwendungsbereich und Regelungsgehalt des neuen § 17a eGovG unklar.

Die avisierten Regelungen in §§ 15a bis 15c des Entwurfs des E-Government-Gesetzes Baden-Württemberg normieren die Datenverarbeitung im Dienstleistungsportal des Landes (a), die Rechtsgrundlagen der Datenverarbeitung in einem Onlinedienst (b) und datenschutzrechtliche Verantwortlichkeiten (c), wobei alle drei Normen auf das Landesdatenschutzgesetz, insbesondere § 3 Absatz 1 LDSG, verweisen. Warum neben den Regelungen zur Erprobung und dem Einsatz von KI-Anwendungen im geänderten Landesdatenschutzgesetz auch im E-Government-Gesetz Regelungen zum Einsatz von KI-Anwendungen aufgenommen werden sollen, erschließt sich uns nicht.

Es wird um entsprechende Überprüfung einer möglichen Doppel-Regelung und damit der Gefahr sich widersprechender Regelungen gebeten.

Im Übrigen nehmen wir auf unsere Stellungnahmen zu dem bezeichneten Entwurf eines Änderungsgesetzes zum E-Government-Gesetz vom 18.03.2025 - Az.: LfDIAbt2-0554.2-2/37 - und vom 27.03.2025 - LfDIAbt1-0554.2-4/17 - Bezug.

Unabhängig davon, dass uns der Anwendungsbereich unklar bleibt, weisen wir noch auf die folgenden Punkte hin.

Zu § 17a Absatz 1 eGov-E

Der Ausdruck „KI-System“ ist in Art. 3 Nr 1 KI-VO europarechtlich legal definiert und genießt insofern Anwendungsvorrang. Die Verweisung ist mithin entbehrlich.

Gemäß dem Wortlaut von Absatz 1 dient der Paragraph der Erprobung eines vollständig automatisierten Erlasses von Verwaltungsakten mit Anwendungen der Künstlichen Intelligenz. Der Wortlaut in Absatz 1 erscheint irreführend, da gemäß Absatz 5 des Paragraphen die Landesregierung ermächtigt wird, durch Rechtsverordnung den vollständig automatisierten Erlass von Verwaltungsakten im Rahmen des § 35 a des Landesverwaltungsverfahrensgesetzes (LVwVfG) zuzulassen.

Es wird um entsprechende Überprüfung gebeten.

Zu § 17a Absatz 2 eGovG-E allgemein

Während in der Begründung auf § 88 Absatz 5 der Abgabenordnung Bezug genommen wird, unterbleibt in der Regelung eine entsprechende Regelung zur Erforderlichkeit eines Risikomanagements. Es bleibt unklar, warum dieser Ansatz keine entsprechende Umsetzung in der Norm erfahren hat.

Wir können insgesamt nicht ohne weiteres erkennen, dass der Regelungsentwurf gemäß Artikel 22 Absatz 2 Buchstabe b DS-GVO „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten“ würde. Soweit in der Entwurfsbegründung ausgeführt wird, diesen Voraussetzungen werde 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 Bekanntgabeerfordernis gemäß § 41 LVwVfG sowie zu den Rechtsbehelfsmöglichkeiten hinreichend Rechnung getragen, können wir so nicht erkennen, zumal den spezifischen Gefahren der automatisierten Verarbeitung dadurch nicht hinreichend Rechnung getragen wird und zudem von den in § 17a Absatz 2 Satz 2 eGovG-E genannten Voraussetzungen schon bei Vorliegen einer einzigen von einem Überwiegen der Interessen der Stelle ausgegangen werden soll.

Zu § 17a Absatz 2 Satz 2 Nummer 1 eGovG-E

Liegt ein Einverständnis i.S. einer Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO vor, kann nicht zugleich von einem überwiegenden Interesse der verantwortlichen Stelle ausgegangen werden. Eine Verarbeitung der personenbezogenen Daten erfolgt dann vielmehr ausschließlich aufgrund der vorliegenden datenschutzrechtlichen Einwilligung. Diese muss zudem nach Artikel 22 Absatz 2 Buchstabe c DS-GVO ausdrücklich erteilt werden; von diesem Erfordernis einer ausdrücklichen Erklärung kann nicht ohne weiteres durch mitgliedsstaatliches Recht unter Berufung auf Artikel 22 Absatz 2 Buchstabe b DS-GVO abgewichen werden.

Zu § 17a Absatz 2 Satz 3 und 4 eGovG

Unklar bleibt, warum die getroffene Regelung nicht ausdrücklich auf § 39 Abs. 2 Nr. 1 und 2 LVwVfG Bezug nimmt und somit Rechtsklarheit für die Verantwortlichen herstellt.

Zu § 17a Absatz 3 eGovG

Unklar bleibt, welche Unterlagen gemäß der DS-GVO (bspw. Datenschutz-Folgenabschätzung) und der KI-VO (bspw. Grundrechts-Folgenabschätzung) verantwortliche Stellen mit der Anzeige des Vorhabens vorlegen müssen, um eine präventive Prüfung von der obersten Fachaufsichtsbehörde und dem für das Verwaltungsverfahrensrecht zuständigen Innenministerium zu ermöglichen

Zu § 17a Absatz 4 eGovG

Fraglich erscheint uns, ob eine Erprobungszeit von 2 bis 5 Jahren verhältnismäßig ist, ohne dass die Datenverarbeitung zeitnah in einer Rechtsverordnung geregelt wurde.

Zu Artikel 4 – Änderung des Landesinformationsfreiheitsgesetzes

Zu § 2 Absatz 3 LIFG-E:

§ 2 Absatz 3 des LIFG soll wie folgt gefasst werden:

„Keine Informationspflicht nach diesem Gesetz besteht für [...]“

Außerdem soll unter Ziff. 5 neu eingefügt werden:

„Informationen, die die Freiheit der Kunst, Wissenschaft, Forschung oder Lehre betreffen sowie [...]“

Unter Ziff. 6 neu soll eingefügt werden.

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

Hierzu nehmen wir aus Sicht der Informationsfreiheit wie folgt Stellung:

Allgemeines

„Keine Informationspflicht nach diesem Gesetz besteht für [...]“

Entsprechend der geltenden Gesetzesystematik formuliert § 2 Absatz 3 des LIFG derzeit echte Bereichsausnahmen, welche sich auf die jeweiligen Stellen beziehen. Dies sollte nach der ursprünglichen Gesetzesbegründung gerade nicht dazu führen, dass Informationen bei anderen Stellen nicht zugänglich gemacht werden müssen (vgl. LT Drs. 15/7720, S. 61).

Die nun avisierte Aenderung von stellenbezogenen Bereichsausnahmen auf informationsbezogene Bereichsausnahmen wird für systemwidrig erachtet. Zusätzlich führen

die Verwendung von unbestimmten Rechtsbegriffen und der weite Anwendungsbereich zu Schwierigkeiten bei der Rechtsanwendung. Ein erhöhter bürokratischer Aufwand aufgrund der zusätzlichen Prufverfahren und der nicht definierten Tatbestandsmerkmale ist zu erwarten.

Im Sinne eines klaren Gesetzesaufbaus wäre es erstrebenswert, den Charakter einer rein stellenbezogenen Bereichsausnahmeverordnung beizubehalten. Diese Systematik hat ursprünglich auch der Gesetzgeber unterstrichen. In der Gesetzesbegründung hierzu heißt es, dass ein informationsbezogener Schutz über §§ 4 bis 6 LIFG gewährleistet wird (LT-Drs. 15/7720, S. 61). Die Kombination von informationsbezogenen und stellenbezogenen Ausnahmen in einer Norm führt jedenfalls zu einer Prfung mit gesteigerter Komplexität für die informationspflichtigen Stellen, anstatt mehr Klarheit zu schaffen.

Die Aufnahme der informationsbezogenen Ausnahmen ist aus Sicht des LfDI BW nicht, jedenfalls nicht in dem avisierten Umfang, erforderlich. Bereits im Zuge der Evaluation zum Landesinformationsfreiheitsgesetz hatten wir darauf hingewiesen, dass die Bereichsausnahmen unter § 2 Absatz 3 LIFG zu weitgehend formuliert sind und auf ein Minimum reduziert werden sollten. In vielen Bereichen ist den öffentlichen Belangen mit den Ausnahmeverordnungen des § 4 LIFG hinreichend Rechnung getragen. Mit den nun neu hinzukommenden Ausnahmen, wird der Zugang von amtlichen Informationen für die Öffentlichkeit noch weiter beschränkt. Vor dem Hintergrund, dass einige Gesetze der anderen Länder mittlerweile zu Transparenzgesetzen mit Veröffentlichungspflichten weiterentwickelt wurden, entspricht das weitere Ausweiten der Bereichsausnahmen in § 2 Absatz 3 LIFG jedenfalls nicht mehr dem heutigen rechtlichen Standard von Informationsfreiheitsgesetzen.

Begründung im Einzelnen:

Zu § 2 Absatz 3 Nr. 5 LIFG-E (Forschung)

Es soll eine neue informationsbezogene Ausnahmeregelung in § 2 Absatz 3 Nr. 5 LIFG-E eingeführt werden. Diese lautet wie folgt. „Keine Informationspflicht besteht für [.] Informationen, die die Freiheit der Kunst, Wissenschaft, Forschung oder Lehre betreffen“.

Die stellenbezogene Bereichsausnahme für die Schulen nach § 2 des Schulgesetzes für Baden-Württemberg soll beibehalten werden.

Bislang wurde die Bereichsausnahme zugunsten der Kunst- und Wissenschaftsfreiheit formuliert für Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung und Hochschulen nach § 1 LHG soweit die Forschung, Kunst oder Lehre betroffen sind. Mit der neu formulierten Ausnahme wird diese bisherige einrichtungsbezogenen Bereichsausnahme nach § 2 Absatz 3 Nummer 2 LIFG isoliert und als neue informationsbezogene Ausnahme definiert.

Dass grundsätzliche Bedenken aufgrund des Systembruchs des Landesinformationsfreiheitsgesetzes bestehen, wurde bereits oben unter Allgemeines angemerkt.

In den Gesetzen der anderen Bundesländer findet sich entweder keine explizite Bereichsausnahmeregelung für die Forschung, oder aber sie ist einrichtungsbezogen formuliert. Soweit eine einrichtungsbezogene Formulierung in den anderen Gesetzen nicht gegeben ist, handelt es sich jedenfalls um eine begriffliche Einschränkung dahingehend, dass die „Grundlagenforschung“ und die „anwendungsbezogene“ Forschung benannt sind. Lediglich in Hessen findet sich eine Regelung, die zu einem informationsbezogenen Verständnis führt. Hier ist in § 81 Absatz 1 Nr. 6 HDSIG zunächst eine einrichtungsbezogene Ausnahme formuliert. Der dortige Absatz 3 normiert jedoch wie folgt. Soweit ein Informationszugang nach Absatz 1 oder 2 ausgeschlossen ist, gilt dies auch für Datei- und Aktenbestandteile, die sich in Dateien oder Akten anderer öffentlicher Stellen befinden

Das Einfügen einer informationsbezogenen Ausnahme ist nicht erforderlich. Insbesondere hat auch der VGH in der in der Gesetzbegründung genannten Entscheidung (VGH BW Urteil vom 25.10.2023 – 10 S 125/22) eine Regelungslücke nicht gesehen, die geschlossen werden musste – im Gegensatz zu vorhandenen Informationen im Bereich der Kirchen, Religions- und Weltanschauungsgemeinschaften, in welchem eine planwidrige Regelungslücke explizit aufgezeigt wurde.

Der Gesetzgeber ging bei der bisherigen Formulierung als stellenbezogene Bereichsausnahme ebenfalls davon aus, dass die derzeitige Regelung die Wissenschafts- und Kunstfreiheit wahrt (LT Drs 15/7720 S. 61). Im Bereich der Drittmittelforschung ist mit § 41a Landeshochschulgesetzes (LHG) ebenfalls bereits eine hinreichende Regelung zum Zugang getroffen.



Als Anlass für die Gesetzänderung wird die Entscheidung des VGH BW vom 25.10.2023, namentlich VGH BW Urteil vom 25.10.2023 – 10 S 125/22, aufgeführt. Hiernach mussten Informationen über bei der Tierschutzbehörde beantragte bzw. angezeigte Tierversuche im Rahmen von Aus-, Fort- und Weiterbildungsveranstaltungen im Bereich Humanmedizin zugänglich gemacht werden.

Der VGH BW hat in seiner Entscheidung jedoch ausgeführt, dass die Nichtanwendbarkeit des § 2 Absatz 3 Nr. 2 LIFG auf die bei der informationspflichtigen Stelle vorhandenen Informationen unter verfassungsrechtlichen Gesichtspunkten mit Blick auf den Schutz der Wissenschaftsfreiheit gerade unbedenklich sei. Aus diesem Grund wurde auch eine Vorlage an das Bundesverfassungsgericht oder den Verfassungsgerichtshof nicht für erforderlich erachtet. Insbesondere wurde aufgezeigt, dass auch die Freiheit der Forschung und Lehre verfassungsimmanenter Schranken unterliegt, welche vorliegend beispielsweise durch ein auf Artikel 20 a GG gestütztes öffentliches Informationsinteresse definiert sein können (vgl. VGH a.a.O. Rn. 58).

Nicht entscheidungserheblich war im Übrigen eine etwaige Offenlegung des Forschungsgeheimnisses, die eine solche gesetzliche Anpassung rechtfertigen würde. Der VGH BW sah die Forschung in dem von ihm zu entscheidenden Fall überhaupt nicht betroffen und den Bereich der Lehre nur punktuell.

Darüber hinaus ist die derzeitige Formulierung zu unbestimmt.

Die Formulierung, „Informationen, die die Freiheit der Kunst, Wissenschaft, Forschung oder Lehre betreffen“, geht weit über den von der Verfassung vorgegebenen Schutz hinaus. Die Ausnahme ist hierdurch denkbar weit formuliert und durfte in der Praxis zu erheblichen Auslegungsschwierigkeiten führen. Die informationspflichtigen Stellen werden durch eine solche weitgehende Prüfung unbestimmter Tatbestandsmerkmale zusätzlich belastet. Weiterhin durfte es, um den verfassungsrechtlichen Schutz der Kunst- und Wissenschaftsfreiheit zu gewährleisten, ausreichend sein, eine Ausnahme erst bei einer „Beeinträchtigung“ anstatt bei einer „Betroffenheit“ zu formulieren.

Bereits der derzeit im Gesetz genannte Begriff der Forschungseinrichtung ist denkbar weit zu verstehen (*HK-IZR BW/Corinna Sicko, 1. Aufl. 2017, LIFG § 2 Rn. 55-57, beck-online*) und demnach bereits weitgehend genug, um die Freiheit der Wissenschaft zu schützen.

Aber auch dieser Begriff ist nicht rechtlich geschützt und demnach nicht unumstritten. Jedenfalls können die entsprechenden Einrichtungen sich aber auf im Hintergrund stehende Forschungsaufträge und die Definition des § 1 LHG berufen. Wenn nun aber die Ausnahme, wie angedacht, auf „Informationen, die die Forschung betreffen“ formuliert wird, wird dies zu weit größeren Abgrenzungs- und Auslegungsschwierigkeiten als bisher führen sowie umfangreiche Prüfverfahren bei den Stellen verursachen, da ein einrichtungsbezogenes Indiz ja gerade nicht mehr relevant ist. Mit dieser Ausnahme werden zusätzlich auch informationspflichtige Stellen den Forschungsbegriff prüfen und bewerten müssen, die in der Regel keine Berührungspunkte hiermit haben.

Weiterhin kann es sich bei den hier gegenständlichen Informationen insbesondere um Unterlagen anderer Forschungseinrichtungen ggf. auch privater Einrichtungen handeln. Es stellt sich daher die Frage, ob eine etwaige Unsicherheit bei den informationspflichtigen Stellen, ob denn die Forschung im Sinne der Ausnahmeverordnung betroffen ist, ein Drittbeziehungsverfahren auslösen müsste.

Hierzu ist im aktuellen Entwurf keinerlei Regelung vorgesehen. Da Drittbeziehungsverfahren ein erheblicher Zeit- und Kostenfaktor sind, die insbesondere auch für antragstellende Personen schwer nachvollziehbar sind, sollte dies unbedingt gesetzlich klargestellt werden. Auch für die informationspflichtigen Stellen gehen Drittbeziehungsverfahren regelmäßig mit einem erheblichen Mehraufwand einher. Zusammenfassend lässt sich vor diesem Hintergrund Folgendes festhalten: Die Erforderlichkeit der Durchführung einer Drittbeziehung sowie der Zeit- und Kostenfaktor im Rahmen des Verfahrens führen in der Praxis häufig zu Unsicherheiten und Divergenzen, weshalb der LfDI BW eine klare Regelung hierzu für wichtig erachtet.

Zu § 2 Absatz 3 Nr. 6 LIFG-E (Kirchen und Religionsgemeinschaften)

Unter § 2 Absatz 3 Nr. 6 LIFG-E soll folgende informationsbezogene Ausnahme neu eingefügt werden:

„Keine Informationspflicht besteht für [] Angelegenheiten der Kirchen, der Religions- und Weltanschauungsgemeinschaften sowie ihrer Untergliederungen und Einrichtungen, soweit diese dem religiösen Selbstbestimmungsrecht unterfallen“

Diese Ausnahme wird nach der Gesetzbegründung aufgenommen zum „Schutz des religiösgemeinschaftlichen Selbstbestimmungsrechts aus Artikel 140 GG in Verbindung mit Artikel 137 Absatz 3 der deutschen Verfassung vom 11. August 1919 (Weimarer Reichsverfassung, WRV).“

Die in dieser Bereichsausnahme genannten Stellen sind keine informationspflichtigen Stellen im Sinne des Landesinformationsfreiheitsgesetzes und demnach derzeit nicht zur Zugänglichmachung von Informationen verpflichtet. Begründet wird die Einführung dieser Ausnahme mit der Entscheidung des VGH BW vom 08.11.2023 (Az.: 10 S 916/22), in welcher in Bezug auf Informationen einer Religionsgemeinschaft, die bei einer auskunftspflichtigen Stelle vorlagen, eine planwidrige Regelungslücke aufgezeigt wurde.

Derzeit ist im Landesinformationsfreiheitsgesetz keine Regelung enthalten, die das von Artikel 140 GG in Verbindung mit Artikel 137 Absatz 3 Satz 1 WRV geschützte Selbstbestimmungsrecht der Religionsgemeinschaften hinreichend berücksichtigt. Ein normativer Anknüpfungspunkt für eine verfassungskonforme Auslegung wurde vom VGH BW in seiner oben zitierten Entscheidung nicht gesehen.

Der VGH führt hierzu wie folgt aus:

„Die Religionsgemeinschaften haben das verfassungsrechtlich garantierte Recht, alle eigenen Angelegenheiten gemäß den spezifisch religiösgesellschaftlichen Ordnungsgesichtspunkten, d. h. auf der Grundlage ihres religiösen Selbstverständnisses, rechtlich gestalten zu können (vgl. VGH Baden-Württemberg, Urteil vom 08.05.2009 - 1 S 2859/06 - juris Rn. 49 m. w. N.). Dabei obliegt die Definitionsmacht hinsichtlich der Frage, was zu dem hiernach geschützten inneren Bereich gehört, in den Grenzen der Plausibilität in erster Linie den Religionsgemeinschaften selbst nach Maßgabe ihres eigenen religiösen Selbstverständnisses (vgl. Korieth in Dürig/Herzog/Scholz, GG, Art. 137 WRV Rn. 26 ff. m. w. N.)“

Vor diesem Hintergrund ist die Bestrebung, diese Regelungslücke zu schließen nachvollziehbar.

Jedoch ist aus Sicht der LfDI BW durch das Einfügen dieser informationsbezogenen Ausnahme in § 2 Absatz 3 LIFG neu wiederum ein Systembruch zu sehen und auch hier der Formulierung zu unbestimmt.

Die Bereichsausnahmeverordnung nach § 2 Absatz 3 LIFG betrifft bislang Stellen, die grundsätzlich als öffentlich-rechtliche Stelle informationspflichtig wären, jedoch aus bestimmten Gründen hiervon ausgeschlossen werden. Bei den Religionsgemeinschaften selbst handelt es sich nach § 3 Nr. 2 LIFG i.V. m. § 2 Absatz 1 LIFG nicht um informationspflichtige Stellen. Vor diesem Hintergrund ist auch keine Bereichsausnahme zu formulieren.

Vielmehr ist die zu regelnde Konstellation so geartet, dass hier Informationen Dritter (der Kirchen, Religions- oder Weltanschauungsgemeinschaften) bei einer informationspflichtigen Stelle vorliegen könnten und deshalb als vorliegende amtliche Information herausgegeben werden müssten.

Die Interessenlage entspricht hier also vielmehr derjenigen des § 6 Satz 2 LIFG. Indem der VGH BW die Analogie zu den Betriebs- und Geschäftsgeheimnissen hergestellt hat, wurde diese vergleichbare Interessenlage ebenfalls gesehen. Der VGH BW hat explizit erwähnt, dass die Gewährung des Schutzes verfassungsrechtlicher Güter zentrales Regelungsziel des § 6 Satz 2 LIFG ist (VGH BW a.a.O., Rn. 63). Die Vorschrift des § 6 LIFG ist gerade für Fälle normiert, in welchen der Informationszugang aufgrund einer Drittberoffenheit nicht oder nicht vollständig gewährleistet werden kann.

Gerade auch deshalb, weil die „Definitionsmacht“ (VGH BW a.a.O., Rn. 62) über die Beeinträchtigung der Selbstverwaltungsgarantie – genau wie bei den Betriebs- und Geschäftsgeheimnissen – bei den jeweiligen Kirchen, Religions- und Weltanschauungsgemeinschaft selbst liegt, ist ein Gleichlauf mit der bereits definierten Ausnahme in § 6 LIFG zu sehen.

Wir empfehlen daher, die angestrebte informationsbezogene Ausnahme in § 6 LIFG aufzunehmen, um hier die gesetzliche Systematik nicht zu durchbrechen.



Weiterhin ist die neu einzufügende Nr. 6 zu unbestimmt formuliert. „Angelegenheiten“ ist kein normenklarer Begriff und wird zu Auslegungsschwierigkeiten führen. Die Begrifflichkeit „Angelegenheiten“ ist außerdem sehr weitgehend und geht weit über den verfassungsrechtlich geforderten Schutz hinaus. Es obliegt dem Gesetzgeber Normierungen hinreichend bestimmbar zu formulieren sowie der Wesentlichkeitstheorie umfassend Rechnung zu tragen. Um Auslegungsschwierigkeiten von vornherein zu begegnen, wird eine Präzisierung angeregt.

Aus Sicht des LfDI BW sollte weiterhin mit der derzeitigen Terminologie des LIFG gearbeitet werden.

Auch in diesem Zusammenhang sollte eine Klarstellung zur Erforderlichkeit eines Drittbeziehungsverfahrens gesetzlich erfolgen. Hierzu verweisen wir auf die Ausführungen, die wir unter § 2 Absatz 3 Nr. 5 LIFG-E (Forschung) dargelegt haben.

Für etwaige Rückfragen oder Erörterungen stehen wir selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

gez. Prof. Dr. Tobias Keber

Anlage:

Stellungnahme des LfDI zum Entwurf des Gesetzes zur Änderung des Landeskrankenhausgesetzes Baden-Württemberg (LKHG-E) für die Weitergabe personenbezogener Daten zur medizinischen, rehabilitativen und pflegerischen Forschung vom 02.06.2025 – Az.: LfDIAbt3-0554.9-269/2