Anwaltsverband Baden-Württemberg
im Deutschen **Anwalt**Verein e. V.

Anwaltsverband BW – Postfach 1221 – 70808 Korntal-Münchingen

Ministerium des Inneren, für Digitalisierung und Kommunen
Baden-Württemberg
- Abteilung 2 -

Frau Susanne Wührl
Herrn Volker Jochimsen
Willy-Brandt-Straße 41
70173 Stuttgart

Geschäftsstelle beim Präsidenten:
RA Prof. Dr. Peter Kothe
Johannes-Daur-Straße 10
70825 Korntal-Münchingen

Telefon 0711 / 2 36 59 63
Telefax 0711 / 2 55 26 55

E-Mail: sekretariat@av-bw.de
Internet: www.av-bw.de

Anschrift der Geschäftsführung:
Kathrin Eisenmann – Syndikusrechtsanwältin
Kissinger Straße 49
70372 Stuttgart

Telefon 0711 / 55 04 29 29
Telefax 0711 / 55 04 29 30
E-Mail: geschaeftsfuehrung@av-bw.de

20. Oktober 2025

Per E-Mail an: Susanne.Wuehrl@im.bwl.de; poststelle@im.bwl.de

Geschäftszeichen: IM2-0557-54/8/1
Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes u. a. Gesetze
- **Stellungnahme des Anwaltsverbandes Baden Württemberg im DAV e. V. zum Anhörungsentwurf vom 23. September 2025**

Sehr geehrte Frau Wührl,
sehr geehrter Herr Jochimsen,

für die Übermittlung der Anhörungsunterlagen zum Entwurf eines Gesetzes zur Änderung des Landesdatenschutzgesetzes u. a. Gesetze mit Schreiben vom 23. September 2025 danken wir Ihnen. Der Anwaltsverband BW nimmt die Gelegenheit zur Stellungnahme gern wahr.

Der Anwaltsverband Baden-Württemberg e. V. ist der Zusammenschluss der 25 örtlichen Anwaltvereine in Baden-Württemberg, die Mitglieder im Deutschen Anwaltverein (DAV) sind. Er repräsentiert damit ca. 7.300 der Kolleginnen und Kollegen in Baden-Württemberg und vertritt so als größte freiwillige Anwaltsorganisation dieses Bundeslandes die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem DAV – auch auf nationaler und internationaler Ebene.

I. Allgemeine Bewertung

1. Geändert werden sollen neben dem **Landesdatenschutzgesetz** von 2018 - (u .a. Änderungen beim Einsatz von KI, Öffentlichkeitsarbeit und Forschung, Auftragsdatenverarbeitung und automatisierte Abrufverfahren, Zulassung von Videoüberwachung für sicherheitsrelevante Einrichtungen und Gegenstände, Dienstgebäude, Kulturgüter und Verkehrsmittel) auch
   - das **E-Government-Gesetz** BW (Erprobung und Einführung des automatisierten Erlasses von Verwaltungsakten einschließlich der Nutzung von KI),
   - das **Gesetz zur Ausführung des Personenstandsgesetzes** (automatisierter Abruf der in den elektronischen Sammelakten gespeicherten personenbezogenen Daten für die Fachaufsicht der Standesämter),
   - das **Landesinformationsfreiheitsgesetz** (Änderung von Bereichsausnahmen wegen Rechtsprechung des VGH BW, wie **VGH BW, Urteil vom 25.10.2023, Az. 10 S 125/22** (zu Anzeigen über Tierversuche bei einer Tierschutzbehörde im Rahmen von Aus-, Fort- und Weiterbildungsveranstaltungen im Bereich Humanmedizin) **und VGH BW, Urteil vom 8.11.2023, Az. 10 S 916/22** (zum Zugang zu beim Ministerium für Kultus, Jugend und Sport Baden-Württemberg vorhandenen Informationen über Religionsgemeinschaften), Regelungen zum Schutz der Kunst- und Wissenschaftsfreiheit sowie des religionsgemeinschaftlichen Selbstbestimmungsrechts),
   - das **Landesmediengesetz** und
   - die **Verordnung der Landesregierung** über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten an den Fünften Medienstaatsvertrag.

   Der Anwaltsverband BW begrüßt, dass mit dem vorliegenden Gesetzentwurf eine Anpassung der Rechtslage im LDSG BW an den **Evaluierungsbericht vom 08.10.2024 (Lt-Drs. 17/7596**) erfolgen soll.

2. Mit dem Landesdatenschutzgesetz vom 12.06.2018 hatte der Landesgesetzgeber das allgemeine Datenschutzrecht an die seit dem 25.05.2018 geltende **Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung**, im folgenden **DSGVO)** angepasst. Da die DSGVO unmittelbar geltendes Recht darstellt, hatte der Landesgesetzgeber nur die Befugnis zu eigenen Regelungen, soweit die DSGVO hierfür Öffnungsklauseln oder Regelungsaufträge enthält. Die ergänzenden Regelungen sollten der **öffentlichen Verwaltung** und anderen öffentlichen Stellen ausreichenden Spielraum für die Erfüllung ihrer Aufgaben im öffentlichen Interesse geben und dabei die schutzwürdigen Interessen der betroffenen Personen wahren.

3. Da das LDSG nur das Datenschutzrecht der öffentlichen Stellen normiert, wurde die **Wirtschaft nicht** an der Evaluierung in 2024 **beteiligt**. Das ist in Zeiten, in denen allseits und insbesondere von den Unternehmen, **Bürokratieabbau** gefordert wird, erstaunlich, da die Wirtschaft von Datenschutzregelungen der öffentlichen Verwaltung stark betroffen sein kann, z. B. auch im Hinblick auf die Entwicklung innovativer Produkte.

Im Rahmen der Überprüfung der **Forschungsregelung in § 13 LDSG** fanden die Anliegen des „Forums Gesundheitsstandort Baden-Württemberg“ einschließlich deren Sprechern Eingang in die Evaluierung.

Wenn es, wie jetzt geplant, aber darum gehen soll, Verbesserungen vorzuschlagen, die die retrospektive Nutzung personenbezogener Daten, das heißt die Weiterverarbeitung bestehender Datensätze für die Forschung, unterstützen sollen, etwa durch **Kooperationen mit der Privatwirtschaft**, verwundert die Nichtbeteiligung der Wirtschaft, insbesondere der Datenwirtschaft, umso mehr.

4. Die Grundsätze der DSGVO lauten:
Grundsatz der Rechtmäßigkeit (Konkretisierung in Artikel 6 Absatz 1 DSGVO),

- **Transparenzprinzip** (Konkretisierung in Artikel 7 Absatz 2, Artikel 12 bis 15, 34 DSGVO),
- Zweckbindungsgrundsatz (Konkretisierung in Artikel 6 Absatz 4 DSGVO),
- **Grundsatz der Datenminimierung** (Konkretisierung in Artikel 25 DSGVO: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen),
- Grundsatz der Richtigkeit (Konkretisierung in Artikel 16, 19 DSGVO),
- Grundsatz der Speicherbegrenzung (Konkretisierung in Artikel 17, 18 DSGVO),
- Grundsatz der Integrität und Vertraulichkeit (Konkretisierung in Artikel 32 DSGVO: Sicherheit der Verarbeitung).

Schließlich ist als allen genannten Grundsätzen übergeordnet der **Grundsatz der Erforderlichkeit** zu nennen. Dieser folgt aus dem in Artikel 8 GRCh garantierten Recht des Einzelnen auf den Schutz seiner personenbezogenen Daten und der Tragweite der garantierten Rechte gemäß Artikel 52 GRCh. Jede Verarbeitung personenbezogener Daten setzt daher die Prüfung voraus, ob es dieses Personenbezugs überhaupt bedarf.

Bereichsspezifisches Datenschutzrecht findet sich u. a. in Rechtsgebieten, die vom sachlichen Anwendungsbereich der DSGVO und dementsprechend, wie in § 2 Absatz 1 und 5 LDSG normiert, vom Anwendungsbereich des LDSG ausgenommen sind.

Dies betrifft in erster Linie den **Verfassungsschutz** sowie den Vollzug des Landessicherheitsüberprüfungsgesetzes.

Auch im **Bereich der Justiz** ist das LDSG größtenteils nicht anwendbar. Es bestehen spezielle Vorschriften für die **justizielle Tätigkeit** in den jeweiligen Prozessordnungen oder **im LDSG für Justiz- und Bußgeldbehörden (LDSG-JB)**. Gemäß § 2 Absatz 5 LDSG gilt das LDSG für die Gerichte nur für die Tätigkeit in Verwaltungsangelegenheiten.

Der **Datenschutz für die Polizei** ist in Umsetzung der **Richtlinie (EU) 2016/680 im Polizeigesetz (PolG)** und ggf. in der Strafprozessordnung geregelt, soweit die Datenverarbeitung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit dient.

Das LDSG subsumiert auch in Bezug auf den **Landtag** nur dessen Verwaltungstätigkeit unter den Anwendungsbereich. Ob die zugrundliegende Annahme, dass die DSGVO die parlamentarische Tätigkeit des Landtags nicht erfasst, zutreffend ist, bedarf infolge neuerer Rechtsprechung der Überprüfung.

Für die Verfolgung und Ahndung von Straftaten und Ordnungswidrigkeiten findet ebenfalls das LDSG keine Anwendung. Hier gilt das **LDSG-JB** sowie die vorrangigen bundesrechtlichen Vorschriften der Strafprozessordnung (StPO) und des Gesetzes über Ordnungswidrigkeiten.

5. Vor diesem Hintergrund verwundert es, dass in **§ 2 Absatz 5 LDSG BW – neu** plötzlich Regelungen zum Einsatz von KI im justiziellen Bereich getroffen werden sollen. Nach dem Verständnis des Anwaltsverbands BW müssten derartige Regelungen eher in die bundesrechtlichen Prozessordnungen oder ins LDSG-JB.

   Für den Bürger wird es so schwer auffindbar, wo welche Regelungen bezüglich dieser Materie zu finden sind. Das neue LDSG BW sollte aber den Anspruch haben, transparent und allgemein verständlich zu sein. Das scheint mit dem Ansinnen der Aufnahme von KI-Einsatz-Regelungen für den justiziellen Bereich nicht zu gelingen.

   Laut dem **Evaluationsbericht der Landesregierung zum Landesdatenschutzgesetz vom 8.10.2024 (Lt-Drs. 17/7596)**, Seite 23 und 29, habe das Justizministerium mitgeteilt, dass im Bereich der Justiz die **Erfahrung mit dem LDSG gering sei, da dieses dort überwiegend nicht anwendbar** sei. Wesentlich sei dort die Abgrenzung zwischen Verwaltungstätigkeit und justiziellen Tätigkeiten zu leisten. Diese bereite in der Regel keine Schwierigkeiten.

   Es erstaunt deswegen nun umso mehr, dass Regelungen für den justiziellen Bereich in das neue LDSG aufgenommen werden sollen, gerade für den datenschutzrechtlich und prozessrechtlich hoch sensiblen Bereich des Einsatzes von KI bzw. deren Training.

6. Generell meint der Anwaltsverband BW zur Verständlichkeit des Gesetzentwurfs, dass es für den Bürger schon sehr hilfreich wäre, den Text mit Seitenzahlen zu versehen, die für die Stichworte relevanten Paragrafen und die für die Änderung des LIFG zugrunde gelegten Gerichtsentscheidungen ins Vorblatt aufzunehmen. So ist es für den Leser sehr mühsam, sich die Tragweite der geplanten rechtlichen Änderungen zu erschließen. Gerade angesichts der Kürze der Anhörungsfrist wäre dies auch ein Gebot der Fairness. So wird der Eindruck erweckt als wolle man die zu Beteiligenden gar nicht erst richtig zu Wort kommen lassen.

7. Soweit in der Gesetzesbegründung behauptet wird, dass der Einsatz von KI in der Verwaltung vielfältige Möglichkeiten der **Effizienzsteigerung** biete, ist zu sehen, dass die Entwicklung von KI und die Erfahrungen damit noch recht am Anfang stehen und **fehlerhafte Ergebnisse geradezu an der Tagesordnung** sind. Im Moment handelt es sich z. B. bei Chatbots um Maschinen zur Erzeugung und zum Verstehen von Texten und Bildern, die Maschinen haben aber keine Konzepte und keine Vorstellungen von der Wirklichkeit. Derzeit besteht deswegen **noch ein erheblicher Schulungs-, Kontroll- und Nacharbeitsbedarf**, der eher Kräfte bindet als freisetzt. Die erfolgreiche Implementierung von KI erfordert Wissen und Expertise. Mitarbeiterinnen und Mitarbeiter sind der Schlüssel zum Erfolg jeder KI-gestützten Verwaltung.

KI-Systeme sind leistungsfähig, aber oft auch **ressourcenintensiv**. Sie benötigen große Rechenkapazitäten und können einen erheblichen Energieverbrauch verursachen. Die technische Ausstattung in den deutschen Verwaltungsstellen ist oft sehr unterschiedlich. Entscheidend ist, dass die Verwaltungen die Technologie nicht nur einsetzen, sondern auch nachhaltig und praxisorientiert gestalten. D.h. ganz so kostengünstig, wie es der Gesetzentwurf den Eindruck zu erwecken versucht, wird die Einführung von KI-gestützten Anwendungen nicht.

II. Im Einzelnen

1. Zu Art. 1 – Änderung des Landesdatenschutzgesetzes

a) Zu § 2 Absatz 5 LDSG BW – neu -Geltungsbereich – Verwaltungsangelegenheiten – Datenverarbeitung mittels KI - <u>Einsatz von KI im justiziellen Bereich von Gerichten</u>

Wie eingangs schon erwähnt, ist der Anwaltsverband BW über die Regelung der Datenverarbeitung im justiziellen Bereich mittels KI im LDSG BW verwundert.

Erst in der speziellen Gesetzesbegründung wird darauf hingewiesen, dass bestimmte Aspekte des Datenschutzes bei justizieller Tätigkeit in den (bundesrechtlichen) Prozessordnungen geregelt sind, z. B. in § 299 Zivilprozessordnung (ZPO) für die Aktenauskunft. In den Prozessordnungen würde es bisher an Regelungen zum Einsatz von KI fehlen.

Damit stellt sich die Frage, ob der Einsatz von KI im justiziellen Bereich deswegen nicht auch vom Bundestag entschieden werden sollte. Immerhin wären beim Einsatz von KI die Rechte der Verfahrensbeteiligten u. U. enorm betroffen.

Die Begründung des Gesetzentwurfs geht davon aus, dass sich Gesetzgebungskompetenz des Landes für die vorliegende Gesetzesänderung aus Artikel 70, 72 Absatz 1 GG ergäbe und verweist

auf das Datenschutzrecht als Querschnittsmaterie. Im Bereich der dem Bund nach Art. 74 Abs. 1 Nr. 1 GG (gerichtliches Verfahren) zustehenden konkurrierenden Gesetzgebungsbefugnis habe er von dieser keinen abschließenden Gebrauch gemacht.

Dies erscheint zweifelhaft, insbesondere dürfte die Verengung der Argumentation auf das Datenschutzrecht verfehlt sein, denn der Bund macht von seiner Gesetzgebungskompetenz Gebrauch, wenn ein Bundesgesetz eine bestimmte Frage hinreichend erkennbar geregelt hat oder wenn dem Gesetz durch „Gesamtwürdigung des betreffenden Normenbereiches“ zu entnehmen ist, dass es eine erschöpfende oder abschließende Regelung einer bestimmten Materie darstellt ,

> vgl. BVerfGE 109, 190/229; 113, 348/371 f; 157, 223 Rdnr.89.

Neben konkreten Einzelregelungen ist dabei auf die Gesamtkonzeption abzustellen,

> vgl. BVerfGE 102, 99/121; 138, 261 Rn.44; 157, 223 Rdnr.92.

Der Bundesgesetzgeber muss sich für eine bestimmte inhaltliche Konzeption entscheiden und diese verbindlich verankern. Ein Gebrauchmachen muss auch nicht ausdrücklich erfolgen, sondern kann auch negativ (BVerfGE 138, 261 Rn.43; 163, 1 Rdnr.27) – insb. durch „absichtsvollen Regelungsverzicht“ (BVerfGE 98, 265/300; 138, 261 Rn.43; BVerwGE 174, 322 Rdnr.19), „absichtsvolles Unterlassen“ (BVerfGE 113, 348/369) oder „beredtes Schweigen“ (BVerwGE 109, 272/283) – geschehen. Entscheidend ist stets der Inhalt des erlassenen Gesetzes, der ggf. auszulegen ist.

> „Ob die bundesgesetzliche Regelung abschließend ist, ist materien- und nicht zielbezogen zu bestimmen, so dass es […] allein auf die Identität der Regelungsmaterien ankommt.“
>
> BVerfGE 157, 223 Rdnr.92.

> „Führt der Vollzug einer landesrechtlichen Bestimmung dazu, dass die bundesrechtliche Regelung nicht mehr oder nicht mehr vollständig oder nur noch verändert angewandt werden kann, ist dies als Indiz für eine Sperrwirkung […] anzusehen.“
>
> BVerfGE 161, 63 Rdnr.82; 163, 1 Rdnr.27.

Gerade die in der Gesetzesbegründung genannten Beispiele legen nahe, dass der Vollzug der bundesrechtlichen Prozessrechtsnorm künftig anders zu handhaben sein sollte als bisher. Dies wiederum spricht für eine Sperrwirkung der einschlägigen Vorschriften der verschiedenen Prozessordnungen, weshalb dem Landesgesetzgeber insoweit die Gesetzgebungskompetenz fehlen dürfte.

Unabhängig von den zuvor dargestellten kompetenzrechtlichen Bedenken ist zu berücksichtigen, dass künstliche Intelligenz in der öffentlichen Verwaltung zwar viele Möglichkeiten eröffnet, zugleich aber auch große Verantwortung mit sich bringt. Der von der Europäischen Union verabschiedete **AI Act (KI-VO)** bildet die Grundlage für den rechtlichen Umgang mit KI. Er verfolgt einen risikobasierten Ansatz, der KI-Systeme nach ihrem Gefährdungspotenzial für Bürgerinnen und Bürger klassifiziert.

Die Justiz arbeitet oft mit personenbezogenen oder besonders schützenswerten Daten, etwa im Medizinrecht oder Familienrecht. Solche Anwendungen fallen fast immer in die **Kategorie der Hochrisiko-KI-Systeme**. Hier müssen Maßnahmen, wie Datenschutz, Informationssicherheit und Qualitätssicherung, oberste Priorität haben. **Unzureichende Anonymisierung** oder **unsichere Systeme** können gravierende Folgen haben. Für den erfolgreichen und sicheren Einsatz von KI-Systemen in der Verwaltung sind verbindliche Standards unerlässlich. Einheitliche hochwertige regelmäßige **Zertifizierungen** können dafür sorgen, dass die Qualität der Systeme überprüfbar ist. Durch Verschlüsselung, Anonymisierung und strenge Kontrollmechanismen kann KI sicher eingesetzt werden. Gleichzeitig sollte kontinuierlich an neuen Standards gearbeitet werden, die den Schutz weiter erhöhen.

Ein Richter muss das Ergebnis einer Software inhaltlich voll nachvollziehen und sich bewusst zu eigen machen, um es in der Entscheidungsbegründung verwenden zu können. Die Ergebnisse von mehrschichtigen „Black-Box"-Systemen können nicht vollständig nachvollzogen werden. Sie dürfen somit nicht Grundlagen von vorbereitenden oder Endentscheidungen von Richtern sein.

Im Grundlagenpapier von 2022 (74. Tagung der OLG-Präsidenten der ordentlichen Gerichtsbarkeit) wird eindeutig klargestellt, dass der Einsatz eines algorithmischen Systems anstelle eines Richters als natürliche Person zur abschließenden Entscheidungsfindung unzulässig ist. Dies ergebe sich aus **Art. 92 Hs. 1 GG** „Ausübung der rechtsprechenden Gewalt durch Richter". Aus dessen personalen Element folgt, dass die Entscheidung durch einen menschlichen Richter unmittelbar getroffen und verantwortet werden muss. Dies ergibt sich einfachgesetzlich z. B. aus §§ 1, 2, 5, 5a ff, 9 Nr. 4, 25 f., 27 Abs. 1, 38 Abs. 1 **DRiG** oder § 348 Abs. 1 S. 1 **ZPO**. Aus seinem institutionellen Element ergibt sich, dass die Rechtsprechung als öffentliche Aufgabe in öffentlicher Hand liegen muss. Privatwirtschaftliche Unternehmen, die KI und algorithmische Systeme entwickeln, dürfen hierdurch nicht in die Kernbereiche der rechtsprechenden Gewalt einwirken.

Aus dem **Recht auf den gesetzlichen Richter aus Art. 101 Abs. 1 S. 2 GG** ergibt sich, dass keine Richter, die nicht den Anforderungen des Art. 92 GG genügen, zu einer gerichtlichen Entscheidung berufen werden dürfen. Der Einsatz eines algorithmischen Systems würde somit auch gegen Art. 101 Abs. 1 S. 2 GG verstoßen.

Aus **Art. 103 GG** ergibt sich das Recht der Parteien auf **rechtliches Gehör**. Bei einer Vollautomatisierung des Verfahrens wäre dieses nicht gewährt, so dass sie auch gemäß Art. 103 GG ausscheidet.

Neben dem Recht auf rechtliches Gehör folgt auch aus dem **Recht auf ein faires Verfahren**, das aus **Art. 1 Abs. 1 GG bzw. Art. 1 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG und dem Rechtsstaatsprinzip des Art. 20 Abs. 3 bzw. aus Art. 6 EMRK** hergeleitet wird, dass die Einzelperson nicht nur Objekt des Verfahrens sein darf. Auch dies schließt den Einsatz eines algorithmischen Systems als Richter aus.

Auch wenn die vorstehend genannten Vorschriften teilweise nicht für die Tätigkeit der **Rechtspfleger** gelten, wird in dem Grundlagenpapier von 2022 mehrfach klargestellt, dass jedenfalls ihr Rechtsgedanke Anwendung findet und eine Vollautomatisierung der Rechtspflegertätigkeit ebenfalls ausgeschlossen ist.

Ein weiterer wichtiger Aspekt ist die **richterliche Unabhängigkeit**. Wie soll sie gewährleistet werden, wenn der Richter von KI „vorbereitete“ Akten bekommt, bei denen er die Fähigkeiten und Funktionsweise der eingesetzten KI möglicherweise nicht nachvollziehen kann? Aus diesem Grund müssen Richter umfangreich in der Funktionsweise der KI geschult werden. Spiegelbildlich erfordert dies wegen des Gebots eines fairen Verfahrens, dass den Parteien und deren Bevollmächtigten diese Funktionsweisen ebenfalls in für sie verständlicher Weise vermittelt werden.

Im Grundlagenpapier der OLG-Präsidenten von 2022 wird darauf hingewiesen, dass es dem Gesetzgeber freistünde, Randbereiche aus dem richterlichen oder rechtspflegerischen Aufgabenbereich auszunehmen und hierdurch ihre Vollautomatisierung zu ermöglichen.

Wegen der kompetenzrechtlichen Bedenken und der grundlegenden Bedeutung der Justizgrundrechte spricht sich der Anwaltsverband BW dagegen aus, den Einsatz von KI im justiziellen Bereich im LDSG BW zu regeln. Die etwaige Zulässigkeit des KI-Einsatzes sollte in den bundesrechtlichen Prozessordnungen erfolgen (die möglicherweise Öffnungsklauseln für die Länder vorsehen könnten).

Anders als die hiesige Gesetzesbegründung den Eindruck zu erwecken versucht, geht es **vorrangig nicht** um **Datenschutzrecht, sondern** um das **Recht auf ein faires rechtsstaatliches Verfahren.** Der Sachzusammenhang besteht doch vielmehr zu den Prozessordnungen als zum Datenschutzrecht.

Aus Sicht des Anwaltsverbandes BW kann es nicht erstrebenswert sein, zukünftig möglicherweise 16 unterschiedliche Landesregelungen zu haben, inwieweit KI zur Bewältigung der bei der Justiz eingehenden Fälle eingesetzt werden kann. Sinn und Zweck der obersten Bundesgerichte ist es, für eine bundesweit möglichst einheitliche Rechtsprechung zu sorgen. Bereits jetzt ist man schon zur Erkenntnis gelangt, dass eine bundeseinheitliche Justizcloud zukunftsfähiger wäre als der derzeitige „Flickenteppich" im elektronischen Rechtsverkehr.

Zu beachten ist auch der Grundsatz der Gewaltenteilung. Der Einsatz von KI in der Verwaltung ist eben nicht das Gleiche wie der Einsatz von KI in der justiziellen Justiz.

Im Grundlagenpapier von 2022 (74. Tagung der OLG-Präsidenten der ordentlichen Gerichtsbarkeit) findet sich eine Übersicht über laufende und geplante Projekte zum Einsatz von KI und algorithmischen Systemen in der deutschen Justiz. So werden z. B. Projekte

- zur effizienteren Bearbeitung von Massenverfahren (z. B. Diesel-Verfahren, Fluggastrechte, OLGA),
- ein Projekt zur automatischen Anonymisierung von Gerichtsentscheidungen (JANO),
- ein Projekt zur Metadaten-Extraktion (Bezeichnung des Gerichts, Bezeichnung der Parteien oder Verfahrensbeteiligten, Verfahrensgegenstand sowie Aktenzeichen und die aktenführende Stelle)
- ein Projekt zur Entwicklung eines Chatbots für die Rechtsantragstelle und
- ein Projekt zur Schaffung digitaler Klagewege

dargestellt. Zudem werden potenzielle weitere Einsatzfelder vorgestellt und bewertet, ob entsprechende Projekte wünschenswert sind.

Beispielsweise könnte die Prüfung und **Bewilligung von Beratungshilfe und PKH** weitgehend KI-gestützt erfolgen. Viel Potenzial hat auch der Einsatz algorithmischer Expertensysteme in allen Bereichen, in denen kein Bewertungs- oder Ermessensspielraum besteht, sondern eine bestimmte Entscheidung folgt, wenn bestimmte Voraussetzungen gegeben sind. Das könnte etwa der Fall bei **Vorprüfungen im Grundbuch- und Registerrecht**, der **Kostenfestsetzung** in Standardfällen und **dem Erlass von Pfändungs- und Überweisungsbeschlüssen** sein.

Die Zahl der KI-Projekte in der deutschen Justiz hat in den letzten Jahren zugenommen, so wird mittlerweile an vielen Gerichten mit Verfahren des maschinellen Lernens experimentiert, um v. a. bei Routineaufgaben zu unterstützen. Gleichzeitig ist festzustellen, dass die Projekte, die sich bewährt haben, durch entsprechende Ausschreibungen noch stärker in die Fläche kommen (siehe etwa FRAUKE in Frankfurt/M. oder Codefy in Hechingen). Des Weiteren geraten Large Language Models (LLms) stärker in den Blick. Ihr Einsatz wird u. a. erprobt, um maschinelle Lernverfahren

einfacher und weniger domänenspezifisch zu gestalten (z. B. im Projekt MAKI). Darüber hinaus soll ein auf die Justizbedürfnisse speziell zugeschnittenes Sprachmodell entwickelt werden.

Um die verschiedenen Projekte stärker zu vernetzen, sollte es 2025 zur „KI-Strategie der Justiz" kommen. Für 2026 ist eine gemeinsame „KI-Plattform" geplant, über die Anwendungen länderübergreifend ausgetauscht und eingesetzt werden können.

Derzeit ist es nicht einfach, den jeweiligen Stand der verschiedenen Vorhaben festzustellen. Man hat zudem den Eindruck, dass einige Projekte ineinander übergehen, ohne dass dies besonders kenntlich gemacht wird. Eine wissenschaftliche Begleitung bzw. Evaluierung, insbesondere unter deutlich stärkerer Anwaltsbeteiligung, wäre wünschenswert. Zu hoffen ist, dass eine gemeinsame „KI-Strategie" sowie eine entsprechende „KI-Plattform" zu **mehr Transparenz** hinsichtlich der verschiedenen Projekte beitragen.

b) Zu § 3 LDSG BW – neu – erforderliche technisch organisatorische Maßnahmen

Die Sicherstellung des Datenschutzes durch technische und organisatorische Maßnahmen (toMs) ist zentral für alle Datenverarbeitungen.

Insbesondere die Ergänzung um die Abschottung interner Systeme vor unbefugten Zugriffen aus öffentlichen Telekommunikationsnetzen durch Firewalls oder Segmentierung wird für sinnvoll gehalten.

c) Zu § 3a LDSG BW – neu – Nutzung von KI-Systemen

Die KI ist das Teilgebiet der Informatik, welches sich mit der Automatisierung intelligenten Verhaltens und dem maschinellen Lernen befasst.

Ein **KI-Modell** ist ein Computerprogramm, das auf Basis von KI-Algorithmen menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität imitieren kann. Insbesondere gibt es KI-Modelle, die nach einer Trainingsphase in der Lage sind, Muster in Datensätzen zu erkennen oder auf Basis von Eingabedaten Entscheidungen zu treffen. **KI-Modelle sind in der Regel in KI-Systeme integriert** und bilden deren Kernkomponente.

KI-Systeme sind Software- und Hardwaresysteme, die KI nutzen, um aus erhaltenen Eingaben „rational" Ausgaben abzuleiten, die je nach Einsatzzweck z.B. als Vorhersagen, Inhalte,

Empfehlungen oder Entscheidungen interpretiert und in der physischen oder virtuellen Welt verwendet werden können. Den Kern eines KI-Systems bildet ein KI-Modell, das jedoch um weitere Systembestandteile – wie z.B. eine Nutzerschnittstelle oder eine zusätzliche Wissensdatenbank – ergänzt wird. KI-Systeme können mehr oder weniger autonom sein.

Die neue Regelung soll lauten:

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

Wie gesagt, birgt der Einsatz von KI nicht nur Chancen, wie mögliche Effektivitätsgewinne, sondern auch Herausforderungen. In rechtlicher Hinsicht kann Folgendes interessant werden:

- intransparente Entscheidungsprozesse (sog. „Black-Box-Problematik", Fehlen von Transparenz in den Algorithmen, Gefahr der Halluzination). Insbesondere kritisch sind KI-Entscheidungen mit Konsequenzen für natürliche Personen.
- Fehlentscheidungen durch fehlerhafte Daten und falsche Optimierung („Garbage-In-Garbage-Out")
- fehlerhafte, aber plausibel wirkende Ergebnisse (sog. „Halluzinationseffekt" bei generativer KI)
- voreingenommene KI-System und mangelnde Unabhängigkeit von fremden Interessen
- Eigentumsrechte an Algorithmen, Betriebssoftware, Schnittstellen, Trainingsdaten, Eingabe- oder Ausgabedaten, usw.

Die Vorgaben der DSGVO sind dabei technikneutral und schützen individuelle Rechte.

Die KI-VO stellt Konformitätsanforderungen und schützt insbesondere Allgemeingüter. Sie legt einheitliche Vorgaben für die Entwicklung und Nutzung von KI in der Europäischen Union fest und gilt in der EU unmittelbar.

Datenschutzrechtliche Kernfragen beim Einsatz von KI sind:

- Wer ist Verantwortlicher? (der Entwickler, Anbieter, Benutzer?)
  „Anbieter" ist eine natürliche oder juristische Person, die ein KI-System entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen in den Verkehr bringt;
  "Betreiber" ist eine natürliche oder juristische Person, die ein KI-System in eigener Verantwortung verwendet; Wichtig ist, dass der Betreiber die Verantwortung für die Verwendung übernimmt.
  Mit der neuen EU-KI-Verordnung sind ab Februar 2025 strenge Schulungspflichten und Verbote für KI-Anbieter und -Betreiber in Kraft getreten. Ab dem 2.2.2025 müssen

Anbieter und Betreiber von KI-Systemen gemäß Art. 4 KI-VO Maßnahmen ergreifen, die sicherstellen, dass „ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen“.

- Außerdem sind ab dem 2. 2.2025 einige KI-Praktiken ausdrücklich verboten.
- Welche Rechtsgrundlage gilt?
- Wie werden die Daten geschützt?
- Wie werden die Grundsätze der Datenverarbeitung gewahrt?
- Datenschutzfolgeabschätzung erforderlich?
- Betroffenenrechte?
  Z. B. Auskunftsrecht, Art. 15 DSGVO: Komplexität der Algorithmen, involvierte Logik (= u. a. Zwecke der Datenverarbeitung schwer/ unmöglich nachzuvollziehen) und Datenweitergaben nicht vollständig nachvollziehbar
  z. B. **Recht auf Löschung, § 17 DSGVO**: Daten sind nicht isolierbarer Bestandteil der KI, Daten sind für Trainingszwecke eingeflossen, Datenempfänger nicht „erreichbar“
- Wie sind Betroffene zu informieren?
- Erfolgt eine Drittlandübertragung?
- Welche Daten können eingespielt werden?

Nach Ansicht der baden-württembergischen Aufsichtsbehörde würden beispielsweise Large Language Models (LLMs) personenbezogene Daten (direkt) speichern. Auch eine mittelbare Identifizierung erscheint wahrscheinlich.

Der Anwaltsverband BW kann nicht erkennen, dass die vorgenannten Aspekte in § 3a LDSG BW – neu ausreichend berücksichtigt wurden.

d) Zu § 4 LDSG BW – neu – Herstellung synthetischer Daten und Anonymisierung

Anonymisierung ist eine zentrale Maßnahme des Datenschutzes. Der Bedarf an der Anonymisierung von Datenbeständen ist daher nicht nur bei der Entwicklung und dem Einsatz von KI-Systemen, sondern auch bei anderen Verarbeitungsvorgängen hoch. Da **Anonymisierung je nach der Art der Daten einen erheblichen Aufwand** bedeuten kann, gibt es verschiedene Ansätze zur Automatisierung. Dabei wird auch KI eingesetzt.

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare lebende (natürliche) Person beziehen. Dazu gehören auch verschiedene Teilinformationen, die

zusammen verwendet werden können, um eine bestimmte Person zu identifizieren, wie Kfz.-Kennzeichen oder Kreditkartennummern (**Psyeudonymisierung**).

Wenn keine Re-Identifikation möglich ist, sind Daten sind nicht mehr personenbezogen und die DSGVO wäre nicht anwendbar (**Anonymisierung**).

Synthetische Daten sind künstliche Daten, die in Eigenschaften und Struktur den Originaldaten stark ähnlich sind, selbst aber keine echten Datenpunkte enthalten. Zur Herstellung synthetischer Daten sind mehr Verarbeitungsschritte erforderlich als bei der Anonymisierung. Wo der Einsatz synthetischer Daten möglich ist, ist dies durch den **Grundsatz der Datensparsamkeit** grundsätzlich geboten. Allerdings können nicht für alle Einsatzzwecke brauchbare synthetische Daten erzeugt werden. Z.B. können Softwaretests zwar im Allgemeinen mit synthetischen Daten durchgeführt werden, jedoch können damit zumeist nicht alle Fehler erkannt werden, da im Echtbetrieb Sonderfälle vorkommen können, die nicht vorhersehbar sind und bei der Erzeugung der synthetischen Daten nicht berücksichtigt wurden.

Die DSGVO enthält keine Definition für pseudonyme Daten, aber für den Vorgang der Pseudonymisierung. Die DSGVO erläutert den Begriff der anonymen Daten nur in ihren Erwägungsgründen.

Nach überwiegender Ansicht ist der Vorgang der Anonymisierung als solcher eine **Verarbeitung** personenbezogener Daten. Dafür spricht, dass der Verarbeitungsbegriff in der DSGVO **weit definiert** ist und jeden Vorgang im Zusammenhang mit personenbezogenen Daten erfasst. Die Folge dieser Ansicht ist, dass die DSGVO auf die Anonymisierung Anwendung findet und alle Datenschutzgrundsätze zu beachten sind. Insbesondere bedarf es einer datenschutzrechtlichen Rechtfertigung, um eine Anonymisierung durchführen zu können, vgl. https://www.it-planungsrat.de

Als mögliche Rechtsgrundlage für eine Anonymisierung von Daten durch eine behördliche Einrichtung kommen – bei Vorliegen der jeweiligen Voraussetzungen – u.a.

- die Wahrnehmung öffentlicher Aufgaben,
- eine rechtliche Verpflichtung,
- eine Einwilligung oder
- die Anbahnung oder Erfüllung eines Vertrages

in Betracht. Hingegen steht die Rechtsgrundlage des berechtigten Interesses, die im nicht-öffentlichen Bereich eine große praktische Bedeutung hat, für die Anonymisierung durch öffentliche Stellen nicht zur Verfügung, vgl. https://www.it-planungsrat.de

Wenn bereits bei einer Behörde vorhandene Daten – z. B. aus einem Fachverfahren –anonymisiert werden, um sie einem anderen Zweck zuzuführen – wie dem Training einer neuen KI – handelt es

sich datenschutzrechtlich um einen Fall der **Zweckänderung**. Hierfür sind grundsätzlich weitere Voraussetzungen zu beachten.

Die rechtliche Systematik der Zweckänderung ist recht komplex und im Detail umstritten. Grundsätzlich gilt, dass eine Zweckänderung auf eine Einwilligung oder eine gesetzliche Erlaubnis gestützt werden kann. Ist das nicht der Fall, kann die Zweckabweichung nach der DSGVO zulässig sein, wenn der neue Zweck mit dem bisherigen Zweck kompatibel ist. Im Rahmen dieser Kompatibilitätsprüfung wird die Verbindung zwischen den Zwecken, der Zusammenhang zwischen Erhebung und Weiterverarbeitung, die Art der Daten und Verarbeitungsfolgen sowie **Garantien** (u.a. Verschlüsselung und Pseudonymisierung) betrachtet.

Umstritten ist, ob das Vorliegen dieser Voraussetzungen ausreicht, um die Zweckänderung zu rechtfertigen, oder ob zusätzlich eine Rechtsgrundlage erforderlich ist (diese Auslegung vertreten mehrheitlich die Aufsichtsbehörden). Die Frage bedarf aber dann keiner Entscheidung, wenn die Zweckänderung auf eine eigene gesetzliche Grundlage gestützt werden kann.

Für die Anonymisierung von personenbezogenen Daten und für die Herstellung synthetischer Daten soll eine Rechtsgrundlage geschaffen werden.

> *Öffentliche Stellen dürfen zum Zweck der Datenminimierung aus den rechtmäßig gespeicherten Daten synthetische Daten herstellen sowie rechtmäßig gespeicherte Daten auf sonstige Weise anonymisieren.*

Der Anwaltsverband BW würde aus den vorgenannten Gründen diese Regelung befürworten.

e) Zu § 5 LDSG BW – neu – Zweckänderung - Verfolgung von Straftaten – interessengerechte Weiterleitung

Laut dem Evaluierungsbericht (LDrs. 17/ 7596, S. 32) könnte eine Erweiterung der Zweckänderungstatbestände des § 5 LDSG zur Rechtssicherheit beitragen, sollte aber in maßvollem Rahmen bleiben. Vorgeschlagen werden insbesondere die Erweiterung zur Verfolgung von Ordnungswidrigkeiten sowie zur Verwendung von Kontaktdaten für die politische Arbeit.

Die **Zweckänderungstatbestände** des § 5 LDSG werden präzisiert und erweitert.

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

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

Die Ermöglichung von Zweckänderungen zugunsten des Betroffenen, etwa Antragsweiterleitungen an die zuständige Stelle, hält der Anwaltsverband BW für sinnvoll.

f) Zu § 6 LDSG BW – neu – Übermittlung personenbezogener Daten

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

Die gefundenen Regelungen hält der Anwaltsverband BW für sinnvoll.

g) Zu § 7a LDSG BW – neu – Auftragsverarbeitung – z. B. BITBW

Um Auftragsverarbeitung zu vereinheitlichen, wird eine gesetzliche Grundlage mit Rechtsverordnungsermächtigung eingeführt.

Laut dem Evaluierungsbericht (LT-Drucks. 17/7596) sollte für die Auftragsverarbeitung die Beauftragung durch die **Fachaufsichtsbehörde** zugelassen werden. Für die Erleichterung der Beauftragung könnten eine gesetzliche Grundlage oder standardisierte Vertragsbedingungen zur Verfügung gestellt werden.

Das erscheint sinnvoll.

h) Zu § 8 LDSG BW – neu – Information der betroffenen Person – Beschränkung

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

Selbstverständlich befürwortet der Anwaltsverband BW die Stärkung der Betroffenenrechte.

i) Zu § 9a LDSG BW – neu – Beschränkung des Berichtigungsrechts nach Art. 16 DSGVO

Die DSGVO hat in **Art. 23 DSGVO** und in **Art. 89 DSGVO** Öffnungsklauseln vorgesehen, die es ermöglichen, den Anspruch auf Berichtigung einzuschränken. Beschränkungen sollten als Ausnahme von der allgemeinen Regel betrachtet werden, wonach die Ausübung von Rechten möglich ist und die in der DSGVO verankerten Pflichten erfüllt werden müssen.2 Beschränkungen sollten daher eng ausgelegt werden; sie sollten nur unter bestimmten Umständen und nur dann Anwendung finden, wenn bestimmte Bedingungen erfüllt sind.

Selbst in Ausnahmesituationen kann der Schutz der personenbezogenen Daten nicht vollständig beschränkt werden. Er muss gemäß Artikel 23 DSGVO bei allen Notfallmaßnahmen eingehalten werden und trägt so zur Wahrung der übergeordneten Werte der Demokratie, der Rechtsstaatlichkeit und der Grundrechte bei, auf die sich die Union gründet: Bei allen von den Mitgliedstaaten ergriffenen Maßnahmen müssen die allgemeinen Rechtsgrundsätze und der Wesensgehalt der Grundrechte und Grundfreiheiten beachtet werden; sie dürfen nicht unumkehrbar sein, und die Verantwortlichen und die Auftragsverarbeiter müssen die Datenschutzvorschriften weiterhin einhalten.

In allen Fällen, in denen Beschränkungen der Rechte der betroffenen Personen oder der Pflichten der Verantwortlichen (einschließlich der gemeinsam Verantwortlichen) und der Auftragsverarbeiter nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig sind, ist zu beachten, dass der **Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DSGVO** weiterhin gilt. Das bedeutet, dass der Verantwortliche für die Einhaltung des Datenschutzrahmens der EU, einschließlich der Grundsätze für die Datenverarbeitung, zuständig ist und in der Lage sein muss, dies gegenüber den betroffenen Personen nachzuweisen.

Legt der EU-Gesetzgeber oder der nationale Gesetzgeber Beschränkungen auf der Grundlage von Artikel 23 DSGVO fest, so muss er sicherstellen, dass er die Anforderungen nach **Artikel 52 Absatz 1 der Charta** erfüllt. Er muss insbesondere eine Bewertung der Verhältnismäßigkeit durchführen, um sicherzustellen, dass die Beschränkung nicht über das notwendige Maß hinausgeht.

Der Begriff „Beschränkungen“ ist in der DSGVO nicht definiert. In Artikel 23 DSGVO und in Erwägungsgrund 73 DSGVO sind lediglich die Bedingungen aufgeführt, unter denen Beschränkungen vorgesehen werden können. Wie in Erwägungsgrund 73 DSGVO erwähnt, sollten die Beschränkungen zudem mit der Charta und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) im Einklang stehen.

In diesen Leitlinien bezeichnet der Begriff „Beschränkungen“ jede Beschränkung des Umfangs der in den Artikeln 12 bis 22 und 34 DSGVO vorgesehenen Pflichten und Rechte sowie der entsprechenden Bestimmungen von Artikel 5 in Übereinstimmung mit Artikel 23 DSGVO. Durch die Beschränkung eines individuellen Rechts müssen **wichtige Ziele** verfolgt werden, zum Beispiel der Schutz der Rechte und Freiheiten anderer oder wichtige Ziele von allgemeinem öffentlichem Interesse der Union oder eines Mitgliedstaats, die in Artikel 23 Absatz 1 DSGVO aufgelistet sind. Daher können die Rechte der betroffenen Personen nur dann beschränkt werden, wenn die aufgeführten Interessen auf dem Spiel stehen und mit diesen Beschränkungen das Ziel verfolgt wird, diese Interessen zu schützen.

Der Anwaltsverband BW kann nicht erkennen, dass solche Ziele mit der geplanten Beschränkung des Berichtigungsanspruchs verfolgt werden. Es scheint doch eher um Bequemlichkeit zu gehen.

Sollte sich der Einsatz von KI in öffentlichen Stellen ausweiten, hätten Bürger u.U. gar kein Recht mehr, den Berichtigungsanspruch durchzusetzen. Die neue Regelung soll lauten:

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

Für die Nutzung von KI kann die **Eingabe** von personenbezogenen Daten erforderlich sein und die **Ausgabe** der KI kann ebenfalls personenbezogene Daten enthalten.

Richtigerweise führt die Gesetzesbegründung aus, dass schon bei der Dateneingabe Fehler passieren können und die KI auch zu falschen Ergebnissen, z. B. Halluzinationen, kommen kann. Die fehlerhaften Ergebnisse können derzeit teilweise ganz beträchtlich sein und eine betroffene Person ganz erheblich in ihren Rechten verletzten. Hier kommt sowohl ein immaterieller Schaden in der Form der Verletzung des Schutzes personenbezogener Daten in Betracht als auch ein finanzieller Schaden, etwa durch eine ungünstigere Zuwendungsberechnung.

Soweit der Gesetzentwurf hier das wichtige Berichtigungsrecht nach Art. 16 DSGVO beschränken will, hat der Anwaltsverband BW dafür kein Verständnis. Wo bliebe der Anreiz für die öffentliche Verwaltung, sorgfältig zu arbeiten und nur hochwertige KI einzusetzen?

Pauschal zu sagen, das Gemeinwohlinteresse überwiege hier das Betroffenenrecht, ist nicht möglich. Die Gesetzesbegründung übersieht das Recht auf **Einschränkung der Verarbeitung nach Art. 18 DSGVO**. Der Verantwortliche muss die falschen Daten im Regelfall sperren und darf die Daten nicht weiterverarbeiten.

Ein mit den §§ 27 Abs. 2 und 28 Abs. 3 Bundesdatenschutzgesetz (BDSG) für Forschungs-, Statistik- und Archivzwecke vergleichbarer Fall liegt nicht vor. Danach kann ein Betroffener seinen Berichtigungsanspruch nicht geltend machen, wenn dadurch die zur Verarbeitung festgelegten Zwecke beeinträchtigt werden.

Hier geht es aber darum, dass gerade im Einzelfall des Betroffenen ein unrichtiges Ergebnis produziert wurde.
Die öffentlichen Stellen tragen die Verantwortung für die Entwicklung und den Einsatz der KI. Sie müssen im Sinne der Produktsicherheit (KI-VO) Vorsorge dafür treffen, dass fehlerhafte Eingaben nicht dauerhaft im KI-System verbleiben, am besten schon gar nicht hineingelangen können. Das ist eine schlichte Frage des „Produkt-Designs“ und der Mitarbeiter-Schulung.

In Artikel 23 Absatz 1 **Buchstabe e** DSGVO werden sonstige wichtige Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats genannt, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit.

Die Kosten, die durch die Bereitstellung von Informationen entstehen, und damit die finanzielle Belastung der öffentlichen Haushalte reichen jedoch nicht aus, um ein öffentliches Interesse an der Beschränkung der Rechte der betroffenen Personen zu rechtfertigen.

Soweit der Gesetzentwurf auf einen unverhältnismäßig hohen Aufwand abstellt, überzeugt dies nicht.

So hat etwa der **Bundesfinanzhof (BFH)** - zum Auskunftsanspruch nach Art. 15 DSGVO - in seinem Urteil vom 14.01.2025, Az. IX R 25/22, klargestellt, dass der nicht mit dem Argument des unverhältnismäßigen Aufwands verweigert werden darf. Auch der Gedanke des § 275 BGB finde keine Anwendung.

Diese Rechtsprechung kann auf die hiesige Konstellation übertragen werden. Das Recht der betroffenen Person auf Berichtigung hängt eng mit den Transparenzrechten, insbesondere mit dem Auskunftsrecht nach Art. 15 DS-GVO zusammen. Ohne das Recht auf Auskunft könnte der Betroffene von seinem Berichtigungsrecht nicht Gebrauch machen, denn er wüsste nicht von den falschen Informationen, die über ihn verarbeitet werden.

Wenn man also nach der obergerichtlichen Rechtsprechung schon nicht den Auskunftsanspruch wegen unverhältnismäßigen Aufwands beschränken kann, dann auch nicht den Berichtigungsanspruch.

Das Bundesverfassungsgericht besteht auf dem Grundsatz der Normenklarheit. Hier gibt nicht einmal die Gesetzesbegründung Anhaltspunkte dafür, wann so ein „unverhältnismäßig hoher Aufwand“ vorliegen soll.

Der Berichtigungsanspruch umfasst sämtliche Datenbestände, in denen die unrichtigen personenbezogenen Daten des Antragstellers gespeichert sind. Die Berichtigung der Daten ist unverzüglich durch eine entsprechende Maßnahme durchzuführen. Bezogen auf den Einzelfall, kann dies durch Veränderung, teilweise oder vollständige Löschung oder Speicherung ergänzender oder neu erhobener Daten erfolgen. Längstens ist der Antragsteller nach einer absoluten Frist von einem Monat über die Entscheidung bzw. Maßnahmen des Berichtigungsantrages zu informieren. Sofern die Frist unter Berücksichtigung der Komplexität des Antrags nicht eingehalten werden kann, ist eine Verlängerung um weitere zwei Monate möglich. Der Antragsteller ist unter Angaben von Gründen zu informieren.

Hat der Verantwortliche die gespeicherten personenbezogenen Daten des Antragstellers an Dritte übermittelt, müssen auch diese über die Berichtigung der Daten informiert werden, sofern dies vernünftigerweise möglich ist. Alle zur Berichtigung ergriffenen Maßnahmen, sind unentgeltlich zu erbringen.

Verstöße gegen Betroffenenrechte sind keine Kavaliersdelikte. Ein Verstoß gegen das Recht auf Berichtigung, kann mit Geldbußen entsprechend des Art. 83 Abs. 5 lit. b DS-GVO geahndet werden. Daneben steht der betroffenen Person ein Schadensersatzanspruch gemäß Art. 82 DS-GVO zu, soweit ihr durch die Verarbeitung sie betreffender unrichtiger Daten ein materieller oder immaterieller Schaden entstanden ist.

Die Aufsichtsbehörden sollten vor der Verabschiedung etwaiger Gesetzgebungsmaßnahmen zur Festlegung der Beschränkungen konsultiert werden und über die Befugnis verfügen, die Einhaltung der DSGVO durchzusetzen.

j) Zu § 10 LDSG BW – neu – Beschränkung des Löschungsanspruchs nach Art. 17 DSGVO

Hier gilt das zuvor Gesagte ebenfalls. Der Anwaltsverband kann eine ausreichende Rechtfertigung für die Beschränkung des Betroffenenrechts beim Einsatz von KI nicht erkennen, da es einer gänzlichen Abschaffung solcher Ansprüche gleichkommen würde.

k) Zu § 11a LDSG BW – neu – Entwicklung von KI-Systemen

Die neue Regelung soll lauten:

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

Für das erfolgreiche Training von KI sind große Datenmengen erforderlich. Das kann auch urheberrechtliche Fragen aufwerfen. Ohne ein Verständnis der verwendeten Technologie ist eine rechtliche Bewertung der Datenverarbeitung nicht möglich.

Der Begriff der „Verarbeitung" in der DSGVO ist weit auszulegen. Die in Art. 4 DSGVO konkret genannten Vorgänge, wie das Erheben, Speichern, Verändern oder Übermitteln, sind lediglich Beispiele.

Die Datenverarbeitung ist nach Art. 6 DSGVO rechtmäßig, wenn der Verantwortliche ein berechtigtes Interesse daran hat und die Interessen des Betroffenen nicht überwiegen.

Der Anwaltsverband BW vermisst hier eine Abwägung mit dem Aspekt, dass einmal in eine KI-Software eingegebene personenbezogene Daten möglicherweise nicht mehr extrahiert werden können, insbesondere, wenn sie fehlerhaft sind, ein Löschverlangen besteht oder es um mehrschichtige KI geht.

l) Zu § 12a LDSG BW – neu – parlamentarische Kontrolle

Die Verarbeitung zu Zwecken der parlamentarischen Kontrolle wird rechtlich gesondert legitimiert.

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

Diese Regelung erscheint angemessen.

m) Zu § 13 LDSG BW – neu – Forschungszwecke

Laut dem Evaluierungsbericht (LT-Drucks. 17/7596) genüge die Forschungsregelung des § 13 LDSG nicht den Anforderungen, die an die Forschung aus der Praxis gestellt werden. Soweit möglich, werden hier Verbesserungen vorgeschlagen. Die retrospektive Nutzung personenbezogener Daten, das heißt die Weiterverarbeitung bestehender Datensätze für die Forschung, sollte unterstützt werden ebenso Kooperationen mit der Privatwirtschaft ermöglicht werden. Auch für die Veröffentlichung von Forschungsergebnissen entsprechend der guten wissenschaftlichen Praxis sollte die Regelung im LDSG erweitert werden. Die Transparenz und damit das Vertrauen der Bürgerinnen und Bürger in die Datenwirtschaft könnten durch geeignete Maßnahmen wie **Anzeige- und Publikationspflichten** gestärkt werden.

In Bezug auf die Forschungsregelung (§ 13 LDSG) werden nun mehrere Änderungen vorgeschlagen, um die Bedingungen für die Forschung zu verbessern. Neben der **Anpassung an die Bundesregelung** wird die Sekundärnutzung von personenbezogenen Daten für Forschungszwecke, soweit im Rahmen des allgemeinen Datenschutzrechts möglich, unterstützt.

Die Kooperation mit der Privatwirtschaft und deren gemeinwohlorientierte Forschung wird ermöglicht.

Die nun gefundene Regelung erscheint sinnvoll.

n) Zu § 15 LDSG BW – neu – Dienstverhältnisse - Gesundheitsvorsorge – biometrische Daten – Bewerber

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

Zu Absatz 2 – neu:

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

Diese Regelung erscheint dem Anwaltsverband BW sinnvoll.

Zu Absatz 6 – neu:

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

Hier erscheint es zum Schutz der Beschäftigten als nicht ausreichend, dass die Verarbeitung biometrischer Daten in einer Vereinbarung der genannten Art geregelt ist. Entscheidend ist vielmehr, dass der Einsatz biometrischer Daten erforderlich ist, weil es kein anderes Schutzmittel gibt.

Dass eine solche Situation vorliegen könnte, erscheint utopisch. Warum sollte ein ausreichender Schutz nicht mit Zugangscodes möglich sein, die nur der berechtigte Beschäftigte kennt und ändern kann? Wenn aber ausnahmsweise tatsächlich die Erhebung und Verarbeitung biometrischer Daten erforderlich werden sollte, ist dies ausdrücklich zu begründen und dementsprechend zu regeln.

Richtig ist in der Gesetzesbegründung, dass sich aus Artikel 25 DSGVO in Verbindung mit § 3 LDSG ergibt, dass dem Schutzbedürfnis der Daten entsprechende technische und organisatorische Maßnahmen (toMs) zu treffen sind.

Zu Absatz 9 – neu

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

Selbstverständlich reicht es hier nicht aus, die Betroffenen (Beschäftigte und Bewerber) nur über den Einsatz von KI-Systemen, deren Dauer und Zweck zu unterrichten. Diese Personen müssen auch rechtzeitig im Vorfeld erfahren, um welche Produkte es sich handelt und wie sie funktionieren (**Transparenz**). Wie anders sollen die Betroffenen sonst wirksam ihre Einwilligung geben oder kontrollieren können, ob durch die KI-Systeme Rechtsverletzungen hervorgerufen wurden?

Oben wurde bereits ausgeführt, dass die Beschränkung von Berichtigungs- und Löschansprüchen beim Einsatz von KI für hoch bedenklich gehalten wird.

Viele Personalverantwortliche sind fasziniert von der Aussicht, Bewerbungsprozesse mittels KI effizienter und objektiver zu gestalten – etwa durch automatisiertes CV-Screening oder digitale Pre-Interviews.

Automatisierte Entscheidungen sind nach Art. 22 DSGVO grundsätzlich unzulässig, es sei denn, es gibt menschliche Kontrolle. Ein wegweisendes Urteil des Europäischen Gerichtshofs – das sogenannte **SCHUFA-Urteil vom 7.12.2023 (EuGH, Rs. C-634/21**) – hat die Reichweite von Art. 22 Abs. 1 DSGVO betont.

Transparenz über den Einsatz von KI in Bewerbungsprozessen ist gesetzlich gefordert und für Vertrauensbildung wichtig.

Das Allgemeine Gleichbehandlungsgesetz (AGG) schützt vor Diskriminierung; KI kann **ungewollte Bias** in Auswahlprozesse bringen. Bias ist eine tiefgreifende Problematik für Systeme der Künstlichen Intelligenz, die eine Gefährdung für den sicheren Einsatz von solchen Systemen darstellen kann. Der richtige Umgang mit Bias ist komplex und erfordert eine umfassende Beschäftigung mit der Thematik. Bias-Arten weisen eine hohe Diversität auf und können in unterschiedlichen Phasen des Lebenszyklus eines KI-Systems auftreten. Nach Möglichkeit müssen organisatorische und technische Maßnahmen bei der Datenerhebung etabliert werden, die potentiellen Bias in den Daten reduzieren.

Wichtige Stichworte sind hier auch **Zweckbindung** und **Speicherfristen** (max. 6 Monate für Bewerberdaten wegen AGG).

Datenschutz lebt von **Transparenz**. Bewerber haben ein Recht zu erfahren, ob und in welcher Form KI-Systeme im Auswahlprozess eingesetzt werden. Bereits beim Erheben der Daten – typischerweise, wenn der Bewerber seine Unterlagen einreicht – müssen Verantwortliche die Informationspflichten

nach **Art. 13 DSGVO** erfüllen. In dieser **Datenschutzerklärung** für Bewerber sollte ausdrücklich erwähnt werden, dass ein KI-basiertes System zur Unterstützung im Bewerbungsprozess genutzt wird. Wichtig ist, dass der Zweck klar benannt wird (z. B. „Durchführung des Bewerbungsverfahrens, einschließlich einer teil-automatisierten Auswertung der Bewerbungsunterlagen"), und dass die Bewerber über die wesentlichen Punkte aufgeklärt werden: Welche Daten werden verarbeitet? Wie lange werden sie gespeichert? An wen werden sie ggf. übermittelt (etwa an einen externen KI-Dienstleister)? Und vor allem: Wie funktioniert die KI-gestützte Auswertung grundsätzlich?

Die DSGVO verlangt in Art. 13 Abs. 2 lit. f, dass betroffene Personen bei Vorliegen automatisierter Entscheidungen im Sinne von Art. 22 Abs. 1 DSGVO über die involvierte Logik sowie die Tragweite und angestrebten Auswirkungen informiert werden. Konkret: Wenn tatsächlich eine automatisierte Entscheidung im Spiel wäre (etwa eine automatische Absage durch die KI), müsste man dem Bewerber zumindest in Grundzügen erläutern, **nach welchen Kriterien das System urteilt** und welche Bedeutung das für ihn hat.

So, wie ein angeblich einer Trunkenheitsfahrt oder Geschwindigkeitsübertretung Überführter das Recht hat, zu erfahren wie die Verstöße ermittelt/gemessen wurden, um mögliche technische Fehlerquellen, wie unzureichende Software-Updates, aufzeigen zu können, muss das erst recht beim Einsatz von KI gelten, deren Auswirkungen weit gravierender sein können.

Nach Datenschutzrecht kann ein Bewerber einen **Auskunftsanspruch nach Art. 15 DSGVO** geltend machen, um zu erfahren, welche Daten über ihn gespeichert wurden und ggf. ob ein Profiling stattgefunden hat. Spätestens dann muss man erklären können, wie das KI-System gearbeitet hat.

Ein weiterer Punkt ist die **Zweckbindung:** Bewerberdaten dürfen nur für das Verfahren genutzt werden, für das sie erhoben wurden, d. h. die konkrete Bewerbung auf eine konkrete Position. Wenn man sie einsetzt, um z. B. aus den Lebensläufen Erkenntnisse zu gewinnen, dürfen diese Daten nicht plötzlich für ganz andere Zwecke (KI-Training) verwendet werden. Insbesondere ist davon abzuraten, Bewerbungsdaten ungefragt zur Weiterentwicklung des KI-Modells zu benutzen.

Alternativ müsste man die Daten so anonymisieren, dass kein Personenbezug mehr besteht, bevor man sie ins Training speist.

o) Zu § 16 LDSG BW – neu – öffentliche Auszeichnung – Widerspruchsrecht

Die Vorschrift zu öffentlichen Auszeichnungen und Ehrungen wird in Bezug auf das Widerspruchsrecht klarstellend ergänzt. Das kann der Anwaltsverband BW nur befürworten.

p) Zu § 17 LDSG BW – neu - Verarbeitung besonderer Kategorien personenbezogener Daten im öffentlichen Interesse

Die Verarbeitung besonderer Kategorien personenbezogener Daten im öffentlichen Interesse wird im Hinblick auf die Zwecke konkretisiert einschließlich Garantien für die Freiheiten der betroffenen Personen.

Das Vorsehen von technischen und organisatorischen Maßnahmen zum Datenschutz wird vom Anwaltsverband BW ausdrücklich begrüßt.

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

> *(1) Für die Überprüfung der Zuverlässigkeit von Besuchern, Mitarbeitern von Unternehmen und anderen Organisationen sowie sonstigen Personen, die in sicherheits- oder sicherheitstechnisch relevante Bereiche gelangen sollen, für die öffentliche Stellen Verantwortung tragen, gilt § 15 Absatz 1 Satz 1 entsprechend mit der Maßgabe, dass zusätzlich die **Einwilligung** der betroffenen Person erforderlich ist. Besondere Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln dürfen nur aufgrund einer ausdrücklichen Einwilligung verarbeitet werden.*
>
> *(2) Öffentliche Stellen dürfen personenbezogene Daten von Dritten oder Auftragsverarbeitern, die Zugang zu sicherheits- oder sicherheitstechnisch relevanten Datenverarbeitungsanlagen oder -geräten haben, **verarbeiten,** sofern dies für die Durchführung von Maßnahmen, einschließlich Schulungs- und Sensibilisierungsmaßnahmen, zur Gewährleistung der Informationssicherheit, der Cybersicherheit oder des Funktionierens kritischer Infrastruktur **erforderlich** ist. Die Verarbeitung **biometrischer Daten** zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, dass die betroffene Person ausdrücklich zustimmt und kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung steht.*

Der Anwaltsverband BW begrüßt diese Neuregelungen.

r) Zu § 17b LDSG BW – neu – Öffentlichkeitsarbeit – politische Bildung – Bürgerinformation

Laut dem Evaluierungsbericht (LT-Drucks. 17/7596, Seite 31) sollte das LDSG über die Generalklausel hinaus differenzierte Regelungen für die Öffentlichkeitsarbeit der öffentlichen Stellen zur Verfügung stellen.

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

> *(1) Soweit der öffentlichen Stelle ein Auftrag zur politischen Bildung oder zur Bürgerinformation obliegt, dürfen öffentliche Stellen unbeschadet sonstiger Bestimmungen personenbezogene Daten verarbeiten, um die Bürgerinnen und Bürger in angemessener Weise über ihre Arbeit zu informieren einschließlich werblicher Zwecke, sofern die schutzwürdigen Interessen betroffener Personen dem nicht entgegenstehen. In der Regel sind hiernach im erforderlichen Umfang insbesondere die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen und deren Verbreitung, die Verwendung von Kontakt- und Adressdaten für Kontaktpflege und Einladungen zu Veranstaltungen einschließlich deren Organisation zulässig. Die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen und deren Verbreitung unterliegt den Schranken der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie.*
>
> *(2) Den betroffenen Personen ist Gelegenheit zum Widerspruch ohne Angabe von Gründen zu geben."*

Mit den in dieser Vorschrift vorgenommenen Einschränkungen erscheint sie sinnvoll. Nichtsdestotrotz kann der Anwaltsverband BW nur auf eine sehr restriktive Auslegung pochen, insbesondere beim „erforderlichen Umfang". Der vermeintliche Auftrag zur politischen Bildung oder Bürgerinformation sollte nicht für marketingähnliche Selbstdarstellung hochrangiger Funktionsträger missbraucht werden.

s) Zu § 18 LDSG BW – neu – offener Videoschutz – sicherheitsrelevanter Einrichtungen – KI-Systeme

Die Videoüberwachung öffentlich zugänglicher Räume durch Kommunen (für die Ortspolizei) wird als besonders eingriffsintensive Form der Datenverarbeitung gesondert geregelt. § 44 PolG BW dient der Gefahrenabwehr an Kriminalitätsschwerpunkten. Dies aber zeigt, dass es mehrere Rechtsgrundlagen für den Einsatz von Videotechnik im öffentlichen Raum geben kann, was dem normalen Bürger nicht ohne weiteres geläufig sein dürfte.

Die Vorschriften haben zu beachten, dass Videoüberwachung 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 und bedarf daher zum einen besonderer Rechtfertigung, zum anderen besonderer Verfahrensvorschriften zur Speicherung und Löschung der aufgezeichneten Daten.

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

Videoüberwachung kann für die Überwachung sensibler öffentlicher Räume, wie Eingangsbereichen von Dienstgebäuden, wichtig sein. Dabei ist die verfassungsrechtliche Vorgabe zu beachten, dass sich **Videoüberwachung auf das geringstmögliche Maß beschränken** muss. Für den Anwaltsverband BW steht die Voraussetzung der **Erforderlichkeit** nicht zur Disposition. Die Zwecke sind für jede einzelne Kamera gesondert zu dokumentieren. Eine Überwachung „ins Blaue“ oder unter Berufung auf nicht näher beschriebene „Sicherheitsgründe“ ist regelmäßig nicht ausreichend.

Nach Art. 6 Abs. 1 Buchst. f DSGVO ist eine Videoüberwachung zulässig, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Ein berechtigtes Interesse muss ein tatsächlich und gegenwärtig vorliegendes Interesse darstellen. Subjektive Befürchtungen oder ein Gefühl der Unsicherheit sind spekulativer Natur und reichen, ebenso wie eine vermeintlich abschreckende Wirkung von Videoüberwachungen, in der Regel nicht aus. Vielmehr muss sich das berechtigte Interesse anhand konkreter Vorkommnisse, wie beispielsweise Beschädigungen oder anderen Ereignissen, die eine Gefahrenlage objektiv begründen. Solche Vorfälle begründen ein berechtigtes Interesse, wenn sie in der Vergangenheit bei Überwachenden selbst oder aber in der unmittelbaren Nachbarschaft nachweisbar mit erheblicher Schadenshöhe stattgefunden haben.

t) Zu § 18 Absatz 1 LDSG BW – neu

Die Videoüberwachung (§ 18 LDSG) soll nun als generell geeignetes Mittel zum Schutz besonders sicherheitsrelevanter Objekte zugelassen werden. Dies sei angeblich dadurch gerechtfertigt, dass andere Mittel einen **unverhältnismäßigen Aufwand** erfordern würden oder für die Aufgabenerfüllung nicht geeignet sind. Damit soll die Vorrangprüfung anderer Mittel erleichtert werden.

Des Weiteren wird die Abwägung mit den schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen gesetzlich insoweit determiniert, als der **Schutz von Leben, Gesundheit und Freiheit** von Personen an den geschützten Objekten als „besonders wichtiges öffentliches Interesse“ bestimmt wird.

Damit soll eine gesetzliche Angemessenheitsfiktion geschaffen werden. Hiergegen hat der Anwaltsverband BW erhebliche Bedenken. **Pauschal und im Voraus kann keine Erforderlichkeit festgestellt werden**. Es kommt immer auf eine Abwägung der beteiligten Interessen (Selbstbestimmungsrecht ./. Gefahrenabwehr/Strafverfolgung) an. So können in Eingangsbereichen beispielsweise auch die Rechte von Beschäftigten zu beachten sein. Eingangsbereiche könnten evtl. auch durch physische Barrieren, wie „Schikanen" oder „Pforten mit Zugangsberechtigungen", „Wachpersonal" oder bloßen Kamera-Attrappen, geschützt werden.

Soweit sich die Landesregierung im Evaluierungsbericht (LT-Drucks. 17/7596) darauf beruft, dass in der Kommentarliteratur teilweise die Auffassung vertreten werde, dass in die Prüfung der Erforderlichkeit auch die objektive und wirtschaftliche Zumutbarkeit des milderen Mittels für die verantwortliche Stelle eingestellt werden könne, ist zu sehen, dass die Rechtsprechung diesbezüglich bereits das Gegenteil entschieden hat. So hat etwa der **Bundesfinanzhof (BFH)** - zum Auskunftsanspruch nach Art. 15 DSGVO - in seinem **Urteil vom 14.01.2025,** Az. IX R 25/22, klargestellt, dass der **nicht mit dem Argument des unverhältnismäßigen Aufwands** verweigert werden darf. Auch der Gedanke des § 275 BGB finde keine Anwendung.

Diese Rechtsprechung kann auf die hiesige Konstellation übertragen werden.

Die niedrigen Anschaffungskosten und die verbesserte Qualität der Geräte sorgen dafür, dass Videoüberwachungssysteme in der Praxis sowohl im öffentlichen als auch im nicht-öffentlichen Bereich – immer häufiger zum Einsatz kommen sollen, gerade auch noch in Kombination mit KI-Auswertungen.

u) Zu § 18 Absatz 2 LDSG BW – neu – Hinweispflicht

Die Anforderungen an eine transparente und informierte Datenverarbeitung gegenüber betroffenen Personen gilt auch bei der Videoüberwachung. Somit sind die von einer Videoüberwachung betroffenen Personen entsprechend den Vorgaben aus Art. 12 ff DSGVO auf die Überwachung hinzuweisen und darüber zu informieren.

Nach den Empfehlungen der Landesdatenschutzbeauftragten sollte zunächst mit einem vorgelagerten **Hinweisschild**, das **auf Augenhöhe** angebracht sein sollte und den Betroffenen einen schnell wahrnehmbaren Überblick über die wichtigsten Informationen verschafft, auf die Videoüberwachung aufmerksam gemacht werden. Darauf sind neben einem **Kamerasymbol** bereits Angaben zum Verantwortlichen, seinem Datenschutzbeauftragten sowie zu Zwecken, Rechtsgrundlage und Speicherdauer zu platzieren.

Außerdem muss das Schild ein Hinweis enthalten, wie der Betroffene in einem zweiten Schritt die vollständigen Informationen nach Art. 13 DSGVO erhalten kann. Die vollständigen Informationen können an geeigneter Stelle ausgelegt oder ausgehängt und zusätzlich auf einer Webseite vorgehalten werden.

Die Informationspflichten der öffentlichen Stellen sollen mit dem Gesetzentwurf zugunsten der betroffenen Personen erweitert werden, (Art. 13 DSGVO). So sollen die Kontaktdaten für die Betroffenen erkennbar sein. Hier hat der Anwaltsverband BW Zweifel, ob dies angesichts des leider weithin zu beobachtenden Vandalismus eine wirkliche Hilfe wäre. Die Verantwortlichen müssten dann – personalintensiv – regelmäßig überprüfen, ob die Kontaktdaten jederzeit gut erkennbar und richtig sind.

Dass die Verwendung eines QR-Codes für die Übermittlung der Informationen zum Zweck der Videoüberwachung oder der Speicherdauer befriedigend ist, bezweifelt der Anwaltsverband BW ebenfalls. Zum einen setzt das Lesen eines QR-Codes voraus, dass der Betreffende ein Smartphone mit entsprechender Software (App) verfügt, was bei älteren Modellen nicht stets der Fall ist. Zum anderen werden immer mehr Fälle bekannt, in denen z. B. die QR-Codes an E-Mobil-Ladesäulen durch andere QR-Codes von Unbefugten verändert werden.

D.h. wenn eine Ausweitung der Videoüberwachung angestrebt wird, muss auch eine – nicht nur aufs Sparsamste beschränkte - Ausweitung der Bürgerinformation erfolgen.

v) Zu § 18 Absatz 4 LDSG BW – neu – Speicherfrist

Es gilt, dem Datenschutz durch Technikgestaltung (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) nachzukommen. Das betrifft beispielsweise auch die Auswahl der Kameras und deren Einstellungen, die so getroffen werden, dass Betriebszeiten, Aufnahmequalität und Erfassungsbereiche auf ein notwendiges Minimum reduziert werden.

Reicht eine **Beobachtung in Echtzeit** zur Erreichung des Zweckes aus, dürfen die Aufnahmen in aller Regel nicht zusätzlich gespeichert werden.

Ist eine Aufzeichnung zur Erreichung des Zwecks hingegen notwendig, ist auch die Speicherdauer der Aufzeichnung **jeder einzelnen Kamera** auf ein notwendiges Minimum zu reduzieren.

Oft kann **innerhalb von ein bis zwei Arbeitstagen** geklärt werden, ob eine Sicherung des Materials notwendig ist. Das bedeutet, dass eine Speicherdauer von 72 Stunden (3 Tage) – wie bei nicht-öffentlichen Stellen - in der Regel ausreichend sein dürfte.

Eine längere Speicherung der Aufnahmen kann nur für solche Kameras zulässig sein, für die eine besondere Begründung vorliegt.

Darüber hinaus sind Berechtigungskonzepte für den Zugriff auf die Aufnahmen zu erstellen. Bei netzwerkfähigen Videokameras ist regelmäßig die Sicherheit (Firmware-Aktualisierungen, Passwortschutz, Benutzerkonten, etc.) zu überprüfen.

Flankierend soll mit dem Gesetzentwurf die **maximale Speicherfrist von 4 Wochen auf zwei Monate erhöht** werden. Mit der Speicherdauer nimmt auch die Intensität des Eingriffs in die Rechte der gefilmten Personen zu.

Es entspricht der ständigen Rechtsprechung des Bundesverfassungsgerichts, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich untersagt ist,

> vgl. BVerfGE 65, 1 <46> (Volkszählungs-Urteil) v. 15.1.1983; BVerfGE 100, 313 <360> (Telekommunikationsüberwachung); BVerfGE 115, 320 <350> (Rasterfahndung II v. 4.4.2006) und BVerfGE 118, 168 <187 (Kontostammdaten v. 13.6.2007).

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit BW hat bereits bemängelt, dass die bisherige maximale Speicherdauer von vier Wochen in der Praxis häufig ausgenutzt werde, ohne dass dies sachlich erforderlich sei. Hierin sieht er den **Grundsatz der Speicherbegrenzung** aus Artikel 5 Absatz 1 Buchst. e DSGVO als verletzt an. Um dies zu vermeiden, schlägt er vor, die Höchstspeicherdauer von vier Wochen zu streichen. Damit würde die Pflicht zur unverzüglichen Löschung normiert werden.

Soweit die Gesetzesbegründung meint, die Verlängerung der Speicherfrist sei für den Fall notwendig, dass eine verletzte Person erst nach vier Wochen einen Strafantrag stellt, kann der Anwaltsverband BW das nicht nachvollziehen. Auf den Strafantrag sollte es nicht ankommen. Er ist nur in Fällen geringerer Verletzung, etwa tätliche Beleidigungen nach §§ 185ff StGB, erforderlich. Liegt ein schwereres Körperverletzungs-Delikt vor, etwa eine schwere Körperverletzung unter Beisichführen eines Messers nach §§ 223ff StGB, dürfte es sich schon um ein Offizialdelikt handeln, dass von der Staatsanwaltschaft ohnehin zeitnah zu ermitteln ist. In solchen Fällen kann man davon ausgehen, dass auch schnell die Polizei eingebunden ist, die wohl von allein auf die Idee kommen

wird, sich etwaig vorhandene Videoaufzeichnungen innerhalb von ein paar Tagen anzusehen und gegebenenfalls zu sichern.

Soweit die Gesetzesbegründung darauf abstellt, dass bei einem vermehrten Einsatz von Videotechnik mehr strafrechtlich relevante Vorfälle bekannt werden, die dann zu bearbeiten sind und dass bisherige Personal dafür mehr Zeit brauche, überzeugt auch das nicht. Die angemessene Lösung dieses verfassungsrechtlichen Konflikts kann nur darin bestehen, dass es dann entsprechend auch mehr Personalaufwuchses bedarf.

Es fragt sich auch, ob alle installierten Videokameras permanent gleichzeitig laufen müssen oder ob sie nur zu besonders risikoträchtigen Zeiten eingeschaltet sein müssen. D. h. durch intelligente Einsatzregelungen könnte auch Personal eingespart werden.

Nach erfolgreicher Interessensabwägung und danach ausgewählten und eingerichteten Kameras, ist die Videoüberwachung zur Erfüllung der Rechenschaftspflicht detailliert und vollständig zu **dokumentieren**. Dabei sollte jede Kamera (oder bei gegebener Vergleichbarkeit jede Kameragruppe) einzeln ins Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden.

Der Verantwortliche einer Videoüberwachungsanlage hat vorab außerdem eine **Datenschutz-Folgenabschätzung** durchzuführen, wenn eine Form der Verarbeitung, **insbesondere bei Verwendung neuer Technologien**, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Ob die Voraussetzungen dafür erfüllt werden, ist in jedem Einzelfall gesondert zu prüfen. Eine Datenschutz-Folgenabschätzung **ist jedenfalls dann vorzunehmen, wenn eine systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche** erfolgt oder **biometrische Verfahren** zur Datenverarbeitung eingesetzt werden.

Werden für den Betrieb und/oder die Wartung der Videoüberwachungsanlage Dienstleister eingesetzt, die ebenfalls Zugriff auf die Aufnahmen haben, stellt dies eine **Auftragsverarbeitung** gem. Art. 28 DSGVO dar, die den Abschluss eines sogenannten Auftragsverarbeitungsvertrages fordert.

w) Zu § 18a LDSG BW – neu – Videoüberwachung nicht-öffentlich zugänglicher Räume

Es soll eine Regelung zur Videoüberwachung einschließlich der KI-Nutzung nicht öffentlich zugänglicher Räume eingefügt und mit Regelungen zum Schutz der betroffenen Personen versehen werden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit BW hat bereits darauf hingewiesen, dass die Rechtslage umstritten sei. Während manche von einer geringeren Eingriffsintensität ausgingen, bestehe aus seiner Sicht in diesen Bereichen ein **erhöhter Schutzbedarf** im Vergleich zu öffentlich zugänglichen Räumen. Denn in letzteren müsse ohnehin jeder mit Beobachtung rechnen. Mithin sollte sich eine etwa zu schaffende Rechtsgrundlage für die Videobeobachtung auf enge Anwendungsfälle (wie sensible Forschungsbereiche) beschränken, quasi nur als Ultima Ratio, vergleichbar den Anforderungen an die Aufklärung von Straftaten durch Beschäftigte, und unter Beachtung des höheren Schutzbedarfs.

Dem kann sich der Anwaltsverband BW nur anschließen. Er fragt sich, wieso ein höherer Schutzbedarf als beispielsweise im Eingangsbereich von öffentlichen Gebäuden, wie Rathäusern, Hochschulen, Museen oder Baustellen bestehen soll, wenn doch ohnehin nicht Jedermann ein Zutrittsrecht hätte. Dann müsste es bereits ausreichende Vorkehrungen durch Schlüssel, Zugangscodes o.ä. geben.

Sofern öffentliche Stellen zum Schutz ihrer Baustelleneinrichtung oder sonstigen Einrichtung Videoüberwachung benötigen, könnte dies im Rahmen der Ausübung des Hausrechts auf § 4 LDSG gestützt werden, sofern Beschäftigte nicht erfasst werden, z. B. für die Überwachung außerhalb der Betriebszeiten.

Die Videoüberwachung von Beschäftigten beurteilt sich nicht nach § 18 LDSG, sondern nach § 15 LDSG. In § 15 Absatz 7 LDSG wird die Überwachung Beschäftigter mittels optisch-elektronischer Einrichtungen zum Zweck der Verhaltens- und Leistungskontrolle ausdrücklich verboten. Ausnahmen bestehen – nach der Rechtsprechung des BAG - nur bei dem Verdacht auf eine Straftat oder eine schwere Pflichtverletzung gemäß § 15 Absatz 5 LDSG, wobei ein Anfangsverdacht genügt.

x) Zu § 18b LDSG BW – neu – sonstige technische Überwachung – einschließlich KI-Systeme

Die Videoüberwachung soll für sicherheitsrelevante Einrichtungen und Gegenstände, Dienstgebäude, Kulturgüter und Verkehrsmittel abstrakt-generell als verhältnismäßiges Mittel zugelassen werden. In engen Grenzen sollen auch sonstige technische Mittel - mit KI-Unterstützung - zur Überwachung von öffentlichen Zwecken gewidmeten Gegenständen, wie **Bauwerken und Infrastruktur,** eingesetzt werden können, etwa um ihren Erhaltungszustand und die Funktionsfähigkeit zu überprüfen.

Damit soll u.a. auch die Videoüberwachung gemeint sein. Das wiederum kann dazu führen, dass - mehr oder weniger zufällig - auch personenbezogene Daten von Beschäftigten, Dienstleistern oder

Passanten erhoben werden. Aus diesem Grund ist verfassungsrechtlich eine Begrenzung derartiger Befugnisse erforderlich.

Soweit es um die Erfassung verdächtiger Geräusche geht, sieht der Gesetzentwurf eine Löschfrist von Tonaufnahmen binnen 3 Minuten vor.

y) Zu § 27a LDSG BW – neu – Datenschutzaufsicht für digitale Dienste

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

2. Zu Art. 2 – Änderung des E-Government-Gesetzes BW (EGovG BW)

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

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

Bei automatisierten Entscheidungen im Einzelfall (einschließlich Profiling) sind die Vorgaben des **Art. 22 DSGVO** zu beachten.
Einschränkung automatisierter Entscheidungsfindung

- Einschränkung bei Art. 9 DSGVO-Daten
- Transparenzerfordernis

Jede Person hat das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Ausnahmen bestehen in Art. 22 Abs. 2 DSGVO: Eine ausschließlich automatisierte Entscheidung wäre erlaubt, wenn sie für den Abschluss oder die Erfüllung eines Vertrags mit der betroffenen Person erforderlich ist (lit. a), gesetzlich zulässig ist unter Wahrung angemessener Garantien (lit. b) oder ausdrücklich auf der Einwilligung der Person beruht (lit. c).

a) Zu § 17 – neu – Erprobung automatisierter Erlass von Verwaltungsakten einschließlich KI

Aus § 28 LVwVfG und den Verfahrensordnungen (und Art. 103 GG) ergibt sich das Recht des Betroffenen auf rechtliches Gehör. Die danach gebotene Anhörung vor Erlass belastender Verwaltungsakte geschieht häufig durch Übersendung eines Bescheidentwurfs. Wie dies bei einer Vollautomatisierung des Verfahrens geschehen soll oder auch nur kann, ist fraglich. Die Nachholung einer unterbliebenen Anhörung mag im Einzelfall durch ein nachfolgendes Rechtsbehelfsverfahren geheilt werden können. Ein systembedingt ständiges Unterlassen der Anhörung ist hingegen rechtsstaatlich nicht hinnehmbar.

Neben dem Recht auf rechtliches Gehör folgt auch aus dem Recht auf ein faires Verfahren, das aus Art. 1 Abs. 1 GG bzw. Art. 1 Abs. 1 GG i.V. mit Art. 2 Abs. 1 GG und dem Rechtsstaatsprinzip des Art. 20 Abs. 3 bzw. aus Art. 6 EMRK hergeleitet wird, dass die Einzelperson nicht nur **Objekt** des Verfahrens sein darf. Auch dies schließt den Einsatz eines algorithmischen Systems als Entscheider aus.

Um dem Betroffenen Rechtsschutz zu gewähren, bedarf es mindestens eines aufschiebend wirkenden Widerspruchsrechts für den Betroffenen, falls Fehler auftreten. Darauf ist er natürlich rechtzeitig hinzuweisen (Rechtsbehelfsbelehrung).

Wegen der beschriebenen Bedenken ist die Befristung der Erprobungsmöglichkeit jedenfalls zu begrüßen. Die geforderte Evaluierung ist zwingend auch dem Landtag vorgelegt werden, der ggf. Korrekturen des Gesetzes vorzunehmen hat. Würde der Landtag nicht unterrichtet werden, würde seine Gesetzgebungskompetenz faktisch unterlaufen. Gerade im Bereich des Einsatzes von neuartiger KI ist mit Entwicklungen zu rechnen, die jetzt noch nicht zuverlässig abgeschätzt werden können. Konsequenterweise ist der Landtag deshalb auch darüber zu unterrichten, welche KI in welcher Version jeweils eingesetzt werden soll.

3. Zu Art. 3 – Änderung des Gesetzes zur Ausführung des Personenstandsgesetzes (AGPStG)

Die Standesämter sollen Personen, die in der zuständigen unteren Fachaufsichtsbehörde mit der Standesamtsaufsicht betraut sind, zur Erfüllung dieser Aufgaben den Abruf der in ihrem elektronischen Personenstandsregister gespeicherten personenbezogenen Daten - mit Ausnahme der mit einem Sperrvermerk nach § 64 des Personenstandsgesetzes (PStG) versehenen Daten - ermöglichen.

Künftig soll sich das Abrufverfahren auch auf die elektronischen Sammelakten der Standesämter erstrecken.

4. Zu Art. 4 – Änderung des Landesinformationsfreiheitsgesetzes

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

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

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

5. Zu Art 5. – Änderung des Landesmediengesetzes

Die Neufassung dient der Anpassung des Landesmediengesetzes an die Änderungen im Medienstaatsvertrag durch den Fünften Staatsvertrag zur Änderung medienrechtlicher Staatsverträge, der am 01.10.2024 in Kraft trat. Wegen der Überführung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) in das Telekommunikation-Digitale Dienste-Datenschutz-Gesetz (TDDDG) sowie des Telemediengesetzes (TMG) in das Digitale-Dienste-Gesetz (DDG) sind des Weiteren die jeweiligen Verweisungen anzupassen.

Die Verpflichtung zur Sicherung der **Regionalfensterprogramme** in Baden-Württemberg wird gesetzlich klargestellt. Die Zulassung für Fensterprogrammveranstalter wird auf zehn Jahre begrenzt.

Des Weiteren erfolgt die notwendige Anpassung an die bundesgesetzliche Überführung des Telemediengesetzes in das Digitale-Dienste-Gesetz. Die Landesanstalt für Kommunikation übernimmt zusätzlich die

Zuständigkeit der Verwaltungsbehörde für die Verfolgung und Ahndung der Ordnungswidrigkeit nach § 33 Absatz 1 DDG.

6. Zu Art 6. – Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten

In der OWiZuVO ist die Verweisung auf das TTDSG in eine solche auf das TDDDG anzupassen. Die Zuständigkeit für die Ordnungswidrigkeit nach § 33 Absatz 1 DDG übernimmt die Landesanstalt für Kommunikation. Im Übrigen handelt es sich nach dem Verständnis des Anwaltsverbandes um redaktionelle Änderungen, weshalb hiergegen keine Bedenken bestehen.

III. Fazit

Wir würden uns freuen, wenn unsere Hinweise und Vorschläge Berücksichtigung finden würden. Für etwaige Rückfragen oder auch Gespräche stehen wir selbstverständlich gerne zur Verfügung. Sollte im Laufe des weiteren Verfahrens eine weitere Anhörung durchgeführt werden, so bitten wir um eine Unterrichtung und die Gelegenheit zur

Mit freundlichen Grüßen

Prof. Dr. Peter Kothe
Präsident