

Heutiges LDSG	LDSG in der Fassung LT-Beschluss am 04.02.2026, LT-Drs. 17/10253	Aus der Begründung Gesetzesentwurf der Landesregierung LT-Drs. 17/9983	Interessantes aus dem Anhörungsverfahren (Auszüge, LT-Drs. 17/9983)
§ 2[1] Anwendungsbereich (1) 1Dieses Gesetz gilt nach Maßgabe von Absatz 2 bis 7 für die Verarbeitung personenbezogener Daten durch Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). 2Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses Gesetz nichts anderes bestimmt. 3Dieses Gesetz gilt nicht für die Verarbeitung personenbezogener	§ 2[1] Anwendungsbereich (1) 1Dieses Gesetz gilt nach Maßgabe von Absatz 2 bis 7 für die Verarbeitung personenbezogener Daten durch Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). 2Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses <u>oder ein anderes</u> Gesetz nichts anderes bestimmt. 3Dieses Gesetz gilt nicht für die Verarbeitung	S. 63: Klarstellung, dass abweichende Definitionen des Verantwortlichen in anderen Gesetzen erfolgen, z.B. § 67 Abs. 4 SGB X.	

Daten 1.durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes, 2.beim Vollzug des <u>Landessicherheitsüberprüfungsgesetzes</u>, 3.durch die Polizei sowie die Gerichte, Staatsanwaltschaften, das Justizministerium und die Justizvollzugsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von	personenbezogener Daten 1.durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes, 2.beim Vollzug des <u>Landessicherheitsüberprüfungsgesetzes</u>, 3.durch die Polizei sowie die Gerichte, Staatsanwaltschaften, das Justizministerium und die Justizvollzugsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von		
--	--	--	--

Gefahren für die öffentliche Sicherheit und 4.durch andere für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständige Stellen, soweit besondere Rechtsvorschriften keine abweichenden Regelungen treffen. 4§ <u>30</u> gilt auch für die Verarbeitung personenbezogener Daten nach Satz 3. (2) 1Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile	Gefahren für die öffentliche Sicherheit und 4.durch andere für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständige Stellen, soweit besondere Rechtsvorschriften keine abweichenden Regelungen treffen. 4§ <u>30</u> gilt auch für die Verarbeitung personenbezogener Daten nach Satz 3. (2) 1Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile		
--	--	--	--

oder absoluter Mehrheit der Stimmen beteiligt sind. 2Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts nach Satz 1 an einer weiteren Vereinigung des privaten Rechts, findet Satz 1 entsprechende Anwendung. 3Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes. (3) 1Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. 2Die Vorschriften dieses Gesetzes gehen denen des <u>Landesverwaltungsverfahrensgesetzes</u> vor, soweit bei der	oder absoluter Mehrheit der Stimmen beteiligt sind. 2Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts nach Satz 1 an einer weiteren Vereinigung des privaten Rechts, findet Satz 1 entsprechende Anwendung. 3Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes. (3) 1Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. 2Die Vorschriften dieses Gesetzes gehen denen des <u>Landesverwaltungsverfahrensgesetzes</u> vor, soweit bei der		
--	--	--	--

Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden. (4) 1Soweit die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit stattfindet, die nicht in den sachlichen Anwendungsbereich der <u>Verordnung (EU) 2016/679</u> oder der <u>Richtlinie (EU) 2016/680</u> des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI	Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden. (4) 1Soweit die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit stattfindet, die nicht in den sachlichen Anwendungsbereich der <u>Verordnung (EU) 2016/679</u> oder der <u>Richtlinie (EU) 2016/680</u> des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI		
--	--	--	--

des Rates (ABl. L 119 vom 4. Mai 2016, S. 89) fällt, gelten die Regelungen der <u>Verordnung (EU) 2016/679</u> und dieses Gesetz entsprechend, sofern die Verarbeitung nicht in besonderen Rechtsvorschriften geregelt ist. 2Die Artikel <u>30</u>, <u>35</u> und <u>36</u> der Verordnung (EU) 2016/679 gelten nur, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. 3Auf die Prüfungstätigkeit des Rechnungshofs und der staatlichen Rechnungsprüfungsämter finden Artikel <u>30</u> und Kapitel VI der Verordnung (EU) 2016/679 sowie §§ <u>25</u> und <u>26</u> dieses Gesetzes keine Anwendung.	des Rates (ABl. L 119 vom 4. Mai 2016, S. 89) fällt, gelten die Regelungen der <u>Verordnung (EU) 2016/679</u> und dieses Gesetz entsprechend, sofern die Verarbeitung nicht in besonderen Rechtsvorschriften geregelt ist. 2Die Artikel <u>30</u>, <u>35</u> und <u>36</u> der Verordnung (EU) 2016/679 gelten nur, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. 3Auf die Prüfungstätigkeit des Rechnungshofs und der staatlichen- <u>RechnungsprüfungsämterGemeindeprüfungsanstalt Baden-Württemberg</u> finden Artikel <u>30</u> und Kapitel VI der Verordnung (EU) 2016/679 sowie §§ <u>25</u> und <u>26</u>		
--	---	--	--

(5) Dieses Gesetz gilt unbeschadet des Absatz 1 Nummer 3 für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. (6) 1Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nichtöffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden. 2Satz 1 gilt nicht für Zweckverbände. (7) Die Vorschriften dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten zur Ausübung des Begnadigungsrechts.	dieses Gesetzes keine Anwendung. (5) Dieses Gesetz gilt unbeschadet des Absatz 1 Nummer 3 für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden.<u>„(5) Dieses Gesetz gilt für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Abweichend hiervon gelten die §§ 2a, 3a, 4 Absatz 2, §§ 9a, 10 Absatz 4 und § 11a für Gerichte auch außerhalb von Verwaltungsangelegenheiten bei der Datenverarbeitung mittels künstlicher Intelligenz (KI) in Bezug auf KI-Systeme und KI-Modelle, soweit nicht besondere Rechtsvorschriften über Verfahren der Rechtspflege auf die Datenverarbeitung anzuwenden sind, die den Vorschriften dieses</u>		
--	---	--	--

	<u>Gesetzes vorgehen; Abschnitt 5 gilt nicht. Absatz 1 Satz 3 Nummer 3 bleibt unberührt.“</u> (6) 1Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nichtöffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden. 2Satz 1 gilt nicht für Zweckverbände. (7) Die Vorschriften dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten zur Ausübung des Begnadigungsrechts.		
	§ 2a Begriffsbestimmungen (1) Für die in diesem Gesetz verwendeten Begriffe sind, soweit nichts anderes bestimmt ist, die	Zu Absatz 3 (S. 65): „Das KI-Modell wird in der KI-Verordnung nicht im umfassenden Sinn definiert. In Artikel 3 Nummer 63 findet sich lediglich die	Im Anhörungsverfahren gab es die Forderung nach einer Definition „synthetischer Daten“. Dazu wird ausgeführt:

	Begriffsbestimmungen der Verordnung (EU) 2016/679 in der jeweils geltenden Fassung maßgeblich. (2) Ein System künstlicher Intelligenz (KI-System) ist ein KI-System im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L vom 12.7.2024) in der jeweils	Begriffsbestimmung des „KI-Modells mit allgemeinem Verwendungszweck“. Diese ist zu erweitern um KI-Modelle für spezielle Verwendungszwecke. Ein Beispiel wäre ein KI-Modell, das spezifisch dazu dient, Baugenehmigungsanträge oder Gerichtsakten zu strukturieren. Wie in den Sätzen 6 bis 8 von Erwägungsgrund 97 der KI-VO zum Ausdruck kommt, sind KI-Modelle wesentliche Komponenten von KI-Systemen, aber sie stellen für sich genommen keine KI-Systeme dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon.	„Die neu eingefügten Begriffsbestimmungen in § 2a dienen der Einheit der Rechtsordnung durch Verweisung auf bereits bestehende Begriffsbestimmungen. Demgegenüber hat sich für den unbestimmten Rechtsbegriff der synthetischen Daten noch keine allgemein anerkannte Definition herausgebildet, die übernommen werden könnte. Eine gesetzliche Definition sollte daher aktuell noch vermieden werden“ (S. 38)
--	--	--	---

	geltenden Fassung. (3) Ein Modell künstlicher Intelligenz (KI-Modell) ist ein KI-Modell mit allgemeinem Verwendungszweck im Sinne des Artikels 3 Nummer 63 der Verordnung (EU) 2024/1689 in der jeweils geltenden Fassung oder ein vergleichbares Modell, welches lediglich einen oder mehrere spezielle Verwendungszwecke aufweist, einschließlich KI-Modelle für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen.	Einbezogen werden in Bezug auf die Verarbeitung personenbezogener Daten KI-Modelle für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen; die KI-VO gilt für diese, ebenso wie für KI-Systeme mit demselben Zweck, gemäß Artikel 2 Absatz 6 der KI-VO nicht.“	
§ 3 (1) 1Bei der Datenverarbeitung sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen.	§ 3 (1) 1Bei der Datenverarbeitung sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen.	S. 65: Absatz 1 umformuliert zur Vermeidung von Missverständnissen. „Es sind zumindest die aufgezählten Maßnahmen auf ihre	

2Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. 3Zu den Maßnahmen können insbesondere gehören: 1.technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der <u>Verordnung [EU] 2016/679</u> erfolgt, 2.Maßnahmen, die die nachträgliche Überprüfung und Feststellung	2Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. 3<u>Zu den Maßnahmen können insbesondere gehören Technische und organisatorische Maßnahmen müssen sicherstellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt; zu den erforderlichen Maßnahmen können insbesondere gehören:</u> <u>1.technische und organisatorische Maßnahmen, um sicherzustellen, dass die</u>	Erforderlichkeit zu prüfen. Dies schließt es ein, ihre Einhaltung zu kontrollieren.“ Zur Nr. 6: Eine häufige Ursache für Datenschutzvorfälle ist die unnötige direkte Anbindung von rein internen Systemen an das Internet. Es wird daher als zusätzliche zu prüfende Maßnahme die Abschottung der internen Systeme vor unbefugten Zugriffen aus öffentlichen Telekommunikationsnetzen eingefügt. Die Abschottung ist nicht alleine durch die physische Trennung erreichbar, sondern auch durch logische Trennung, wie dem Einsatz von Segmentierung oder Firewallsystemen. Bei der physischen Trennung wird	
--	---	---	--

gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind, 3. die Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten, 4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern, 5. die Pseudonymisierung personenbezogener Daten, 6. die Verschlüsselung personenbezogener Daten, 7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme	Verarbeitung gemäß der Verordnung [EU] 2016/679 erfolgt, 21. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind, 32. die Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten, 43. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern, 54. die Pseudonymisierung personenbezogener Daten,	z. B. ein System komplett ohne Netzwerkschnittstelle betrieben oder vom bestehenden Netzwerk abgekoppelt. Bei der logischen Trennung kann z. B. eine Firewall oder ein virtuelles, logisch getrenntes Netzwerk (VLAN) eingesetzt werden, um den Zugang zum Internet softwareseitig zu steuern oder zu unterbinden. Eine gänzliche Abschottung von rein internen Systemen wird häufig nicht umsetzbar sein, da auch rein interne Systeme oftmals eine Anbindung an das Internet benötigen, etwa zur Fernwartung oder zur Durchführung von Herstellerupdates. Daher wird die Abschottung auf unbefugte Zugriffe beschränkt.	
--	---	---	--

und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, 8.die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und 9.spezifische	<u>65</u>.die Verschlüsselung personenbezogener Daten, <u>6. die Abschottung von internen Systemen vor unbefugten Zugriffen aus öffentlichen Telekommunikationsnetzen</u> 7.die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,		
---	---	--	--

Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der <u>Verordnung [EU] 2016/679</u> sicherstellen.	8.die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und 9.spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der <u>Verordnung [EU] 2016/679</u> sicherstellen.		
	§ 3a Nutzung von KI-Systemen	S. 66: „§ 3a knüpft an bestehende	Ausführungen im

	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.	Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten an und erklärt die Verarbeitung– soweit die Voraussetzungen zur Verfügung stehen – für zulässig. [...] Die Vorschrift soll zum Ausdruck bringen, dass KI-Tools für die Verwaltung Betriebsmittel zur Erledigung von Aufgaben darstellen und als solche für ihre Nutzung den Zulässigkeitsvoraussetzungen für die Aufgabenerfüllung unterliegen. Zugleich wird vorausgesetzt, dass die eingesetzte KI entsprechend den rechtlichen Vorschriften entwickelt wurde und daher einsetzbar ist. Insbesondere sind die Vorschriften der KI-VO zu beachten. Für die Verarbeitung	Anhörungsverfahren: „Das KIT sowie ZENDAS regen an, § 3a LDSG als eigenständige umfassende Rechtsgrundlage auszugestalten. Nach Ansicht der DHBW hat die Regelung nur deklaratorische Wirkung. [...] Haltung der Landesregierung Die Aufsichtsbehörden werden prüfen, inwieweit konkrete Hilfsmittel bereitgestellt werden können. Im Übrigen werden die Anregungen nicht aufgegriffen. Explizitere Klauseln und Verweise würden den Gesetzestext unübersichtlich machen und bieten die Gefahr, dass sie regelmäßig umfangreich zu aktualisieren wären. Nur wenn kein (Nach-)Training des KI-Systems stattfindet, soll §
--	---	--	--

		besonderer Kategorien personenbezogener Daten bedarf es zusätzlich des Vorliegens der Voraussetzungen einer Ermächtigungsnorm aus Artikel 9 Absatz 2 DSGVO. Die Verarbeitung von personenbezogenen Daten durch Nutzung von KI-Systemen nach § 3a dient allein dem ursprünglichen Verarbeitungszweck und verändert das KI-System nicht. In Abgrenzung dazu wird in § 11a die Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen geregelt. Wenn bei der Nutzung von KI-Systemen gleichzeitig auch ein Training etc. des KI-Systems erfolgen soll, dann müssen die Voraussetzungen von § 3a und § 11a	3a die Nutzung von KI-Systemen als Betriebsmittel legitimieren; ansonsten bedarf es daneben das Vorliegen der Voraussetzungen des § 11a. Falls bei einem KI-System das Risiko (noch) nicht eingeschätzt werden kann, erweist sich dazu ein Test in einem KI-Reallabor in der Regel mit Beteiligung des LfDI als sinnvolles Mittel zur Risikobewertung. Das Erfordernis von geeigneten technischen und organisatorischen Maßnahmen ergibt sich bereits aus § 3. Die Nutzung der KI trotz verbleibenden hohen Risikos, welche durch ein parlamentarisches Gesetz legitimiert werden sollte, dürfte wenig praxisrelevant sein. Durch die Möglichkeit, ergänzend auf die bereits in der
--	--	--	--

		nebeneinander erfüllt sein.	Praxis bewährte Regelung in § 4 sowie sonstige Regelungen, die eine Datenverarbeitung erlauben, zurückzugreifen, wird eine umfassende Rechtsgrundlage geschaffen. Ein „klarstellender Verweis“ in § 3a auf § 11a ist nicht sinnvoll, weil die Nutzung von KI-Systemen nach § 3a unabhängig von Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen nach § 11a ist. Lediglich wenn die Daten aus der Nutzung von KI-System gleichzeitig zum Training eines KI-Modells verwendet werden, sind für das Training des KI-Modells die Voraussetzungen des § 11a zu prüfen. Die vom Anwaltsverband BW aufgezeigten Aspekte sind in der DSGVO, KI-VO bzw. im LDSG mit
--	--	------------------------------------	--

			den vorgeschlagenen Änderungen berücksichtigt.
§ 4 Zulässigkeit der Verarbeitung personenbezogener Daten Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.	§ 4 Zulässigkeit der Verarbeitung personenbezogener Daten <u>(1) Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.</u> <u>(2) Öffentliche Stellen dürfen, soweit zur Aufgabenerfüllung oder zur Ausübung öffentlicher Gewalt erforderlich, aus den rechtmäßig gespeicherten Daten synthetische Daten herstellen sowie rechtmäßig gespeicherte Daten</u>	S. 66 ff.: „Ergänzend zur datenschutzrechtlichen Generalklausel wird eine Erlaubnisnorm zur Anonymisierung sowie zur Herstellung synthetischer Daten eingefügt. Anonymisieren ist das Verändern von Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Synthetische Daten sind »künstliche« Daten, die in Eigenschaften und Struktur (idealerweise) den Originaldaten stark ähnlich sind, selbst aber keine »echten« Datenpunkte enthalten. Synthetische Daten	Ausführungen im Anhörungsverfahren, Haltung der Landesregierung: „Zwar sind die Voraussetzungen der Rechtsgrundlage sehr weit formuliert, aber durch eine Anonymisierung bzw. Synthetisierung wird allenfalls marginal in die Rechte der Betroffenen eingegriffen, sodass dem Verhältnismäßigkeitsgrundsatz genüge geleistet ist. Die vom LfDI gewünschte Pflicht zur regelmäßigen Überprüfung der Anonymität der Daten besteht immer, wenn vermeintlich anonyme Daten weiterverarbeitet werden. [...] Eine Anonymisierung „zum Zwecke der Datenminimierung“ bedeutet nicht,

	<u>auf sonstige Weise anonymisieren. Besondere Kategorien personenbezogener Daten dürfen entsprechend Satz 1 verarbeitet werden, wenn zusätzlich die Voraussetzungen des Artikels 9 Absatz 2 der Verordnung (EU) 2016/679 oder einer speziellen Rechtsgrundlage vorliegen.</u>	werden aus Originaldaten generiert, indem ein mathematisches Modell trainiert wird, das die Struktur der ursprünglichen Daten lernt und reproduzieren kann. Synthetische Daten und Originaldaten sollten daher bei einer statistischen Analyse sehr ähnliche Ergebnisse liefern (vgl. Kompetenzzentrum öffentliche IT, abrufbar unter: https://www.oeffentliche-it.de/blog/synthetische-daten/). Bei der Herstellung synthetischer Daten sind also im Verhältnis zu einer bloßen Entfernung von personenbezogenen Daten beim Regelfall der Anonymisierung mehr Datenverarbeitungsschritte erforderlich, damit die „synthetischen Daten“ nach der Anonymisierung in Eigenschaften und Struktur den Originaldaten	dass dies anstelle einer Löschung erfolgen müsste. Der Zweck der Datenminimierung wird bei einer Anonymisierung auch erfüllt, wenn der bisherige Datenbestand für den ursprünglichen Zweck weiterverwendet wird und die anonymisierten Daten für das Training eines KI-Modells verwendet werden sollen. Das Ergebnis der Herstellung von synthetischen Daten und Anonymisierung ist identisch, weil in beiden Fällen danach anonyme Daten vorliegen. Die Herstellung von synthetischen Daten ist aber in der Regel aufwendiger als eine normale Anonymisierung. “
--	---	--	--

		stark ähneln, aber keine personenbezogenen Originaldaten enthalten. Vor allem für die Forschung (§ 13) (andernfalls müssten die Voraussetzungen des § 13 für die Verarbeitung personenbezogener Daten vorliegen) sowie für die Entwicklung und das Training von KI (ansonsten § 11a) werden anonyme – und möglichst synthetische – Daten benötigt. Unabhängig von der strittigen Frage, ob die Anonymisierung eine Verarbeitung im Sinne der DSGVO ist, wird zur Klarstellung eine Rechtsgrundlage gemäß Artikel 6 DSGVO geschaffen, um dem Grundsatz der Datenminimierung – Daten dürfen nur in dem für die Zwecke der Verarbeitung notwendigen Maß verarbeitet	
--	--	--	--

		werden – nach Artikel 5 Absatz 1 Buchstabe c DSGVO Rechnung zu tragen. Da Echtdaten als Muster oder Vorlage für die Erstellung synthetischer Daten herangezogen werden, bedarf es diesbezüglich einer datenschutzrechtlichen Regelung. Die Erlaubnisnorm des § 4 Absatz 2 schafft eine rechtssichere Grundlage hierfür. Es bleibt aber zu betonen, dass der Anonymisierung jeweils ein legitimer Grund nach der DSGVO in Verbindung mit dem LDSG zugrunde liegen muss; dieser kann beispielsweise in der Forschung für einen bestimmten Zweck oder dem Training von KI für eine bestimmte Aufgabe liegen. Sind besondere Kategorien personenbezogener Daten betroffen, bedarf es einer	
--	--	---	--

		Legitimation nach Artikel 9 Absatz 2 DSGVO oder einer speziellen Rechtsgrundlage.	
§ 5 Datenverarbeitung zu anderen Zwecken (Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679) (1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist unbeschadet der Bestimmungen der <u>Verordnung [EU] 2016/679</u> zulässig, wenn 1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,	§ 5 Datenverarbeitung zu anderen Zwecken (Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679) (1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist unbeschadet der Bestimmungen der <u>Verordnung [EU] 2016/679</u> zulässig, wenn 1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist; <u>das Gemeinwohl ist</u>	S 67: Zu Nr. 1: Erlaubnis zur Zweckänderung aus Gründen des Gemeinwohls beruht auf Art. 6 Abs. 4 iVm Art. 23 Abs. 1 lit. e DS-GVO. Der Begriff Gemeinwohl soll gem. Art. 23 Abs. 2 lit. a DS-GVO konkretisiert werden. Man möchte offenbar sagen „Gemeinwohl“ = „öffentliches Interesse“ im Sinne von Art. 23 Abs. 1 lit. e DS-GVO. Zu Nr. 3: Geltende Fassung zu eng. Neufassung orientiert sich an § 23 Abs. 1 Nr. 4 BDSG. Beschränkung auf die Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung wird	

2.sie zum Schutz der betroffenen Person oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist, 3.sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung ergeben und die Unterrichtung der für die Verhütung, Verfolgung oder Vollstreckung zuständigen Behörden erforderlich ist oder 4.Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,	<u>gleichzusetzen mit den gesetzlich anerkannten allgemeinen öffentlichen Interessen,</u> 2.sie zum Schutz der betroffenen Person oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist, 3.sich bei der rechtmäßigen Aufgabenerfüllung- Anhaltspunkte für Straftaten- oder Ordnungswidrigkeiten- von erheblicher Bedeutung- ergeben und die- Unterrichtung der für die Verhütung, Verfolgung oder Vollstreckung zuständigen Behörden erforderlich ist- oder sie zur Verfolgung von Straftaten oder	aufgegeben. Korrektiv dafür ist die Verhältnismäßigkeit. Zu Nr. 5: Eingefügt auf Grundlage von Art. 6 Abs. 4 iVm Art. 23 Abs. 1 lit. i DS-GVO. Stellt klar, dass Zweckänderungen zugunsten der betroffenen Person zulässig sind, sofern dies objektiv im Interesse der betroffenen Person ist. Diese soll keine Nachteile durch unnötige Einbeziehung erleiden, wenn es sich um eine erkennbar begünstigende Maßnahme handelt und notwendige Angaben bereits bekannt sind. Die Zweckänderung ist jedoch unzulässig, wenn (z. B. aufgrund vorliegender Äußerungen) anzunehmen ist, dass die betroffene Person mit der	
---	---	--	--

soweit die Verarbeitung notwendig und verhältnismäßig ist.	<u>Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist.</u> 4. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen <u>oder</u>, <u>5. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zwecks ihre Einwilligung nicht erteilen</u>	Zweckänderung nicht einverstanden wäre. Im Zusammenspiel mit § 6 erlaubt die Regelung insbesondere eine Weiterleitung an die zuständige Behörde, wenn die betroffene Person ihr Anliegen an die unzuständige Behörde adressiert; denn die Weiterleitung an die zuständige Behörde entspricht in der Regel dem Interesse der betroffenen Person. Ob eine Ausnahme von dieser Regel vorliegt, ist jeweils zu prüfen.	
---	--	--	--

	<u>würde,</u> soweit die Verarbeitung notwendig und verhältnismäßig ist.		
§ 6 Übermittlung personenbezogener Daten (1) Die Übermittlung personenbezogener Daten zu anderen als ihren Erhebungszwecken ist zulässig, wenn 1.sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 5 zulassen würden oder 2.der Empfänger eine nichtöffentliche Stelle ist, die ein berechtigtes Interesse an	§ 6 Übermittlung personenbezogener Daten <u>(1) Die Übermittlung</u> <u>personenbezogener Daten zu</u> <u>anderen als ihren</u> <u>Erhebungszwecken an Stellen</u> <u>innerhalb des öffentlichen</u> <u>Bereichs ist zulässig, wenn sie zur</u> <u>Erfüllung der in der Zuständigkeit</u> <u>der übermittelnden oder der</u> <u>empfangenden öffentlichen Stelle</u> <u>liegenden Aufgaben erforderlich</u> <u>ist und die Voraussetzungen</u> <u>vorliegen, die eine Verarbeitung</u> <u>nach § 5 zulassen würden.</u> <u>(2) Die Übermittlung</u> <u>personenbezogener Daten zu</u> <u>anderen als ihren</u>	S. 68: Neufassung „zum besseren Verständnis“. Abs. 1/Abs. 2: Inhaltlich wurde keine Veränderung zu § 6 Absatz 1 LD SG vorgenommen, lediglich nunmehr die Alternative der Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen der übermittelnden Stelle eingefügt (vgl. Absatz 2 Nummer 3) sowie klargestellt, dass die Norm für die Übermittlung an alle Stellen innerhalb des öffentlichen Bereichs, also auch an die	

ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden. (2) 1Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde öffentliche Stelle. 2Erfolgt die Übermittlung an eine öffentliche Stelle im Geltungsbereich des <u>Grundgesetzes</u> auf deren Ersuchen, trägt diese die Verantwortung und erteilt die Informationen nach Artikel <u>14</u> der Verordnung [EU] 2016/679. 3Die übermittelnde öffentliche Stelle hat	<u>Erhebungszwecken an nichtöffentliche Stellen ist zulässig, wenn</u> <u>1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 5 zulassen würden,</u> <u>2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder</u> <u>3. es zur Geltendmachung, Ausübung von Rechtsansprüchen oder Verteidigung gegen Rechtsansprüche Dritter erforderlich ist.</u>	öffentlichen Stellen des Bundes und der Länder, gilt. Abs. 4: Eine andere Bestimmung ist in Absatz 4 für Datenübermittlungen auf Ersuchen aufgenommen, die nur für Ersuchen einer inländischen Stelle gelten. In Absatz 4 wird der Grundsatz festgelegt, dass die übermittelnde öffentliche Stelle die Verantwortung für die Übermittlung trägt. Dies gilt auch im Fall von Datenübermittlungen auf Ersuchen. Die Verantwortung für die Rechtmäßigkeit des Ersuchens oder des Abrufs im Fall von automatisierten Abrufen trägt die ersuchende bzw. die abrufende Stelle. Im Ergebnis ist die übermittelnde Stelle dafür	
--	--	---	--

im Falle des Satzes 2 lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden öffentlichen Stelle liegt. 4Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht. (3) 1Erfolgt die Übermittlung aufgrund eines automatisierten Verfahrens, welches die Übermittlung personenbezogener Daten durch Abruf ermöglicht, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Dritte, an den übermittelt wird. 2Die übermittelnde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass besteht. 3Sie hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt	<u>(3) Für die Übermittlung an Stellen in anderen Mitgliedstaaten der Europäischen Union, in Vertragsstaaten des Europäischen Wirtschaftsraums oder an Organe und Einrichtungen der Europäischen Union gelten Absatz 1 und 4 sowie die §§ 4 und 5 entsprechend, soweit nichts anderes bestimmt ist.</u> <u>(4) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde öffentliche Stelle. Erfolgt die Übermittlung aufgrund eines automatisierten Verfahrens, welches die Übermittlung personenbezogener Daten durch Abruf ermöglicht oder aufgrund eines Ersuchens einer öffentlichen Stelle im Geltungsbereich des Grundgesetzes, trägt die</u>	verantwortlich, dass für die Durchführung der Übermittlung eine Rechtsgrundlage besteht, ausgehend davon, dass das Ersuchen oder der Abruf rechtmäßig sind. Abs. 5: In Absatz 5 werden die Voraussetzungen für die Einrichtung eines automatisierten Abrufverfahrens normiert, sofern die Einrichtung nicht durch das Registermodernisierungsgesetz oder andere Gesetze (z. B. das AGPStG) geregelt ist. Eine solche Regelung fehlt bisher. Wegen der erhöhten Gefahren für den Schutz personenbezogener Daten durch automatisierte Abrufe	
---	--	--	--

und überprüft werden kann.	<u>Verantwortung für die Rechtmäßigkeit des Abrufs oder des Ersuchens die abrufende oder ersuchende Stelle; die übermittelnde Stelle prüft die Zulässigkeit des Abrufs oder die Rechtmäßigkeit des Ersuchens nur, wenn dazu Anlass besteht.</u> <u>(5) Automatisierte Abrufverfahren oder eine gemeinsame automatisierte Datei, in oder aus der mehrere öffentliche Stellen personenbezogene Daten verarbeiten, dürfen eingerichtet werden, soweit die rechtlichen Voraussetzungen zur Übermittlung vorliegen und die Einrichtung unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und</u>	bedarf die Einrichtung einer Abwägung des Nutzens mit der Beeinträchtigung des informationellen Selbstbestimmungsrechts der betroffenen Personen sowie technischer und organisatorischer Maßnahmen zur Vermeidung von Beeinträchtigungen. Ein Bedürfnis für gemeinsame Dateien kann bestehen, wenn verschiedene öffentliche Stellen gemeinsam in einer Datei arbeiten. Dies kann eine erhebliche Arbeitserleichterung darstellen. Abrufverfahren, die für jedermann zugängliche Daten eingerichtet werden, sind von der Regelung in Satz 1 nicht betroffen. Dies gilt unabhängig davon, ob es einer Zulassung der Person zum Abruf bedarf.	
-----------------------------------	--	--	--

	<u>organisatorische Maßnahmen</u> <u>Risiken für die Rechte und</u> <u>Freiheiten der betroffenen</u> <u>Personen vermieden werden.</u> <u>Automatisierte Abrufverfahren für</u> <u>Abrufe aus Datenbeständen, die</u> <u>jedermann ohne oder nach</u> <u>besonderer Zulassung</u> <u>offenstehen, dürfen ungeachtet</u> <u>der Bestimmungen in Satz 1</u> <u>eingerrichtet werden.</u>		
	§ 7a Auftragsverarbeitung; Verordnungsermächtigung (1) Soweit eine staatliche Behörde oder eine Anstalt in alleiniger Trägerschaft des Landes im Auftrag einer anderen öffentlichen Stelle, welche verpflichtet oder berechtigt ist, das Dienstleistungsangebot der staatlichen Behörde oder der Anstalt für die Erbringung von	S. 68: „Als Beispiel und Hauptanwendungsfall ist die BITBW anzuführen, die als Landesoberbehörde fungiert. [...] Insbesondere soll damit die Einbeziehung der L-Bank gewährleistet werden, sofern sie als Auftragsverarbeiter für das Land (z. B. bei Förderanträgen) tätig wird. [...]	Im Anhörungsverfahren aufgegriffen: „In die Verordnungsermächtigung des § 7a des Gesetzentwurfs wird der Bezug auf Absatz 1 ergänzt, um die Nichtanwendbarkeit für die Hochschulen auch hier klarzustellen“. Regelungstechnisch umgesetzt wurde dies, indem in Absatz 2

	Dienstleistungen zu nutzen, personenbezogene Daten nach Artikel 28 der Verordnung (EU) 2016/679 verarbeitet, erfolgt dies auf der Grundlage eines Auftragsverarbeitungsvertrags nach Artikel 28 Absatz 3 Satz 1 Alternative 1 der Verordnung (EU) 2016/679 nach Maßgabe der folgenden Bestimmungen. Zur Begründung des Auftragsverarbeitungsverhältnisses durch Vertrag teilt die verantwortliche öffentliche Stelle der staatlichen Behörde oder der Anstalt als Auftragsverarbeiter in Textform mit: 1. Gegenstand und Dauer der Verarbeitung, 2. Art und Zweck der Verarbeitung, 3. die Art der personenbezogenen	Die staatlichen Hochschulen im Sinne des § 1 Absatz 2 des Landeshochschulgesetzes werden von der Regelung ausgenommen. Für sie gilt auch Absatz 2 nicht. Die Spielräume, die die DSGVO für die Auftragsverarbeitung bietet, sollen für die Hochschulen erhalten bleiben.“	Satz 1 gegenüber dem Anhörungsentwurf eine Ergänzung (fett) aufgenommen wurde: „die Bestandteile der Auftragsverarbeitungsverträge nach Absatz 1 werden.“ „Nach Auffassung der Landesregierung ist Absatz 3 nicht auf die Hochschulen anwendbar, da die Hochschulen nach dem Landeshochschulgesetz nicht der Fachaufsicht unterliegen.“ (S. 42)
--	---	---	--

	Daten und 4. die Kategorien betroffener Personen. Die Sätze 1 und 2 gelten nicht für die staatlichen Hochschulen. (2) Die Landesregierung wird ermächtigt, durch Rechtsverordnung 1. die Pflichten und Rechte der verantwortlichen öffentlichen Stelle sowie des Auftragsverarbeiters festzulegen, 2. die Maßgaben nach Artikel 28 Absatz 3 Satz 2 der Verordnung (EU) 2016/679 für eine Auftragsverarbeitung durch den Auftragsverarbeiter zu bestimmen, 3. die Verpflichtung weiterer Auftragsverarbeiter, deren Dienste die staatliche Behörde oder die Anstalt in Anspruch nimmt, auf dieselben Datenschutzpflichten zu		
--	--	--	--

	regeln sowie 4. weitere Nutzungsbedingungen festzulegen, die Bestandteile der Auftragsverarbeitungsverträge nach Absatz 1 werden. Bestehende einzelvertragliche Regelungen zur Auftragsverarbeitung werden entsprechend der Rechtsverordnung ersetzt. Abweichende einzelvertragliche Vereinbarungen sind im Rahmen des nach Artikel 28 der Verordnung (EU) 2016/679 zulässigen Regelungsinhalts möglich. (3) Der Auftrag zur Verarbeitung personenbezogener Daten kann auch durch die Fachaufsichtsbehörde mit Wirkung für die ihrer Aufsicht		
--	---	--	--

	unterliegenden Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten.		
§ 8 Beschränkung der Informationspflicht (Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679) (1) Eine Pflicht zur Information der betroffenen Person besteht nicht, soweit und solange 1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, 2. die Information die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung	§ 8 Beschränkung der Informationspflicht (Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679) (1) Eine Pflicht zur Information der betroffenen Person besteht nicht, soweit und solange 1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde, 2. die Information die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung	S. 69: „Wie Artikel 23 Absatz 2 DSGVO regelt, müssen spezifische Vorschriften in Bezug auf die Transparenz und die Rechte der betroffenen Personen getroffen werden. Solche Regelungen fehlen bisher in § 8. Solche Regelungen fehlen bisher in § 8. In Anlehnung an die Regelungen in §§ 32, 33 BDSG werden entsprechende Maßnahmen vorgeschrieben. Die Pflicht zur Nachholung der Information, sobald der vorübergehende Hinderungsgrund entfallen ist, ergibt sich bereits aus dem Wort „solange“ in § 8 Absatz 1.“	Im Anhörungsverfahren aufgegriffen: „Wegen der im Forschungsbereich häufig nicht angezeigten Information der betroffenen Person bei Erhebung der Daten wird in Absatz 2 die Nummer 5 des Absatz 1 gestrichen. Dies hebt nicht die Verpflichtung auf, sobald wie möglich die Information zu erteilen bzw. nachzuholen.“ Regelungstechnisch umgesetzt wurde dies, indem die im Absatz 2 des Anhörungsentwurf genannte Nummer 5 gestrichen wurde.

gefährden würde, 3.die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde, 4.die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen oder 5.die Information voraussichtlich die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks unmöglich macht oder ernsthaft beeinträchtigt	gefährden würde, 3.die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde, 4.die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen oder 5.die Information voraussichtlich die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks unmöglich macht oder	Abs. 2: „Die Information kann beispielsweise durch die Bereitstellung der Information auf einer allgemein zugänglichen Webseite der verantwortlichen öffentlichen Stelle, ggf. auch in abstrakter Form, erfolgen (vgl. Erwägungsgrund 58 Satz 2 der DSGVO).“	
--	---	--	--

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. (2) 1Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten an Staatsanwaltschaften, Polizeibehörden oder den Polizeivollzugsdienst, Verfassungsschutzbehörden und, soweit sie in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der <u>Abgabenordnung</u> zur Überwachung und Prüfung personenbezogene Daten speichern, an Behörden der Finanzverwaltung, ist diesen Behörden vorab Gelegenheit zur Stellungnahme zu geben. 2Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener	ernsthaft beeinträchtigt und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. <u>(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1 Nummern 1 oder 2, ergreift die öffentliche Stelle geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 oder Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache.</u>		
--	--	--	--

Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, an andere Behörden des Bundesministers der Verteidigung. 3Satz 1 und 2 gelten entsprechend für die Information über die Herkunft der Daten von den genannten Behörden. (3) Die Gründe für das Absehen von der Information sind zu dokumentieren.	(23) 1Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten an Staatsanwaltschaften, Polizeibehörden oder den Polizeivollzugsdienst, Verfassungsschutzbehörden und, soweit sie in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der <u>Abgabenordnung</u> zur Überwachung und Prüfung personenbezogene Daten speichern, an Behörden der Finanzverwaltung, ist diesen Behörden vorab Gelegenheit zur Stellungnahme zu geben. 2Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes		
---	---	--	--

	berührt wird, an andere Behörden des Bundesministers der Verteidigung. 3Satz 1 und 2 gelten entsprechend für die Information über die Herkunft der Daten von den genannten Behörden. (43) Die Gründe für das Absehen von der Information sind zu dokumentieren.		
	§ 9a Beschränkung des Rechts auf Berichtigung (Ergänzung zu Artikel 16 der Verordnung [EU] 2016/679) Die Berichtigung von mit KI-Systemen und KI-Modellen verarbeiteten personenbezogenen Daten kann nicht verlangt werden, solange dies nur mit einem unverhältnismäßig hohen Aufwand an technischen oder wirtschaftlichen Mitteln oder	S. 70: „Nach dem Stand der Technik können Wahrscheinlichkeitsparameter, die als personenbezogene Daten gedeutet werden könnten, ob unrichtig oder rechtmäßig gespeichert, sehr schwierig oder gar nicht aus den KI-Modellen entfernt oder berichtigt werden. In dieser Lage könnten die KI-Modelle, um dem Berichtigungs-	Aus dem Anhörungsverfahren (S. 44 ff.): „Öffentliche Stellen werden häufig KI-Modelle übernehmen und entweder nachtrainieren oder in KI-Systeme integrieren. Fehlerhaften personenbezogenen Daten dürften in den großen Sprachmodellen bereits enthalten sein, bevor öffentliche Stellen überhaupt mit dem Training beginnen. Für die bereits in den

	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.“	oder Löschungsanspruch zu entsprechen, nur verworfen werden. Dies würde letztlich dazu führen, dass die öffentliche Verwaltung derzeit und auf unbestimmte Zeit dieses KI-Modell nicht einsetzen kann. Auf der anderen Seite ist die Anwendung von KI in der öffentlichen Verwaltung unverzichtbar, um effizient, in der gebotenen Qualität und ressourcenschonend die gesetzlichen Aufgaben zu erfüllen. Gemäß Artikel 23 Absatz 1 Buchst. e DSGVO erlaubt die Abwägung des Interesses des Einzelnen an der Wahrnehmung seiner Betroffenenrechte mit dem erheblichen öffentlichen Interesse am Einsatz von KI, die Betroffenenrechte – hier das Recht auf Berichtigung und	KI-Modellen vorhandenen fehlerhaften personenbezogenen Daten bedarf es einer Beschränkung der Berichtigungs-/Löschungsrechte, damit diese KI-Systeme einsetzbar bleiben. [...] Die Vorteile bei der Filterlösung durch diese Datenverarbeitung überwiegen aufgrund der gesetzlich nach § 9a Satz 4 (in Verbindung mit § 10 Absatz 4) festgelegten strengen Zweckbindung die Nachteile dieser Datenverarbeitung. Filter zur Berichtigung bekannter fehlerhafter Ausgaben von KI-Modellen sind in kommerziellen Produkten regelmäßig integriert und an deren sicherer und dauerhafter Umsetzung bestehen
--	--	--	--

		Löschung – zu beschränken. Die Beschränkung darf nur in verhältnismäßigem Umfang erfolgen, also nur, soweit die Erfüllung des Anspruchs auf Berichtigung oder Löschung unverhältnismäßigen Aufwand erfordern würde. Desgleichen müssen alle zur Verfügung stehenden technischen Maßnahmen genutzt werden, um die Betroffenenrechte zu erfüllen. Nach derzeitigem Stand kommen hierfür insbesondere Filter in Betracht. Unbeeinträchtigt bleibt das Recht nach Artikel 16 Satz 2 DSGVO, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. Ebenso wenig kann eine Entscheidung	keine durchgreifenden Zweifel. Bei der Einschränkung der Betroffenenrechte wird dem Verhältnismäßigkeitsgrundsatz dadurch Rechnung getragen, dass der Berichtigungsanspruch (§ 9a) bzw. Löschungsanspruch (§ 10 Absatz 4) nur ausgeschlossen ist, „solange dies nur mit einem unverhältnismäßig hohen Aufwand an technischen oder wirtschaftlichen Mitteln oder erheblichen ökologischen Folgen möglich wäre oder solange der rechtmäßige Zweck der Verarbeitung erheblich erschwert würde“. Dadurch, dass an die Stelle der Berichtigung ein Filter oder sonstige geeignete Maßnahmen treten, erfolgt eine Abwägung des Interesses des Einzelnen an der Wahrnehmung seiner Betroffenenrechte mit dem
--	--	--	---

		gegenüber der betroffenen Person auf eine unrichtige Eingabe oder Ausgabe gestützt werden.“	erheblichen öffentlichen Interesse am Einsatz von KI. Aus dem Wortlaut des § 9a (in Verbindung mit § 10 Absatz 4) und dem Regelungszusammenhang mit Artikel 23 Absatz 1 Buchstabe e DSGVO ergibt sich die Darlegungslast der öffentlichen Stelle, dass die Berichtigung bzw. Löschung „nur mit einem unverhältnismäßig hohen Aufwand an technischen oder wirtschaftlichen Mitteln oder erheblichen ökologischen Folgen möglich wäre oder solange der rechtmäßige Zweck der Verarbeitung erheblich erschwert würde“. Die Frage des unverhältnismäßigen hohen Aufwands ist eine Frage des Einzelfalls, die nicht durch den Gesetzgeber präzise definiert
--	--	--	--

			werden kann. [...] Eine entsprechende Beschränkung des Auskunftsrechts wird für nicht erforderlich bewertet, weil nicht ersichtlich ist, warum die Geltendmachung des Auskunftsrechts ähnlich schwerwiegende Folgen wie die Geltendmachung eines Berichtigungsanspruchs oder Löschungsanspruchs hätte. Die Nennung weiterer geeigneter Maßnahmen neben Filtern kommt mangels bereits bekannter technischer Möglichkeiten nicht in Betracht. Die Formulierung sollte aber zukunfts offen noch keine weiteren Möglichkeiten ausschließen. Sobald zukünftig im Einzelfall geeignetere
--	--	--	--

			Maßnahmen zur Verfügung stehen, sind diese je nach Beurteilung der Verhältnismäßigkeit des Aufwands zu ergreifen. [...]“
§ 10 Beschränkung des Rechts auf Löschung (Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679) (1) Die Bestimmungen des <u>Landesarchivgesetzes</u> zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten bleiben unberührt. (2) 1Die Pflicht zur Löschung personenbezogener Daten nach Artikel 17 der Verordnung [EU] 2016/679 besteht nicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung	§ 10 Beschränkung des Rechts auf Löschung (Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679) (1) Die Bestimmungen des <u>Landesarchivgesetzes</u> zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten bleiben unberührt. (2) 1Die Pflicht zur Löschung personenbezogener Daten nach Artikel 17 der Verordnung [EU] 2016/679 besteht nicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung	S. 70: „Ein Löschungsanspruch entsteht in den in Artikel 17 DSGVO genannten Fällen, insbesondere, wenn die Speicherung zur Aufgabenerfüllung nicht mehr erforderlich ist oder die betroffene Person ihre Einwilligung widerrufen oder Widerspruch eingelegt hat. Auch hier soll die Speicherbegrenzung nicht regelmäßig dazu führen, dass KI-Systeme nicht mehr einsetzbar sind. Denn ein KI-Modell von Grund auf neu zu trainieren, ist extrem teuer und zeitaufwändig Da die praktische Umsetzung des Löschungsanspruchs auf	

schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. 2In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel <u>18</u> der Verordnung [EU] 2016/679. 3Die öffentliche Stelle unterrichtet die betroffene Person über das Absehen von der Löschung und die Einschränkung der Verarbeitung. 4Widerspricht die betroffene Person dem Absehen von der Löschung, sind die Daten zu löschen. (3) 1Ist eine Löschung im Falle nichtautomatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering	schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. 2In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel <u>18</u> der Verordnung [EU] 2016/679. 3Die öffentliche Stelle unterrichtet die betroffene Person über das Absehen von der Löschung und die Einschränkung der Verarbeitung. 4Widerspricht die betroffene Person dem Absehen von der Löschung, sind die Daten zu löschen. (3) 1Ist eine Löschung im Falle nichtautomatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering	vergleichbare Schwierigkeiten wie beim Berichtigungsanspruch stößt, wird der Lösungsanspruch entsprechend der Beschränkung beim Berichtigungsanspruch behandelt, nämlich auf Maßnahmen reduziert, die mit verhältnismäßigem Aufwand machbar sind. Hierzu kann ein Filter dienen, der die Antwort des KI-Modells in Bezug auf bestimmte personenbezogene Daten filtert, so dass diese nicht ausgegeben werden.“	
---	---	--	--

anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht der öffentlichen Stelle zur Löschung personenbezogener Daten nicht. 2In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. 3Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.	anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht der öffentlichen Stelle zur Löschung personenbezogener Daten nicht. 2In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. 3Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden. <u>(4) Für die Löschung gilt § 9a entsprechend.</u>		
	§ 11a Entwicklung, Training, Testen, Validierung und Beobachtung von KI-Systemen und KI-Modellen Für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen dürfen zum Zweck der Erfüllung von in	S. 70 ff: „Öffentliche Stellen sind „Akteure“ im Sinne des Artikels 3 Nummer 8 der KI-VO. Sie dürfen also KI-Systeme insbesondere in eigener Verantwortung im Rahmen ihrer Tätigkeit verwenden (Betreiber im Sinne des Artikels 3 Nummer 4 der KI-VO) und KI-Systeme oder	

	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.	ein KI-Modell mit allgemeinem Verwendungszweck entwickeln oder entwickeln lassen und in den Verkehr bringen oder in Betrieb nehmen (Anbieter im Sinne des Artikel 3 Nummer 3 der KI-VO). Der Einsatz ist auf die Wahrnehmung der öffentlich-rechtlichen Verwaltungstätigkeit begrenzt und setzt die Einhaltung der maßgeblichen Rechtsvorschriften voraus. [...] § 11a schafft für die Entwicklung und das Training sowie weitere benannte Verarbeitungsschritte, die der KI-Einsatz erfordert, eine Rechtsgrundlage. [...] Der Begriff des Trainings ist folglich umfassend gemeint und schließt sämtliche Trainingsformen mit ein, sowohl bei der Entwicklung und Initialisierung von KI-Systemen als auch bei der Nutzung und im	
--	--	--	--

		Rahmen der Anpassung und Verbesserung bestehender KI-Systeme. Im Rahmen des Trainings kommen Trainings-, Validierungs- und Testdatensätze im Sinne der KI-VO zum Einsatz. [...] Soweit ein Datensatz personenbezogene Daten im Sinne von Artikel 4 Nummer 1 DSGVO enthält, schaft § 11a eine Rechtsgrundlage für deren Verarbeitung im Sinne von Artikel 4 Nummer 2 DSGVO nach Maßgabe des Artikels 6 Absatz 1 in Verbindung mit Absatz 3 Buchst. b DSGVO zum Zweck des Trainings von KI-Systemen. [...] Ist das Training mit pseudonymisierten Daten wiederum nicht zweckmäßig oder der Aufwand der Pseudonymisierung unverhältnismäßig, dürfen die	
--	--	--	--

		personenbezogenen Daten ohne vorherige Anonymisierung und Pseudonymisierung für das Training verarbeitet werden. Entscheidend für die Verwendung personenbezogener Klardaten für das Training ist also, dass die beabsichtigte Art und Qualität der Ergebnisse, die durch das KI-System erzeugt werden, nicht mit anonymen oder pseudonymen Daten herbeigeführt werden kann.	
	§ 12a Verarbeitung zu Zwecken der parlamentarischen Kontrolle Die Landesregierung darf personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten zur Beantwortung parlamentarischer Anfragen und Anträge sowie zur Vorlage von	S. 72: Für die Verarbeitung personenbezogener Daten zu Zwecken parlamentarischer Kontrolle wird zur Klarstellung eine Rechtsvorschrift in das LDSG eingefügt. Die gesetzliche Regelung orientiert sich an der	

	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.	verfassungsgerichtlichen Rechtsprechung des Verfassungsgerichtshofs für das Land Nordrhein-Westfalen vom 20. April 2021, Az.: VerfGH 177/20, https://openjur.de/u/2337610.html) .	
§ 13 Datenverarbeitung zu wissenschaftlichen oder	§ 13 Datenverarbeitung zu wissenschaftlichen oder	S. 73:	Aus dem Anhörungsverfahren (S.

historischen Forschungszwecken und zu statistischen Zwecken (1) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. 2 Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz	historischen Forschungszwecken und zu statistischen Zwecken (1) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten <u>und vorhandene Daten der genannten Art weiterverarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können wenn die Verarbeitung zu diesen Zwecken erforderlich ist</u> und die Interessen der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem	Abs. 1 „Mit der eingefügten Erlaubnis zur zweckändernden Weiterverarbeitung vorhandener Daten zu Forschungs- oder Statistikzwecken (retrospektive Nutzung) wird der in der DSGVO angelegten Privilegierung der Forschung, wonach unter Einhaltung von Garantien für die Rechte und Freiheiten der betroffenen Personen die Weiterverarbeitung personenbezogener Daten für die Forschung zulässig ist, ausdrücklich Rechnung getragen. Dies gilt auch für die zweckändernde Weiterverarbeitung besonderer Kategorien personenbezogener Daten. [...] Absatz 1 erlaubt auch die	47 ff.): Zu Absatz 1 (LfDI hielt Vorschrift nur für berechtigt, wenn der Stelle die Aufgabe der Forschung zugewiesen wurde): „Es muss den öffentlichen Stellen im Rahmen ihrer Aufgabenerfüllung erlaubt sein, Forschungsvorhaben durchzuführen. Hierfür spricht auch die Regelung in Artikel 5 Absatz 1 Buchstabe b DSGVO Forschung stellt einen Annex zur jeweiligen Aufgabe dar. Ein Beispiel hierfür ist die Mobilitätsforschung oder die kriminalpolizeiliche Forschung. Die ausdrückliche Legitimation für die Sekundärforschung wird für berechtigt gehalten.“ Zu Absatz 2 (LfDI hielt Verarbeitung öffentlich zugänglicher Daten für Forschung
--	---	--	---

<u>1</u> der Verordnung (EU) 2016/679 genannten Daten. (2) 1Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. 2Bis zur Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmaren Person zugeordnet werden können. 3Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert. (3) Die wissenschaftliche oder historische Forschung betreibenden öffentlichen Stellen	Ausschluss der Verarbeitung überwiegen. 2Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten. <u>(2) Für wissenschaftliche Forschungszwecke ist die Verarbeitung allgemein zugänglicher personenbezogener Daten zulässig, es sei denn, dass schutzwürdige Interessen der betroffenen Person der Datenverarbeitung entgegenstehen.</u> (32) 1Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. 2Bis zur	Forschung mit Kooperationspartnern in gemeinsamer Verantwortung unter den genannten Voraussetzungen. Die Übermittlung an Dritte für deren eigene Forschungsvorhaben ist in Absatz 4 geregelt. In der Evaluierung wurde festgestellt, dass die Formulierung in Satz 1 des Absatz 1 der Zulässigkeit der Verarbeitung personenbezogener Daten, „wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können“ zum Missverständnis in der Praxis dergestalt geführt hat, dass ein Vorrang der Einwilligung als Grundlage für die Datenverarbeitung angenommen	nicht pauschal für zulässig): „Aus der Norm ergibt sich eindeutig, dass die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen sind. Dies ist jeweils zu prüfen.“ Zu Absatz 3: „Die zu treffenden Maßnahmen müssen sich nach der Schutzbedürftigkeit der Daten richten. Bei der Vielfalt möglicher Forschungsvorhaben müssen die zu treffenden technischen und organisatorischen Maßnahmen im Einzelfall bestimmt werden. Hier besteht der Unterschied zu der geregelten Forschung mit Gesundheitsdaten und genetischen Daten. Diesbezüglich finden die spezifischen Regelungen vorrangige
---	--	--	---

dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. (4) 1Die in Artikel <u>15</u>, <u>16</u>, <u>18</u> und <u>21</u> der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der jeweiligen Forschungs- oder Statistikzwecke notwendig ist. 2Das Recht auf Auskunft gemäß Artikel <u>15</u> der Verordnung (EU) 2016/679 besteht darüber hinaus	Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbar Person zugeordnet werden können. 3Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert. <u>Zur Wahrung der Interessen der betroffenen Person sind weitere angemessene und spezifische Maßnahmen entsprechend § 3 Absatz 1 zu treffen.</u> (43) Die wissenschaftliche oder historische Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen über	wurde. Die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 DSGVO stehen gleichberechtigt nebeneinander; die einwilligungsbasierte Verarbeitung hat keinen Vorrang vor der auf gesetzlicher Grundlage beruhenden Verarbeitung. Zur Klarstellung werden daher in Satz 1 die genannten Wörter ersetzt und stattdessen die Erforderlichkeit zum Maßstab für die Zulässigkeit eingeführt. Dies entspricht auch der von der DSGVO verwendeten Terminologie in Artikel 9 Absatz 2 Buchst. j DSGVO. Inhaltlich ist weiterhin zu prüfen, ob der Zweck mit weniger eingriffsintensiven Mitteln, insbesondere mit anonymisierten oder, falls dies	Anwendung. Forschung mit genetischen Daten ist im LDSG nicht bezweckt, da der damit verbundene Grundrechtseingriff eine spezifische Regelung erfordert.“ Zu Absatz 5 (S. 48 ff.): „Den betroffenen Personen steht das Widerspruchsrecht nach Artikel 21 DSGVO zur Verfügung. Ein darüber hinausgehendes Widerspruchsrecht wird nicht für erforderlich gehalten. Der Forschung wird ein hohes Gewicht zugunsten der Allgemeinheit zugemessen, weshalb die Regelung eingeführt wird. Die Verarbeitung von Gesundheitsdaten im Krankenhausbereich richtet sich nicht nach dem LDSG, sondern nach dem
---	--	--	---

nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.	Ereignisse der Zeitgeschichte unerlässlich ist. <u>(5) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten an nichtöffentliche Stellen zu deren gemeinwohlbezogenen Forschungszwecken übermitteln, wenn dies zur Erfüllung des Forschungszwecks erforderlich ist und die Interessen der forschenden Dritten die Interessen der betroffenen Personen überwiegen. Absatz 3 gilt entsprechend. Die Übermittlung darf nur erfolgen, wenn die Empfänger sich gegenüber der übermittelnden Stelle verpflichten und die Gewähr dafür bieten, Maßnahmen entsprechend § 3 einschließlich der Geheimhaltung zu treffen, die Daten zu</u>	nicht möglich ist, mit pseudonymisierten Daten, erreicht werden kann. Unterbleiben kann die Anonymisierung oder ersatzweise die Pseudonymisierung nur, wenn sie nicht möglich oder im Einzelfall unverhältnismäßig ist.“ Abs. 2 (neu): „Die (Weiter)Verarbeitung allgemein zugänglicher Daten, z. B. bereits veröffentlichter Daten, wird für wissenschaftliche Forschungszwecke zugelassen. Ein Grund hiervon abzuweichen, besteht nur dann, wenn schutzwürdige Belange der betroffenen Person entgegenstehen, z. B. bei rechtswidrig erlangten, kompromittierenden Daten, Vorliegen eines Widerspruchs	Landeskrankenhausgesetz. Das dort bestehende Widerspruchsrecht ist zu beachten. Die vorgeschriebenen Maßnahmen werden als ausreichend erachtet. Der Empfänger ist, nachdem ihm die Daten unter Einhaltung der normierten Schutzmaßnahmen überlassen wurden, der Verantwortliche in Bezug auf die Einhaltung der Datenschutzanforderungen. Diesbezüglich unterliegt er ebenfalls der Datenschutzaufsicht. Der Verweis auf § 3 schließt die Geheimhaltungspflicht ein. Die gesetzliche Regelung der Verpflichtungen des Empfängers unterliegt nicht der Kompetenz des Landesgesetzgebers. Das
--	---	--	---

	<u>anonymisieren, sobald der Personenbezug für das Forschungsvorhaben nicht mehr erforderlich ist, die Daten nicht an Dritte weiterzugeben und der übermittelnden Stelle jederzeit auf Verlangen die Einhaltung dieser Verpflichtungen nachzuweisen.</u> (46) 1Die in Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der jeweiligen Forschungs- oder Statistikzwecke notwendig ist. 2Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU)	oder Daten, die unrechtmäßig veröffentlicht wurden. Die Informationspflicht kann unter den Voraussetzungen des Artikels 14 Absatz 5 Buchstabe b DSGVO und § 8 entfallen. Die Verarbeitung allgemein zugänglicher Daten kann die Entwicklung von KI-Anwendungen in der Forschung unterstützen. Für besondere Kategorien personenbezogener Daten gilt diesbezüglich Artikel 9 Absatz 2 Buchst. e DSGVO. Abs. 3 S. 2 (neu): „Die öffentliche Stelle muss gemäß Artikel 89 Absatz 1 DSGVO geeignete Garantien für die Rechte und Freiheiten der betroffenen Person treffen. Neben den in Absatz 3 genannten Maßnahmen der	Bundesdatenschutzgesetz regelt das Datenschutzrecht der nichtöffentlichen Stellen. Der Gemeinwohlbegriff ist in § 5 Absatz 1 Nummer 1 als gesetzlich anerkannte allgemeine öffentlichen Interessen definiert. Gemeinwohlorientierte Unternehmen sind daher solche, deren Forschung der Förderung dieser Interessen dient. Beispiele sind Forschung zur Bewältigung drängender sozialer und ökologischer Herausforderungen. Die KI-VO findet Anwendung, sofern ihr Anwendungsbereich eröffnet ist: Gemäß Artikel 2 Absatz 8 KI-VO gilt die KI-VO nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr gebracht
--	---	--	---

	2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.	Anonymisierung und Pseudonymisierung sind insbesondere Maßnahmen zu treffen, um sicherzustellen, dass die in Artikel 5 DSGVO dargelegten Grundsätze der Verarbeitung personenbezogener Daten eingehalten werden. Zu verweisen ist insbesondere auf die Grundsätze der Datenminimierung, der Richtigkeit sowie der Vertraulichkeit und Integrität von Daten. Beispiele zur Umsetzung dieser Grundsätze mittels technischer und organisatorischer Maßnahmen sind insbesondere § 3 zu entnehmen, der Artikel 32 Absatz 1 DSGVO konkretisiert; insbesondere ist an Verschlüsselung oder Zugangs- und Zutrittsbeschränkungen (z. B. Multi-Faktor-Authentisierung)	oder in Betrieb genommen werden. Solche Tätigkeiten werden im Einklang mit dem geltenden Unionsrecht durchgeführt. Maßgeblich ist danach vor allem die DSGVO. Absatz 5 dient dazu, eine datenschutzrechtliche Befugnis zur Übermittlung von Forschungsdaten zu begründen. Eine solche ist in der KI-VO nicht zu finden.
--	--	--	---

		sowie ein Rechte- und Rollenkonzept zu denken. Die Höhe der Schutzmaßnahmen muss der Schutzbedürftigkeit der personenbezogenen Daten entsprechen; im allgemeinen Datenschutzrecht ist daher die Festlegung spezifischer Maßnahmen nicht angezeigt. Die Maßnahmen sind in einem Datenschutzkonzept niederzulegen; der Datenschutzbeauftragte der öffentlichen Stelle ist zu beteiligen (vgl. Artikel 38 Absatz 1 DSGVO).“ Abs. 5 (neu): „Entscheidend für die Privilegierung der Forschung öffentlicher Stellen ist deren Verpflichtung auf das Gemeinwohl. Soweit privat finanzierte Forschung sich	
--	--	--	--

		ebenfalls dem Gemeinwohl verpflichtet, wird die Übermittlung personenbezogener Daten zu Forschungszwecken legitimiert. Das Gemeinwohl wird in § 5 Absatz 1 Nummer 1 definiert. [...] Sofern spezielle Übermittlungsregelungen bestehen, gehen diese als Lex Specialis den allgemeinen Regelungen des § 13 LDSG vor. Dies betrifft insbesondere im Hinblick auf Geheimhaltungspflichten für statistische Daten die Regelung in § 16 Absatz 6, 10 des Bundesstatistikgesetzes oder zur Übermittlung von Sozialdaten für die Forschung und Planung die spezielle Vorschrift des § 75 des Zehnten Buches Sozialgesetzbuch (SGB X) oder zur Forschung mit Patienten die	
--	--	--	--

		spezielle Regelung im Landeskrankenhausgesetz (LKHG).“	
§ 15 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen (1) 1 Personenbezogene Daten von Bewerberinnen und Bewerbern sowie Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich oder in einer Rechtsvorschrift,	§ 15 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen (1) 1 Personenbezogene Daten von Bewerberinnen und Bewerbern sowie Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich oder in einer Rechtsvorschrift,	Abs. 2 (S. 75): „Entsprechend dem Ergebnis der Evaluierung werden die Zwecke der Verarbeitung besonderer Kategorien personenbezogener Daten erweitert für die in Artikel 9 Absatz 2 Buchst. h DSGVO genannten Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin und der Beurteilung der Arbeitsfähigkeit der Beschäftigten, sofern die Verarbeitung auf einer rechtlichen Grundlage erfolgt. [...] Als rechtliche Grundlage für Maßnahmen zur Gesundheitsvorsorge kann auf die Dienstpflichten des Dienstherrn, die aus der Fürsorgepflicht folgen, verwiesen werden. Für	

einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist. 2Die Verarbeitung ist auch zulässig, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. (2) Besondere Kategorien personenbezogener Daten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit die Verarbeitung erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen oder der betroffenen Person, auch aufgrund von Kollektivvereinbarungen, auf dem	einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist. 2Die Verarbeitung ist auch zulässig, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. (2) Besondere Kategorien personenbezogener Daten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit die Verarbeitung erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen oder der betroffenen Person, auch aufgrund von Kollektivvereinbarungen, auf dem	Maßnahmen zur Aufrechterhaltung der körperlichen und psychischen Gesundheit der Beschäftigten kann es erforderlich sein, besondere Kategorien personenbezogener Daten, vor allem Gesundheitsdaten, zu erheben. [...]“ Abs. 6 (S. 76): „Absatz 6 wird zur Vermeidung von Missverständnissen klarer gefasst. Es wird ferner klargestellt, dass die erfassten Daten nur für die in Satz 1 genannten Zwecke verarbeitet werden dürfen. Darüber hinaus ergibt sich aus Artikel 25 DSGVO in Verbindung mit § 3 LDSG, dass dem Schutzbedürfnis der Daten entsprechende technische und organisatorische Maßnahmen zu	
--	--	--	--

Gebiet des Dienst- und Arbeitsrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes zu genügen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. (3) 1Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbezogener Daten einer Bewerberin oder eines Bewerbers bei dem bisherigen Dienstherrn oder Arbeitgeber nur zulässig, wenn die betroffene Person eingewilligt hat. 2Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherrn oder Arbeitgeber. (4) Auf die Verarbeitung von	Gebiet des Dienst- und Arbeitsrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes zu genügen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. <u>Besondere Kategorien personenbezogener Daten dürfen entsprechend Satz 1 auch verarbeitet werden, soweit die Verarbeitung für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin oder der Beurteilung der Arbeitsfähigkeit der Beschäftigten erforderlich ist und wenn diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht</u>	treffen sind. Insbesondere ist dafür zu sorgen, dass die biometrischen Daten nicht für andere Zwecke ausgelesen werden können.“ Abs. 9 (S. 76): Die Nutzung von KI bei der Verarbeitung personenbezogener Daten in Dienst- und Arbeitsverhältnissen kann sowohl die Einstellung und Auswahl von Personen als auch die Durchführung oder Beendigung bestehender Beschäftigungsverhältnisse betreffen. Erwähnt seien Lebenslauf-Parsing, Online-Assessments, mittels derer eine Auswahl unter Bewerberinnen und Bewerbern getroffen wird. Diese Nutzung von KI bringt spezifische Gefahren mit sich, indem statt von	
--	--	---	--

Personalaktendaten von Arbeitnehmerinnen und Arbeitnehmern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamtinnen und Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor. (5) Zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht	<u>unterliegen, oder unter deren Verantwortung verarbeitet werden.</u> (3) Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbezogener Daten einer Bewerberin oder eines Bewerbers bei dem bisherigen Dienstherrn oder Arbeitgeber nur zulässig, wenn die betroffene Person eingewilligt hat. 2 Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherrn oder Arbeitgeber. (4) Auf die Verarbeitung von Personalaktendaten von Arbeitnehmerinnen und Arbeitnehmern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die	einem Menschen von einer Maschine aufgrund eines Algorithmus Festlegungen getroffen werden, die zum Nachteil einer bestimmten Person ausfallen können und sich auf Entscheidungen auswirken. Dementsprechend gehören KI-Systeme, die für Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit eingesetzt werden, nach Artikel 6 Absatz 2 KI-VO in Verbindung mit Nummer 4 des Anhangs III zur KI-VO zu den Hochrisiko-Systemen. Eine Ausnahme besteht nach Artikel 6 Absatz 3 KI-VO lediglich, wenn das KI-System kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, so z. B. bei ausschließlich	
--	---	--	--

begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat oder schwerwiegende Pflichtverletzung begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. (6) Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, die betroffene Person hat ausdrücklich eingewilligt oder sie ist durch Dienst- oder Betriebsvereinbarung geregelt und	für Beamtinnen und Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor. (5) Zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat oder schwerwiegende Pflichtverletzung begangen hat, die Verarbeitung zur Aufdeckung	vorbereitenden Aufgaben. Die Einstufung als nicht hochriskant ist im Beschäftigtenkontext wegen des bestehenden Abhängigkeitsverhältnisses nur in Ausnahmefällen anzunehmen. Für Hochrisiko-Systeme sieht die KI ein Risikomanagementsystem vor, mit dem den wesentlichen Risiken begegnet werden muss (vgl. Artikel 9 KI-VO). Als Risiko gelten Gefahren für die Grundrechte betroffener Personen, im Besonderen die Gefahr von Diskriminierung. Entsprechend Artikel 88 Absatz 2 DSGVO ist für Regelungen im Beschäftigtenverhältnis insbesondere für Transparenz zu sorgen. Ergänzend zu den Informationspflichten nach der KI-	
--	--	---	--

für die Datenverarbeitung besteht jeweils ein dringendes dienstliches Bedürfnis. (7) 1Eine Überwachung von Beschäftigten mit Hilfe optisch-elektronischer Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig. 2Absatz 5 bleibt unberührt. 3Für sonstige technische Einrichtungen gilt Absatz 1 entsprechend; die öffentliche Stelle muss geeignete Maßnahmen treffen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. (8) 1Beschäftigte sind alle bei öffentlichen Stellen beschäftigten Personen unabhängig von der Rechtsform des	erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. (6) Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, die betroffene Person hat ausdrücklich eingewilligt oder sie ist durch Dienst- oder Betriebsvereinbarung geregelt und für die Datenverarbeitung besteht jeweils ein dringendes dienstliches Bedürfnis. Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und	VO und der DSGVO wird daher als gesetzliche Pflicht konstituiert, die Beschäftigten sowie die Bewerberinnen und Bewerber über den Einsatz von KI-Systemen, ihre Dauer und ihre Zwecke zu unterrichten. Artikel 22 DSGVO verbietet öffentlichen Stellen unabhängig von der KI-VO, einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Artikel 22 DSGVO gilt für die Anwendung von KI im Beschäftigtenverhältnis uneingeschränkt. Die Regelungen der KI-VO stellen keine Ausnahmeregelung im	
--	--	--	--

Beschäftigungsverhältnisses. 2Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.	<u>Autorisierungszwecken ist untersagt, es sei denn, die Verarbeitung ist durch Dienst- oder Betriebsvereinbarung geregelt oder die betroffene Person hat ausdrücklich eingewilligt und für die Erreichung der Zwecke steht in beiden Fällen kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung. Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.</u> (7) 1Eine Überwachung von Beschäftigten mit Hilfe optisch-elektronischer Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig. 2Absatz 5 bleibt unberührt. 3Für sonstige technische Einrichtungen gilt Absatz 1 entsprechend; die öffentliche Stelle muss geeignete Maßnahmen treffen, um	Sinne des Artikels 22 Absatz 2 Buchst. b DSGVO dar. Dies verbietet, dass Personalentscheidungen ausschließlich durch KI getroffen werden ebenso wie Profiling. Letzteres wird in Artikel 4 Nummer 4 DSGVO definiert als automatisierte Verarbeitung personenbezogener Daten, die persönliche Aspekte bewertet, insbesondere indem sie die Arbeitsleistung, die Gesundheit, die Interessen, Zuverlässigkeit oder Verhalten analysiert und vorhersagt. Es ist zu verlangen, dass ein überprüfender Mensch einen Entscheidungsspielraum haben muss, die Computer-Entscheidung zu ändern (vgl. BeckOK DatenschutzR/von Lewinski, 49. Ed. 1.8.2024, DSGVO Art. 22 Rn. 23-25.2).“	
---	--	---	--

	sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. (8) 1Beschäftigte sind alle bei öffentlichen Stellen beschäftigten Personen unabhängig von der Rechtsform des Beschäftigungsverhältnisses. 2Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt. <u>(9) Die Beschäftigten sowie die Bewerberinnen und Bewerber sind über den Einsatz von KI-Systemen, die Dauer von deren Einsatz und deren Zwecke zu unterrichten.</u>		
§ 16 Öffentliche Auszeichnungen und Ehrungen	§ 16 Öffentliche Auszeichnungen und Ehrungen	S. 77: „In Ergänzung zur bisherigen	

(1) Zur Entscheidung über öffentliche Auszeichnungen und Ehrungen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten verarbeitet werden; die öffentlichen Stellen sind insofern nicht zur Informations- und Auskunftserteilung gemäß Artikel <u>13</u> bis <u>15</u> der Verordnung (EU) 2016/679 verpflichtet. (2) Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden, es sei denn, sie werden für protokollarische Zwecke benötigt.	(1) Zur Entscheidung über öffentliche Auszeichnungen und Ehrungen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten verarbeitet werden; die öffentlichen Stellen sind insofern nicht zur Informations- und Auskunftserteilung gemäß Artikel <u>13</u> bis <u>15</u> der Verordnung (EU) 2016/679 verpflichtet. <u>Satz 1 findet keine Anwendung, wenn der datenverarbeitenden Stelle bekannt ist, dass die betroffene Person ihrer öffentlichen Auszeichnung oder Ehrung oder der mit ihr verbundenen Datenverarbeitung widersprochen hat.</u> (2) Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden, es sei denn, sie werden	Regelung der Entscheidung über öffentliche Auszeichnungen und Ehrungen wird klargestellt, dass ein bekannter Widerspruch der betroffenen Person eine entsprechende Datenverarbeitung verbietet. Dies gebietet es nicht, dass die öffentliche Stelle vorher entsprechende Erkundigungen einholt. Es ist wie bisher nicht erforderlich, dass die betroffene Person zustimmt.“	
---	---	---	--

	für protokollarische Zwecke benötigt.		
§ 17 Verarbeitung personenbezogener Daten im öffentlichen Interesse (1) 1Für 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. 2Besondere Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und	§ 17 Verarbeitung personenbezogener Daten im öffentlichen Interesse (1) 1Für 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. 2Besondere Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und	S. 77: „Gemäß Artikel 9 Absatz 2 Buchst. g DSGVO verlangt die Verarbeitung besonderer Kategorien personenbezogener Daten im erheblichen öffentlichen Interesse eine gesetzliche Regelung, die den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsieht. [...]“	Aus dem Anhörungsverfahren (S. 50): „Entgegen der Auffassung des LfDI ist die Vorschrift des § 17 nicht als Generalklausel, sondern auf der Grundlage des Artikels 9 Absatz 2 Buchstabe g als Auffangtatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten konzipiert, falls eine bereichsspezifische Rechtsgrundlage nicht zur Verfügung steht (vgl. Begründung in der Landtagsdrucksache 16/3930, S. 106).“

Straftaten oder damit zusammenhängende Sicherungsmaßnahmen dürfen nur aufgrund einer ausdrücklichen Einwilligung verarbeitet werden. (2) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses oder zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist und die Interessen der öffentlichen Stelle an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.	Straftaten oder damit zusammenhängende Sicherungsmaßnahmen dürfen nur aufgrund einer ausdrücklichen Einwilligung verarbeitet werden. (2) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses oder zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist und die Interessen der öffentlichen Stelle an der Datenverarbeitung die Interessen der betroffenen Person überwiegen. <u>Die öffentliche Stelle trifft angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und</u>		
---	--	--	--

	<u>Interessen der betroffenen Person; hierfür sind mindestens die Maßnahmen nach § 3 Absatz 1 Nummern 1 bis 3 zu treffen.</u>		
	§ 17a Absicherung des Zugangs zu personenbezogenen Daten (1) Für die Überprüfung der Zuverlässigkeit von Besuchern, Mitarbeitern von Unternehmen und anderen Organisationen sowie sonstigen Personen, die in sicherheits- oder sicherheitstechnisch relevante Bereiche gelangen sollen, für die öffentliche Stellen Verantwortung tragen, gilt § 15 Absatz 1 Satz 1 entsprechend mit der Maßgabe, dass zusätzlich die Einwilligung der betroffenen Person erforderlich ist. Besondere	S. 77 ff.: „Für die spezifische Verarbeitung personenbezogener Daten im Rahmen von Maßnahmen zum Schutz der Informations- und Cybersicherheit wird eine eigene Ermächtigungsgrundlage geschaffen und zusammen mit dem bisherigen § 17 Absatz 1 LDSG in einer Norm zusammengefasst. Absatz 1 entspricht unverändert § 17 Absatz 1 LDSG alter Fassung. Zu Absatz 2 Als Ergebnis der Evaluierung	

	Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen 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	wurde der Bedarf erkannt, personenbezogene Daten für Maßnahmen zu verarbeiten, die zur Gewährleistung der Informationssicherheit, der Cybersicherheit oder des Funktionierens kritischer Infrastruktur erforderlich sind, wenn außenstehende Personen Zugang zu den relevanten Anlagen haben. Neben der Verarbeitung zu Authentifizierungszwecken kann es beispielsweise für ein Sicherheitsaudit, für Schulungs- oder Sensibilisierungsmaßnahmen erforderlich sein, personenbezogene Daten der genannten Personen zu verarbeiten, insbesondere zu erheben oder zu übermitteln. Die Informationssicherheit ist in § 2	
--	--	---	--

	Infrastruktur erforderlich ist. Die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, dass die betroffene Person ausdrücklich einwilligt und kein gleichermaßen geeignetes Mittel mit geringerer Eingriffstiefe zur Verfügung steht; zu anderen Zwecken dürfen die Daten nicht verarbeitet werden.	Absatz 9 Cybersicherheitsgesetz (CSG) definiert; sie umfasst alle technischen und nichttechnischen Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Cybersicherheit umfasst nach § 2 Absatz 11 CSG alle Aspekte der Sicherheit in der Informationstechnik und den Schutz gesellschaftlich relevanter Prozesse vor Angriffen im gesamten Cyberraum. Entsprechend der Regelung für Beschäftigte wird die Verarbeitung biometrischer Daten für Authentifizierungs- und Autorisierungszwecke geregelt: Sie ist im Hinblick auf die erhöhten Gefahren, die von der Verarbeitung biometrischer Daten ausgehen, nur mit ausdrücklicher Zustimmung der betroffenen	
--	---	---	--

		Person und als Ultima Ratio zulässig. Denn im Gegensatz zu Kennwörtern können biometrische Daten nicht zurückgesetzt werden, bieten aber andererseits einen höheren Schutz vor unbefugtem Zugang als jene. Der Unterschied zu Absatz 1 besteht in der Anwendung auf Personen, die bereits (physischen) Zugang zu den genannten Datenverarbeitungsanlagen haben und der engeren Zweckbestimmung. Die Verarbeitung besonderer Kategorien personenbezogener Daten wird in der Regel nicht erforderlich sein; ansonsten ist sie ggf. auf § 17 zu stützen oder es ist eine Einwilligung einzuholen. Für Beschäftigte kommt § 15 zur Anwendung, da diese nicht Dritte	
--	--	---	--

		sind. In Bezug auf Videoüberwachung ist gegebenenfalls § 18a zusätzlich anzuwenden.“	
	§ 17b Öffentlichkeitsarbeit (1) Soweit der öffentlichen Stelle ein Auftrag zur politischen Bildung oder zur Bürgerinformation obliegt, dürfen öffentliche Stellen unbeschadet sonstiger Bestimmungen personenbezogene Daten verarbeiten, um die Bürgerinnen und Bürger in angemessener Weise über ihre Arbeit zu informieren einschließlich werblicher Zwecke, sofern die schutzwürdigen Interessen betroffener Personen dem nicht entgegenstehen. In der Regel sind hiernach im erforderlichen Umfang insbesondere die	S. 78 ff.: „Öffentliche Stellen benötigen rechtssichere Grundlagen für die Öffentlichkeitsarbeit. Kaum eine öffentliche Stelle kommt mehr ohne öffentlichen Auftritt aus, sei es mittels Informationsveranstaltungen, Informationsbroschüren oder in sozialen Medien. Regelmäßig werden hierfür personenbezogene Daten benötigt. Bisher wird für die datenschutzrechtliche Legitimation die Generalklausel des § 4 LDSG bemüht. Diese vermag aber keine Auskunft darüber zu geben, welche Art der Öffentlichkeitsarbeit	Aus dem Anhörungsverfahren (S. 50): „Als spezielles Gesetz geht das Landeshochschulgesetz, soweit es die Öffentlichkeitsarbeit regelt, gemäß § 1 Absatz 3 LDSG vor. Dort ist kein Widerspruchsrecht normiert. Vorrangig zum LHG gilt jedoch das KunstUrhG, das für Abbildungen außer in den in § 23 genannten Fällen die Einwilligung der abgebildeten Person voraussetzt. Sofern daneben noch § 15 LDSG zur Anwendung kommt, dürfen Beschäftigtendaten nur für die Durchführung des Beschäftigtenverhältnisses im erforderlichen Umfang verarbeitet

	Fertigung von Bild- und Tonaufnahmen von Veranstaltungen und deren Verbreitung, die Verwendung von Kontakt- und Adressdaten für Kontaktpflege und Einladungen zu Veranstaltungen einschließlich deren Organisation zulässig. Die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen und deren Verbreitung unterliegt den Schranken der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266,	zulässig ist. Deshalb soll in der Praxis mit § 17a mehr Sicherheit gegeben werden bezüglich dessen, was zu welchem Zweck zulässig ist. Es ist jedenfalls zu beachten, dass auch im Rahmen der Öffentlichkeitsarbeit alle datenschutzrechtlichen Grundsätze, insbesondere die aus Artikel 5 DSGVO, gelten. Grundsätzlich ist die Öffentlichkeitsarbeit durch einen verfassungsrechtlichen oder gesetzlichen Auftrag zur politischen Bildung, zur Information der Bürgerinnen und Bürger verfassungsrechtlich gerechtfertigt und sorgt für Transparenz staatlichen Handelns für die Zivilgesellschaft. Dabei wird von einer objektiv gehaltenen Information der Öffentlichkeit ausgegangen. Dieser	werden. Inwieweit dies für die Öffentlichkeitsarbeit zutrifft, muss im Einzelfall bestimmt werden.“
--	--	---	--

	280) geändert worden ist, in der jeweils geltenden Fassung. (2) Den betroffenen Personen ist Gelegenheit zum Widerspruch ohne Angabe von Gründen zu geben.	verfassungsrechtliche Auftrag ist in Einklang zu bringen mit dem informationellen Selbstbestimmungsrecht des Einzelnen, selbst über die Verwendung seiner Daten zu bestimmen. Die jeweilige Schutzbedürftigkeit der Adressatengruppe ist zu berücksichtigen; dies erfordert insbesondere im Hinblick auf Minderjährige besondere Prüfpflichten. Mit der gesetzlichen Regelung wird die Eingriffsschwelle bestimmt, ab der zur Verarbeitung personenbezogener Daten die Einwilligung der betroffenen Person erforderlich ist. Hierbei wird in Bezug auf die Angemessenheit auch berücksichtigt, was	
--	--	---	--

		vernünftigerweise von Personen, die öffentliche Dienste in Anspruch nehmen oder sich in öffentlichen Kanälen informieren, erwartet wird und deshalb davon auszugehen ist, dass voraussichtlich keine Einwendungen gegen die Verarbeitung bestehen. Vorausgesetzt wird, dass nur Mittel eingesetzt werden, die zum Zweck der Öffentlichkeitsarbeit erforderlich sind, das heißt nur in erforderlichem Umfang von der Ermächtigung Gebrauch gemacht wird. Legitimer werblicher Zweck kann die Nachwuchswerbung öffentlicher Stellen sein. Zu den in der Regel legitimen Mitteln der Öffentlichkeitsarbeit gehören und werden explizit ohne	
--	--	---	--

		Anspruch auf Vollständigkeit aufgezählt: die Fertigung von Bild- und Tonaufnahmen von Veranstaltungen (z. B. Streaming) und deren Verbreitung, die Verwendung von Kontakt- und Adressdaten für Kontaktpflege und Einladungen zu Veranstaltungen einschließlich deren Organisation. Die Zusendung von Newslettern gehört nicht zur Kontaktpflege und bedarf der Einwilligung. Die Zulassung der Verarbeitung personenbezogener Daten zum Zweck der Öffentlichkeitsarbeit erfolgt unbeschadet sonstiger Bestimmungen. Daher sind zumindest die Schranken der Fertigung von Bild, Film- und Tonaufnahmen während Veranstaltungen (Fotografie und Live-Streaming) und deren	
--	--	---	--

		Verbreitung nach §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) zu beachten. Wegen der Strafbarkeit nach § 33 KunstUrhG erfolgt die Aufnahme in den Gesetzestext. Zu beachten ist insbesondere, dass Personen nur als Beiwerk erscheinen dürfen. Die Nutzung sozialer Medien wird in Satz 2 nicht explizit erwähnt, da sie jeweils genauer Prüfung bedarf, ob ihr Einsatz nach Satz 1 gerechtfertigt ist. Die Nutzung sozialer Medien hat insbesondere die zu Facebook ergangene Rechtsprechung des Europäischen Gerichtshofs zu beachten. In einem richtungsweisenden Urteil hat der Europäische Gerichtshof im Jahr	
--	--	---	--

		2018 entschieden, dass Betreiber von Fanpages auf Facebook gemeinsam mit Facebook als Dienstanbieter für den Schutz der Nutzerdaten verantwortlich sind. Für die gemeinsame Verantwortlichkeit legt Artikel 26 DSGVO die zu beachtenden Pflichten fest. Für sonstige soziale Medien sind ebenfalls die Voraussetzungen einer gemeinsamen Verantwortlichkeit nach Artikel 26 DSGVO zu prüfen. Die Prüfung der Tatbestandsvoraussetzungen des Artikels 26 DSGVO entscheidet darüber, ob eine gemeinsame Verantwortlichkeit anzunehmen ist und wie weit diese reicht. Da die Voraussetzungen der Nutzung sozialer Medien von den Vorgaben der DSGVO bestimmt	
--	--	---	--

		werden, muss eine Regelung zur Verantwortlichkeit im LDSG unterbleiben. Zur Orientierung kann die Broschüre des LfDI „Wesentliche Anforderungen an die behördliche Nutzung Sozialer Netzwerke“ dienen. Zu Absatz 2 Zur Wahrung des Rechts auf Datenschutz ist den betroffenen Personen Gelegenheit zum Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten zu geben, und zwar ohne die Angabe von Gründen. In diesem Fall unterbleibt die Verarbeitung. Auf das Widerspruchsrecht ist hinzuweisen.“	
§ 18 Videoüberwachung öffentlich zugänglicher Räume	§ 18 <u>VideoüberwachungVideoschutz</u>	S. 79 ff.:	Im Anhörungsverfahren

(1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, 1.um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder 2.um Kulturgüter, öffentliche	öffentlich zugänglicher Räume (1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, 1.um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder	Abs. 1 S. 1 (neu): „In § 18 Absatz 1 Satz 1 wird die Beschränkung auf den Schutz bestimmter Objekte und Personen aufgehoben. Gemäß Artikel 6 Absatz 1 Buchstabe e DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie für die Erfüllung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Umfasst sind Aufgaben, die in der Zuständigkeit der jeweiligen öffentlichen Stelle liegen. Maßgebend sind die spezifischen Bestimmungen der Aufgabennorm. Die Videoüberwachung muss für die Erfüllung der öffentlichen Aufgabe erforderlich sein; sie braucht aber nicht die eigentliche Aufgabenerfüllung darzustellen. Sofern die Videoüberwachung die	aufgegriffen: Bedenken gegen die Vereinbarkeit des Satzes 2 in Absatz 2 des Anhörungsentwurfs hinsichtlich Vereinbarkeit mit Art. 13: „Zudem ist auf die Möglichkeit hinzuweisen, die weiteren Informationen nach Artikel 13 der Verordnung (EU) 2016/679 vom Verantwortlichen zu erhalten.“ Unser Vorschlag wurde vollständig übernommen: „Zudem ist darauf hinzuweisen, wo die weiteren Informationen des Verantwortlichen nach Artikel 13 der Verordnung (EU) 2016/679 verfügbar sind.“ S. 52: „Die neu eingeführte Fiktion der
--	---	---	---

Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. (2) Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen; dabei ist der Verantwortliche mitzuteilen. (3) Für einen anderen Zweck dürfen die Daten nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur	2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. <u>(1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall</u>	Aufgabenerfüllung unterstützen kann, kann ihr Einsatz zulässig sein. Zu betonen ist aber, dass weiterhin die Erforderlichkeit im Einzelfall gegeben sein muss, also eine konkrete oder abstrakte Gefahrenlage vorliegen muss, was die regelmäßige Anwendung ausschließt. Sofern optisch-elektronische Systeme regelmäßig eingesetzt werden sollen, bedarf es einer spezialgesetzlichen Grundlage. [...] Vorrangig bleiben fachgesetzliche Regelungen. Diese bleiben nach dem Wesentlichkeitsgrundsatz erforderlich, wenn die Videoüberwachung besonders eingriffsintensiv ist. Wegen des als Ausprägung des allgemeinen Persönlichkeitsrechts verfassungsrechtlich verbürgten	Angemessenheit der Videoüberwachung für bestimmte als besonders sicherheitsrelevant eingestufte Objekte führt eine abstrakt-generelle Bewertung der Videoüberwachung als angemessenes Mittel ein. Sie soll die öffentlichen Stellen entlasten, eine Vorrangprüfung auch in Fällen vorzunehmen, in denen Videoüberwachung letztlich das wirksamste Schutzmittel ist, das heißt kein gleich geeignetes milderer Mittel zur Verfügung steht. Wenn Videoüberwachung als ein wirksames Mittel für die Gefahrenabwehr betrachtet wird, wie in der Regelung des § 18 zum Ausdruck kommt, und der Einsatz sichergestellt werden
--	---	--	--

Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist. (4) 1 Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, besteht die Pflicht zur Information der betroffenen Person über diese Verarbeitung nach Artikel 13 und 14 der Verordnung (EU) 2016/679. 2 § 8 gilt entsprechend. (5) Die Videoaufzeichnungen und daraus gefertigte oder sich auf die Videoüberwachung beziehende Unterlagen sind unverzüglich, spätestens jedoch vier Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von	<u>erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Der Schutz von Leben, Gesundheit und Freiheit von Personen ist ein besonders wichtiges öffentliches Interesse. Sofern die Videoüberwachung zum Schutz von sicherheitsrelevanten Einrichtungen, Dienstgebäuden, Dienstfahrzeugen, Kulturgütern oder öffentlichen Verkehrsmitteln und den dort oder in unmittelbarer Nähe jeweils befindlichen Personen und Sachen erforderlich ist, gilt Videoüberwachung als angemessen und verhältnismäßig.</u> (2) Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen; dabei ist	Grundrechts auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes muss die Anwendung der Vorschrift nach dem Verhältnismäßigkeitsprinzip erfolgen. Es ist jeweils zu prüfen, ob die Maßnahme der Videoüberwachung, geeignet, erforderlich und angemessen ist. Dies kommt in der Vorschrift hinreichend zum Ausdruck, indem auf den Einzelfall und die Erforderlichkeit abgestellt wird, außerdem eine Abwägung mit den schutzwürdigen Interessen der betroffenen Personen erfolgen muss. “ Abs. 1 S. 2 (neu): „Satz 2 soll klarstellen, dass der Schutz von Leben, Freiheit und Gesundheit von Personen, die	soll, ist es angezeigt, dies die Mittelauswahl betreffend gesetzgeberisch zum Ausdruck zu bringen. Die Annahme der Angemessenheit bleibt aber beschränkt auf die Fälle, in denen der Videoschutz erforderlich ist, also bei der nachweisbaren erheblichen Gefährdung hochwertiger Schutzgüter. Maßnahmen mit geringerer Eingriffstiefe sind damit nicht ausgeschlossen und können ebenfalls eingesetzt werden. Die Einhaltung der Datenschutzgrundsätze und der Schutz nicht beteiligter Personen durch technische Maßnahmen, wird außerdem vorausgesetzt. Die Auflistung der Objekte, für die das Mittel der Videoüberwachung als
---	---	--	--

Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden. (6) Öffentliche Stellen haben ihren jeweiligen Datenschutzbeauftragten unbeschadet des Artikels 35 Absatz 2 der Verordnung (EU) 2016/679 rechtzeitig vor dem erstmaligen Einsatz einer Videoüberwachungseinrichtung den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen und ihm Gelegenheit zur Stellungnahme zu geben.	der Verantwortliche mitzuteilen. <u>Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen; dabei sind mindestens der Verantwortliche mitsamt seinen Kontaktdaten sowie die Kontaktdaten des behördlichen Datenschutzbeauftragten mitzuteilen. Zudem ist darauf hinzuweisen, wo die weiteren Informationen des Verantwortlichen nach Artikel 13 der Verordnung (EU) 2016/679 verfügbar sind.</u> (3) Für einen anderen Zweck dürfen die Daten nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Ordnungswidrigkeiten von	sich im Bereich der nach Satz 1 geschützten Objekte aufhalten, für die Videoüberwachung ein besonders wichtiges öffentliches Interesse ist.“ Abs. 1 S. 3 (neu): „[...] Es wird daher gesetzlich die Verhältnismäßigkeit im engeren Sinn, damit im Besonderen die Angemessenheit der Videoüberwachung als Mittel zum Schutz der genannten Objekte festgestellt.“ Abs. 2 (neu) „Der Umfang der Informationspflicht ergibt sich grundsätzlich aus Artikel 13 DSGVO. Mindestens die Kontaktdaten müssen erkennbar sein. Für die weiteren Informationen, z. B. über den	angemessen bewertet wird, ist bewusst beschränkt auf sicherheitsrelevante und kulturell bedeutsame Objekte. Im Übrigen bedarf es einer Abwägung im Einzelfall. Schließlich stellt Videoüberwachung einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, der nur zulässig ist, wenn er verhältnismäßig ist. Außerdem dient Videoüberwachung nach § 18 nicht der Kriminalitätsbekämpfung.“ S. 53: „Die Speicherfrist von zwei Monaten stellt die maximale Speicherdauer dar, die nur ausnahmsweise angemessen ist. Im Einzelfall kann sie aber
---	---	---	---

	erheblicher Bedeutung oder von Straftaten <u>oder zur Geltendmachung von Rechtsansprüchen</u> erforderlich ist. (4) 1 Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, besteht die Pflicht zur Information der betroffenen Person über diese Verarbeitung nach Artikel 13 und 14 der Verordnung (EU) 2016/679. 2§ 8 gilt entsprechend. (54) Die Videoaufzeichnungen und daraus gefertigte oder sich auf die Videoüberwachung beziehende Unterlagen sind unverzüglich, spätestens jedoch <u>vier Wochen</u> <u>zwei Monate</u> nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von	Zweck der Videoüberwachung und die Speicherdauer, muss erkennbar sein, wo diese verfügbar sind. Die Informationspflicht kann beispielsweise durch Anbringung eines QR-Codes mit Bereitstellung der Information an der angegebenen URL oder der Angabe einer Webseite erfüllt werden. Piktogramme mit der Möglichkeit, die erforderlichen Hinweise aufzunehmen, sind verfügbar. Es sollte auch möglich sein, die Informationen in Textform zu erhalten.“ Abs. 3: „Zur Klarstellung wird zur Kongruenz mit dem bisherigen Absatz 5 die Weiterverarbeitung zur Verfolgung von Rechtsansprüchen	erforderlich sein. Der besonderen Begründungspflicht wird zugestimmt. Der LfDI selbst führt hierfür Ferien und Urlaubszeiten an. Ein ausreichender Schutz der Daten durch organisatorische und technische Maßnahmen minimiert den Grundrechtseingriff.“
--	--	--	--

	Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden. (65) Öffentliche Stellen haben ihren jeweiligen Datenschutzbeauftragten unbeschadet des Artikels 35 Absatz 2 der Verordnung (EU) 2016/679 rechtzeitig vor dem erstmaligen Einsatz einer Videoüberwachungseinrichtung den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen und ihm Gelegenheit zur Stellungnahme zu geben. <u>(6) Videoüberwachung öffentlich zugänglicher Räume unter Nutzung von KI-Systemen ist</u>	aufgenommen.“ Abs. 4: „Die bisherige maximale Speicherdauer von vier Wochen wird entsprechend den Regelungen in Bayern, Rheinland-Pfalz und Sachsen auf zwei Monate ausgedehnt. Die maximale Speicherdauer soll im Spannungsverhältnis der präventiven Gefahrenabwehr beziehungsweise des staatlichen Interesses an Strafverfolgung und des grundrechtlich verbürgten Schutzes der betroffenen Personen, die keinen Anlass für die Videoüberwachung gegeben haben, die Grenze des verfassungsrechtlich Zulässigen gesetzlich regeln. Grundsätzlich verbleibt es bei der Pflicht,	
--	---	---	--

	<u>zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, um</u> <u>1. Leib oder Leben von Personen zu schützen, oder</u> <u>2. den Erhaltungszustand und die Funktionsfähigkeit des Eigentums öffentlicher Stellen und zu öffentlichen Zwecken gewidmeter Gegenstände zu überwachen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Absätze 2 bis 5 gelten entsprechend.</u>	Videoaufzeichnungen zu löschen, sobald feststeht, dass diese für die aufgeführten Zwecke nicht mehr benötigt werden. Für die Auswertung der Videoüberwachung im Hinblick auf relevante Vorkommnisse einschließlich des Geschehens davor und danach bedarf es aber einer ausreichenden maximalen Speicherdauer. Es sollte außerdem gewährleistet sein, dass im Fall von aufgezeichneten Tötlichkeiten (z. B. in öffentlichen Verkehrsmitteln) die Videoaufzeichnungen noch zur Verfügung stehen, wenn erst nach Ablauf von vier Wochen Anzeige erstattet wird. Dies gebietet der in Absatz 1 herausgestellte Schutz von Leben, Gesundheit und Freiheit der geschützten Personen. Ferner ist nach der	
--	--	--	--

		Neuregelung in Absatz 1 Satz 2 und 3 zu erwarten, dass Videoüberwachung häufiger als präventives Mittel der Gefahrenabwehr eingesetzt werden wird und mehr strafrechtlich relevante Vorfälle erkannt werden, die zu bearbeiten sind. Eine sorgfältige Auswertung, für die qualifiziertes Fachpersonal erforderlich sein wird, kann diesbezüglich mehr als vier Wochen benötigen. Durch eine längere Speicherfrist wird die Verhältnismäßigkeit der Datenspeicherung nicht infrage gestellt, wenn dies im Einzelfall zur Auswertung der Videoaufzeichnungen zum Zweck der Strafverfolgung einschließlich der Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder zur	
--	--	--	--

		Geltendmachung von Rechtsansprüchen erforderlich ist und technisch-organisatorische Maßnahmen (wie z. B. Zugriffsbeschränkungen, sichere Speicherung) den Eingriff minimieren. Höchstspeicherdauer heißt aber auch weiterhin: Im konkreten Fall kann – und wird in der Regel – die rechtlich zulässige Frist der Speicherung deutlich kürzer sein. Werden die Videoaufzeichnungen durchgesehen und keine Vorkommnisse festgestellt, die für die genannten Zwecke der Gefahrenabwehr oder der Strafverfolgung relevant sind, so sind die Daten umgehend zu löschen.“ Abs. 6 (neu)	
--	--	--	--

		„Zu Absatz 6 Nummer 1 In Nummer 1 wird Videoüberwachung unter Nutzung von KI-Systemen ermöglicht, soweit dies erforderlich ist, um Leib oder Leben von Personen zu schützen. Ein Anwendungsbeispiel könnte die KI-basierte Videoüberwachung in öffentlichen Schwimmbädern zur Vermeidung von Ertrinkungsunfällen sein. Zu Absatz 6 Nummer 2 Des Weiteren kann Videoüberwachung unter Nutzung von KI-Systemen nützlich sein, um den Erhaltungszustand und der Funktionsfähigkeit von Bauten, Anlagen u. ä. in öffentlicher Nutzung zu überwachen. Hierbei kommen zunehmend KI-Systeme zum	
--	--	--	--

		Einsatz. Dabei ist die Verarbeitung personenbezogener Daten häufig unvermeidlich; sie ist aber nicht der Zweck der Videoüberwachung. Zu nennen sind hier exemplarisch die Pflege und Wartung öffentlicher Einrichtungen und Infrastruktur (z. B. Straßen, Brücken, Elektrizitätswerke, Wasserwerke) oder der Einsatz in der staatlichen oder kommunalen Bauwirtschaft, sofern diese öffentlich zugänglich sind. Neben § 3a wird hiermit klarstellend auch die Nutzung von KI-Systemen zu dem genannten Zweck zugelassen, wenn damit die Verarbeitung personenbezogener Daten verbunden ist. Dies betrifft überwiegend Personen, die sich zufällig in den überwachten	
--	--	--	--

		Räumen aufhalten, deren Identität aber wie bei der Videoüberwachung keine Rolle spielt. Auch hier wird mit der Zulassung im Einzelfall das Bestehen einer Gefahrenlage vorausgesetzt, wobei das Bestehen einer konkreten oder abstrakten Gefahr, z. B. der Materialermüdung, des Diebstahls oder des Vandalismus ausreicht. Der Eingriff sollte dann auch zeitlich und räumlich auf die Abwendung der Gefahr beschränkt werden. Möglich wäre es z. B., die Videoüberwachung durchzuführen, wenn nicht mit der Anwesenheit von Personen zu rechnen ist.“	
	§ 18a Videoüberwachung nicht öffentlich zugänglicher Räume Die Videoüberwachung nicht	S. 83: „[...] Maßstab für ihre Zulässigkeit ist wie für die Videoüberwachung	

	öffentlich zugänglicher Räume einschließlich der Nutzung von KI-Systemen zur Überwachung des Erhaltungszustands und der Funktionsfähigkeit des Eigentums öffentlicher Stellen und zu öffentlichen Zwecken gewidmeter Gegenstände ist entsprechend § 18 Absatz 6 zulässig. Der Schutz beschäftigter oder sich im Überwachungsbereich aufhaltender Personen ist durch technische und organisatorische Maßnahmen so weit wie möglich zu gewährleisten; § 15 Absätze 5, 7 und 9 gelten entsprechend.	in öffentlich zugänglichen Räumen in § 18 Absatz 6 ihre Erforderlichkeit im Einzelfall zur Überwachung des öffentlichen Eigentums und zu öffentlichen Zwecken gewidmeter (beweglicher und unbeweglicher) Gegenstände im Hinblick auf Erhaltungszustand und Funktionsfähigkeit. Gedacht werden kann an umzäunte Baustellen, Gasversorgung, Elektrizitäts- und Wasserwerke in umfriedetem Gelände, Serverräume, Geräte in Forschungseinrichtungen oder allgemein an die Nutzung von KI-Systemen im Gebäudemanagement. Mit der Videoüberwachung kann ebenso Vandalismus und Diebstahl vorgebeugt werden. Die Identifizierung von Personen	
--	---	--	--

		kommt nur unter den Voraussetzungen des § 18 Absatz 3 in Betracht. Die Videoüberwachung ist in § 18 LDSG für öffentlich zugängliche Räume geregelt und berücksichtigt die an diesen Orten bestehende Gefährdungslage für den Schutz von Personen und Objekten auf der einen Seite und das Recht auf informationelle Selbstbestimmung auf der anderen Seite, die gegeneinander abzuwägen sind. Die Videoüberwachung im öffentlichen Raum erfasst überwiegend unbekannte Personen, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff in ihr informationelles Selbstbestimmungsrecht durch ihr	
--	--	--	--

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

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

		Löschung hat unverzüglich, das heißt ohne schuldhaftes Zögern, zu erfolgen, sobald die Daten nicht mehr benötigt werden. Die Vorschrift regelt nur die Verarbeitung personenbezogener Daten, die, auch unabsichtlich, bei der Videoüberwachung (auch mittels KI) von Objekten erstellt werden. Die technischen Daten können dauerhaft gespeichert werden, soweit die personenbezogenen Daten entfernt wurden. In Bezug auf Beschäftigte unterliegt die Weiterverarbeitung zur Aufdeckung von Straftaten und Pflichtverletzungen den Beschränkungen des § 15 Absatz 5 und 7.“	
	§ 18b Sonstige technische Überwachung	S. 84: „Ausgehend von der Tatsache,	

	Der Einsatz sonstiger technischer Mittel einschließlich der Nutzung von KI-Systemen zur Überwachung des Erhaltungszustands und der Funktionsfähigkeit des Eigentums öffentlicher Stellen und zu öffentlichen Zwecken gewidmeter Gegenstände ist in öffentlich zugänglichen Räumen entsprechend § 18 Absatz 6 und in nicht öffentlich zugänglichen Räumen entsprechend § 18a zulässig. Tonaufnahmen mit personenbezogenen Daten sind so weit wie möglich zu vermeiden; ist dies nicht oder nur mit unzumutbarem Aufwand möglich, sind sie innerhalb von 180 Sekunden automatisch zu löschen.	dass es eine Vielzahl technischer Möglichkeiten gibt, um die im öffentlichen Eigentum stehenden oder zu öffentlichen Zwecken gewidmeten Gegenstände auf ihren Erhaltungszustand und ihre Funktionsfähigkeit zu überwachen, wird eine weitere Ermächtigungsgrundlage zu deren Nutzung einschließlich der Nutzung von KI-Systemen eingefügt. Insbesondere im Gebäudemanagement hat der Einsatz von KI zu Überwachungszwecken großes Potenzial und beschränkt sich nicht auf Videoüberwachung, Da hierbei die Verarbeitung personenbezogener Daten nicht immer ausgeschlossen werden kann, wird eine weitere Ermächtigungsgrundlage	
--	--	---	--

		eingeführt. Sofern hierbei Tonaufnahmen gefertigt werden, muss die Aufzeichnung von menschlichen Stimmen soweit wie möglich vermieden werden. Mindestens ist die Weiterverarbeitung solcher Tonaufnahmen ausgeschlossen; die Löschung muss automatisch innerhalb von 180 Sekunden erfolgen. Grund hierfür ist, dass mit Tonaufnahmen in den Kernbereich privater Lebensgestaltung eingegriffen werden kann, weshalb eine längere Speicherung ausgeschlossen werden muss. Außerdem erfordert der Überwachungszweck in der Regel keine Tonaufnahmen mit personenbezogenen Daten und kann daher nicht gerechtfertigt werden. Um eine	
--	--	---	--

		Reaktionsmöglichkeit auf verdächtige Geräusche in Bezug auf den Überwachungszweck zu ermöglichen, darf die Speicherdauer von Tonaufnahmen nicht zu kurz sein. Hieraus resultiert die Speicherdauer von 180 Sekunden.“	
	§ 27a Datenschutzaufsicht für digitale Dienste Die oder der Landesbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde für digitale Dienste im Sinne des § 1 Nummer 8 zweiter Halbsatz des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; ber. 2022 I S. 1045), das zuletzt durch Artikel 44 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234, S. 19)	S. 84: Die Bestimmung der Aufsicht der oder des LfDI für digitale Dienste ergänzt die Zuweisung der Zuständigkeit der oder des LfDI für die Ordnungswidrigkeiten nach § 3a der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten nach „§ 28 Absatz 1 Nummer 10, 11 und 13 des Telekommunikation-Telemedien-Datenschutz-Gesetzes“ (nunmehr § 28	

	geändert worden ist, in der jeweils geltenden Fassung. Im Hinblick auf die Befugnisse der oder des Landesbeauftragten für den Datenschutz im Rahmen ihrer oder seiner Aufsichtstätigkeit über die Einhaltung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung	Nummer 10, 11 und 13 TDDDG), soweit nicht der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig ist. Es handelt sich um eine klarstellende Vorschrift, da gemäß § 1 Absatz 1 Nummer 8 TDDDG bei digitalen Diensten die Aufsicht durch die nach Landesrecht zuständigen Behörden und § 40 des Bundesdatenschutzgesetzes unberührt bleibt. Insbesondere wird klargestellt, dass die oder der LfDI die Befugnisse nach Artikel 58 DSGVO ausüben kann.	
	EgovG § 17a Automatisierter Erlass von Verwaltungsakten; Verordnungsermächtigung (1) Dieser Paragraph dient der	S. 85: „§ 35a des Landesverwaltungsverfahrensgesetzes statuiert einen landesrechtlichen Gesetzesvorbehalt für den	

	Erprobung und nach erfolgreicher Erprobung der Zulassung des vollständig automatisierten Erlasses von Verwaltungsakten einschließlich der Nutzung künstlicher Intelligenz (KI) durch KI-Systeme in verschiedenen Anwendungsbereichen und der daran anknüpfenden, durch die Landesregierung erfolgenden dauerhaften Zulassung des automatisierten Erlasses von Verwaltungsakten in einzelnen Anwendungsbereichen. KI-Systeme nach Satz 1 sind solche im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008,	vollständig automatisierten Erlass eines Verwaltungsaktes. Diesen Gesetzesvorbehalt füllt § 17a EGovG BW unter Berücksichtigung der Rahmenbedingungen des Artikels 22 DSGVO aus. Die weiteren datenschutzrechtlichen Verarbeitungsvoraussetzungen bleiben unberührt. [...] Dabei wird der Anwendungsbereich für die Erprobungsmöglichkeit unter Verweisung auf § 35a LVwVfG insoweit beschränkt, als für den vollständig automatisierten Erlass des Verwaltungsaktes weder ein Ermessen noch ein Beurteilungsspielraum bestehen darf. [...]"	
--	--	--	--

	(EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L vom 12.7.2024) in der jeweils geltenden Fassung. (2) Die für die Durchführung eines Verwaltungsverfahrens zuständige Behörde kann im Rahmen des § 35a des Landesverwaltungsverfahrensgesetzes Verwaltungsakte vollständig automatisiert erlassen, soweit nicht überwiegende Interessen derjenigen entgegenstehen, für die die Verwaltungsakte bestimmt sind oder die von ihnen betroffen werden. Deren Interessen überwiegen in der Regel nicht,		
--	---	--	--

	soweit 1. sie ausdrücklich und freiwillig ihre Einwilligung zum vollständig automatisierten Erlass des Verwaltungsakts geben, 2. gegen die Entscheidungen Widerspruchsverfahren eröffnet sind und die Widerspruchsbescheide nicht ihrerseits vollständig automatisiert erlassen werden, 3. die Behörde den Anträgen entspricht oder Erklärungen folgt und die Verwaltungsakte nicht in die Rechte anderer eingreifen oder 4. kein Anlass besteht, den Einzelfall durch Amtsträger zu bearbeiten, da die vorliegenden Informationen und die Angaben derjenigen, für die der Verwaltungsakt bestimmt oder die		
--	---	--	--

	von ihm betroffen werden, keine vom Regelfall abweichenden Hinweise enthalten. (3) Mindestens einen Monat vor Aufnahme des Verfahrens zum vollständig automatisierten Erlass von Verwaltungsakten ist der obersten Fachaufsichtsbehörde oder der zuständigen Rechtsaufsichtsbehörde und dem Innenministerium die neue Verfahrensweise anzuzeigen. (4) Die Erprobung ist für eine angemessene Zeit zu befristen. Der Erprobungszeitraum beträgt mindestens ein Jahr und darf höchstens zwei Jahre betragen und wird durch die für die Durchführung des Verwaltungsverfahrens zuständige Behörde festgelegt. Innerhalb eines Jahres nach Ende des nach Satz 2 festgelegten		
--	---	--	--

	Erprobungszeitraums ist ein Evaluierungsbericht der obersten Fachaufsichtsbehörde oder der zuständigen Rechtsaufsichtsbehörde und dem Innenministerium vorzulegen, wenn eine Fortführung der Erprobung oder der Dauerbetrieb beabsichtigt ist. Innerhalb dieses Jahres kann die Erprobung fortgesetzt werden, sowie für zwei weitere Jahre nach dem Ablauf dieses Jahres, wenn ein Evaluierungsbericht vorgelegt wird. Wird innerhalb der Jahresfrist nach Satz 3 kein Evaluierungsbericht vorgelegt, darf der vollständig automatisierte Erlass von Verwaltungsakten danach nur mit Einverständnis der obersten Fachaufsichtsbehörde oder der zuständigen Rechtsaufsichtsbehörde im		
--	---	--	--

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

	Vorgaben für ein Risikomanagementsystem aufgenommen werden.		
LIFG § 2 Anwendungsbereich (1) Dieses Gesetz gilt nach Maßgabe der Absätze 2 und 3 für die Stellen 1. des Landes, 2. der Gemeinden und Gemeindeverbände sowie 3. der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. (2) Dieses Gesetz gilt für	LIFG § 2 Anwendungsbereich (1) Dieses Gesetz gilt nach Maßgabe der Absätze 2 und 3 für die Stellen 1. des Landes, 2. der Gemeinden und Gemeindeverbände sowie 3. der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. (2) Dieses Gesetz gilt für	S. 89: „Bisher enthielt § 2 Absatz 3 LIFG ausschließlich stellenbezogene Bereichsausnahmeregelungen, das heißt Ausnahmeregelungen, die an bestimmte informationspflichtige Stellen anknüpfen und diese Stellen entweder ganz oder hinsichtlich bestimmter Bereiche von der Informationspflicht nach dem LIFG ausnehmen. Mit der Gesetzesänderung werden zwei informationsbezogene Bereichsausnahmeregelungen angefügt. Diese nehmen bestimmte Informationen insgesamt vom Anwendungsbereich des Gesetzes aus, unabhängig davon, bei welcher Stelle diese Informationen vorliegen. Zu Absatz 3 Nummer 2 In Nummer 2 wird die stellenbezogene Bereichsausnahme in Bezug auf Leistungsbeurteilungen und Prüfungen beibehalten. Dies ist aus	<u>Im Anhörungsverfahren aufgegriffen:</u> <u>„Entsprechend dem Vorschlag der Universität Freiburg wird der bisherige Gesetzeswortlaut der Regelung in § 2 Absatz 3 Nummer 2 LIFG in Bezug auf „Leistungsbeurteilungen und Prüfungen“ aus Gründen der Rechtssicherheit beibehalten und es werden dementsprechend weiterhin alle Stellen, die sich auf die Bereichsausnahme berufen können sollen, dort aufgezählt.</u> <u>– Dem Einwand der Universität Tübingen sowie des KIT entsprechend, wird auf die Verwendung des Begriffs der „Freiheit“ in der Neuregelung des § 2 Absatz 3 Nummer 5 LIFG verzichtet; hierdurch soll verhindert werden, dass Unsicherheiten in der Rechtsanwendung zu einem nicht bezweckten Absenken des Schutzniveaus zu Lasten Kunst- und Wissenschaftsfreiheit im Vergleich zur bisherigen Regelung</u>

1. den Landtag nur, soweit er öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt, 2. den Rechnungshof und die Gemeindeprüfungsanstalt jeweils nur außerhalb ihrer Prüfungs- und Beratungstätigkeit, 3. die Gerichte, die Strafverfolgungs-, Strafvollstreckungs- und Maßregelvollzugsbehörden sowie Disziplinarbehörden jeweils nur, soweit sie nicht als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher oder sachlicher Unabhängigkeit tätig werden, sowie 4. die öffentlich-rechtlichen Rundfunkanstalten nur, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen und dies staatsvertraglich geregelt ist.	1. den Landtag nur, soweit er öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt, 2. den Rechnungshof und die Gemeindeprüfungsanstalt jeweils nur außerhalb ihrer Prüfungs- und Beratungstätigkeit, 3. die Gerichte, die Strafverfolgungs-, Strafvollstreckungs- und Maßregelvollzugsbehörden sowie Disziplinarbehörden jeweils nur, soweit sie nicht als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher oder sachlicher Unabhängigkeit tätig werden, sowie 4. die öffentlich-rechtlichen Rundfunkanstalten nur, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen und dies staatsvertraglich geregelt ist.	Gründen der Rechtssicherheit erforderlich, da diesbezügliche Informationen nicht in jedem Falle unter die neue Bereichsausnahmeregelung in Nummer 5 fallen würden. Zu Absatz 3 Nummer 5 Hinsichtlich der Kunst- und Wissenschaftsfreiheit wird die bisherige stellenbezogene Bereichsausnahme der Nummer 2 in eine informationsbezogene Bereichsausnahme umgewandelt (Nummer 5). Damit sind künftig alle Informationen, die den Bereich der Kunst- oder Wissenschaftsfreiheit betreffen, vom Anwendungsbereich des Gesetzes ausgenommen. Die bisherige stellenbezogene Bereichsausnahme zugunsten der Kunst- und Wissenschaftsfreiheit konnte dazu führen, dass in Bezug auf ein- und dieselbe Information eine Stelle die Herausgabe aufgrund der Bereichsausnahme verweigern kann, eine andere Stelle hingegen nicht (vgl. hierzu Urteil des VGH BW vom 25.10.2023 – 10 S 125/22). Dieses Ergebnis begegnet verfassungsrechtlichen Bedenken, da die schrankenlos gewährleistete Kunst- und Wissenschaftsfreiheit nur durch entgegenstehende Belange mit	<u>führen.“</u> S. 62: Systematisch soll der gesamte Bereich der Kunst- und Wissenschaftsfreiheit sowie der Bereich der Kirchen, Religions- und Weltanschauungsgemeinschaften ausgenommen werden, mithin handelt es sich dem Wesen nach um eine Bereichsausnahme. [...] Die vorgesehene Erweiterung der Bereichsausnahme zum Schutz der Wissenschaftsfreiheit ist verfassungsrechtlich geboten: In dem der Entscheidung des VGH BW (10 S 125/22) zugrunde liegenden Einzelfall stellte der Tierschutz einen legitimen Eingriffsgrund dar, da diesem über Artikel 20a GG ebenfalls Verfassungsrang zukommt. Daher hat der VGH BW auf eine Vorlage an das Bundesverfassungsgericht oder den Verfassungsgerichtshof verzichtet. Ist in einer anderen Fallkonstellation jedoch kein Eingriffsgrund mit Verfassungsrang gegeben, käme allenfalls ein Rückgriff auf die Wissenschaftsfreiheit selbst als verfassungsunmittelbarer Ablehnungsgrund infrage. Einem Rückgriff auf Ablehnungsgründe
---	---	---	--

(3) Das Gesetz gilt nicht gegenüber 1. dem Landesamt für Verfassungsschutz und den sonstigen öffentlichen Stellen des Landes, soweit sie nach Feststellung der Landesregierung gemäß § 35 des Landessicherheitsüberprüfungsgesetzes Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wahrnehmen, 2. den Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, Hochschulen nach § 1 des Landeshochschulgesetzes, Schulen nach § 2 des Schulgesetzes für Baden-Württemberg sowie Ausbildungs- und Prüfungsbehörden, soweit Forschung, Kunst, Lehre, Leistungsbeurteilungen und Prüfungen betroffen sind, 3. der Landesbank Baden-Württemberg, der Landeskreditbank Baden-Württemberg - Förderbank, den Sparkassen sowie ihren	(3) Das Gesetz gilt nicht gegenüber 1. dem Landesamt für Verfassungsschutz und den sonstigen öffentlichen Stellen des Landes, soweit sie nach Feststellung der Landesregierung gemäß § 35 des Landessicherheitsüberprüfungsgesetzes Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wahrnehmen, 2. den Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, Hochschulen nach § 1 des Landeshochschulgesetzes, Schulen nach § 2 des Schulgesetzes für Baden-Württemberg sowie Ausbildungs- und Prüfungsbehörden, soweit Forschung, Kunst, Lehre, Leistungsbeurteilungen und Prüfungen betroffen sind, 3. der Landesbank Baden-Württemberg, der Landeskreditbank Baden-Württemberg - Förderbank,	Verfassungsrang zulässigerweise eingeschränkt werden kann, einem Rückgriff auf Ablehnungsgründe direkt aus der Verfassung jedoch laut VGH BW die Regelungssystematik des LIFG entgegensteht (vgl. Urteil vom 08.11.2023 – 10 S 916/22). Mit der neuen informationsbezogenen Bereichsausnahmeregelung in Nummer 5 sollen die verfassungsrechtlich gewährleistete Kunst- und Wissenschaftsfreiheit umfassend geschützt und so verfassungsrechtliche Bedenken ausgeräumt werden. Für die Beurteilung, ob die vorliegenden Informationen die Kunst- oder Wissenschaftsfreiheit der übermittelnden Stelle berühren, kann die informationspflichtige Stelle – den allgemeinen Grundsätzen des Verwaltungsverfahrenrechts nach § 24 LVwVfG entsprechend – die Stelle, von der die gegenständlichen Informationen übermittelt wurden zur Sachverhaltsaufklärung einbeziehen. Die Regelung zur Durchführung eines Drittbeteiligungsverfahrens nach § 8 LIFG ist hingegen nicht einschlägig, da durch die	direkt aus der Verfassung steht jedoch die Regelungssystematik des LIFG entgegen (vgl. VGH BW vom 08.11.2023 – 10 S 916/22). Demnach kann ergänzend zu den im LIFG normierten Ausschlussgründen nicht unter Verweis auf verfassungsmäßige Rechte auf ungeschriebene Versagungsgründe zurückgegriffen werden, da das LIFG ein abgeschlossenes System von Bereichsausnahmen (§ 2 Absatz 2 und 3 LIFG) und Ausschlussgründen (§§ 4 bis 6 LIFG) enthalte. Die im Rahmen der neuen Regelung des § 2 Absatz 3 Nummer 5 LIFG gewählte Terminologie der „Betroffenheit“ wurde auch schon in der bisherigen gesetzlichen Regelung des § 2 Absatz 3 Nummer 2 LIFG so verwendet: „[...] soweit Forschung, Kunst, Lehre, Leistungsbeurteilungen und Prüfungen betroffen sind [...]“. Würde man stattdessen eine „Beeinträchtigung“ der Kunst- oder Wissenschaftsfreiheit voraussetzen, würde dies zu einer Absenkung des bisherigen Schutzniveaus führen, was gerade nicht bezweckt ist.
--	---	--	---

Verbänden und Verbundunternehmen, den Selbstverwaltungsorganisationen der Wirtschaft, der Freien Berufe und der Krankenversicherung sowie 4. den Landesfinanzbehörden im Sinne des § 2 des Finanzverwaltungsgesetzes, soweit sie in Verfahren in Steuersachen tätig werden. (4) Dieses Gesetz gilt auch für natürliche oder juristische Personen des Privatrechts, soweit sie öffentlich-rechtliche Verwaltungsaufgaben, insbesondere solche der Daseinsvorsorge, wahrnehmen oder öffentliche Dienstleistungen erbringen und dabei der Kontrolle einer Stelle, soweit diese in den Anwendungsbereich nach Absatz 1 fällt, unterliegen. Kontrolle im Sinne des Satz 1 liegt vor, wenn 1. die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe oder bei der Erbringung	den Sparkassen sowie ihren Verbänden und Verbundunternehmen, den Selbstverwaltungsorganisationen der Wirtschaft, der Freien Berufe und der Krankenversicherung sowie 4. den Landesfinanzbehörden im Sinne des § 2 des Finanzverwaltungsgesetzes, soweit sie in Verfahren in Steuersachen tätig werden. <u>Keine Informationspflicht nach diesem Gesetz besteht für</u> <u>1. das Landesamt für Verfassungsschutz und die sonstigen öffentlichen Stellen des Landes, soweit sie nach Feststellung der Landesregierung gemäß § 35 des Landessicherheitsüberprüfungsgesetzes Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wahrnehmen,</u> <u>2. Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, Hochschulen nach § 1 des Landeshochschulgesetzes, Schulen nach § 2 des</u>	Bereichsausnahme zugunsten der Kunst- und Wissenschaftsfreiheit insofern bereits der Anwendungsbereich des LIFG nicht eröffnet ist.“	
--	--	---	--

der öffentlichen Dienstleistung gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt, insbesondere ein Kontrahierungszwang oder ein Anschluss- und Benutzungszwang besteht, oder 2. eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts allein oder zusammen, unmittelbar oder mittelbar a) die Mehrheit des gezeichneten Kapitals der Person des Privatrechts besitzt oder besitzen oder b) über die Mehrheit der mit den Anteilen der Person des Privatrechts verbundenen Stimmrechte verfügt oder verfügen oder	<u>Schulgesetzes für Baden-Württemberg sowie Ausbildungs- und Prüfungsbehörden, soweit Leistungsbeurteilungen und Prüfungen betroffen sind,</u> <u>3. die Landesbank Baden-Württemberg, die Landeskreditbank Baden-Württemberg – Förderbank, die Sparkassen sowie ihre Verbände und Verbundunternehmen, die Selbstverwaltungsorganisationen der Wirtschaft, der Freien Berufe und der Krankenversicherung,</u> <u>4. die Landesfinanzbehörden im Sinne des § 2 des Finanzverwaltungsgesetzes, soweit sie in Verfahren in Steuersachen tätig werden,</u> <u>5. Informationen, die Kunst, Wissenschaft, Forschung oder Lehre betreffen, sowie</u> <u>6. Angelegenheiten der Kirchen, der Religions- und Weltanschauungsgemeinschaften sowie ihrer Untergliederungen und Einrichtungen, soweit diese dem religiösen Selbstbestimmungsrecht</u>		
---	--	--	--

c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans der Person des Privatrechts stellen kann oder können.	<u>unterfallen.“</u> (4) Dieses Gesetz gilt auch für natürliche oder juristische Personen des Privatrechts, soweit sie öffentlich-rechtliche Verwaltungsaufgaben, insbesondere solche der Daseinsvorsorge, wahrnehmen oder öffentliche Dienstleistungen erbringen und dabei der Kontrolle einer Stelle, soweit diese in den Anwendungsbereich nach Absatz 1 fällt, unterliegen. Kontrolle im Sinne des Satz 1 liegt vor, wenn 1. die Person des Privatrechts bei der Wahrnehmung der öffentlichen Aufgabe oder bei der Erbringung der öffentlichen Dienstleistung gegenüber Dritten besonderen Pflichten unterliegt oder über besondere Rechte verfügt, insbesondere ein Kontrahierungszwang oder ein Anschluss- und Benutzungszwang besteht, oder		
--	--	--	--

	2. eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts allein oder zusammen, unmittelbar oder mittelbar a) die Mehrheit des gezeichneten Kapitals der Person des Privatrechts besitzt oder besitzen oder b) über die Mehrheit der mit den Anteilen der Person des Privatrechts verbundenen Stimmrechte verfügt oder verfügen oder c) mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans der Person des Privatrechts stellen		
--	--	--	--

	kann oder können.		
			Aus dem Anhörungsverfahren (S. 61): „Ergänzender Vorschlag – ZENDAS hält eine normenklare Rechtsgrundlage für den Abruf der Identifikationsnummer zur Zulassung zum Hochschulstudium für erforderlich. § 6 Absatz 2 IDNrG sei dafür keine ausreichende Ermächtigungsgrundlage. ZENDAS schlägt vor zu prüfen, ob dies im Rahmen dieses Gesetzgebungsverfahrens erfolgen könne.

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

			gesetzliche Anpassungen können erst nach Beendigung dieser Arbeit erfolgen.“
--	--	--	--