

## A. Gesetzesinfos

### 1. Entgelttransparenzrichtlinie

Noch liegt kein nationaler, konkreter Gesetzentwurf vor. Aber bis zum 07-06-2026 ist die EU-Entgelttransparenzrichtlinie (2023/970) in nationales Recht umzusetzen. Die Anforderungen an Unternehmen werden weitreichender sein als diejenigen aus dem geltenden Entgelttransparenzgesetz (EntgTranspG). Arbeitgeber müssen dann Vergütungsstrukturen einrichten und unterhalten, durch die gleiches Entgelt bei gleicher oder gleichwertiger Arbeit gewährleistet wird. Der Betriebsrat hat ein Mitbestimmungsrecht bei der Festlegung der Kriterien und deren Gewichtung. Hieraus ergeben sich umfangreiche Pflichten im Bewerbungsverfahren und Informationspflichten im laufenden Arbeitsverhältnis. Weitere Infos z. B.: - [LINK](#) –

### 2. KRITIS-Dachgesetz

Nach dem NIS2UmsuCG – dass die Cyber- und Informationssicherheit in den Blick genommen hat – ist nun auch das „Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ (KRITIS-DachG) verabschiedet worden, das den physischen Schutz kritischer Infrastrukturen (also auch Gesundheitswesen) im Fokus hat. – [LINK](#) -

### 3. Neuregelung § 630g BGB

Das Akteneinsichtsrecht in Patientendokumentationen und insbesondere die damit verbundene Kostenfrage wurde in § 630g BGB vor dem Hintergrund des EuGH-Urteil C-307/22 vom 26-10-2023 neu gefasst. Patienten ist „auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Behandlungsakte zu gewähren. .... Die erste Abschrift wird unentgeltlich zur Verfügung gestellt.“ Der datenschutzrechtliche Anspruch auf eine kostenfreie Kopie endet mit dem Tod einer Person (Erwägungsgrund 27 DSGVO). Erben und Angehörige können daher mit Kosten der Akteneinsicht belegt werden (so auch das OVG Rheinland-Pfalz mit Urteil vom 28-11-2025, Az.: 10 A 11059/23OVG).

## B. DSGVO

### 1. BayLDA legt 15. Tätigkeitsbericht für 2025 vor

Das Bayerische Landesamt für Datenschutzaufsicht hat den 15. Tätigkeitsbericht für 2025 vorgelegt. Interessante Themen: Email-Postfächer ehemaliger Beschäftigter, Online-Terminbuchungen und Terminmanagement in einer Arztpraxis, Transkription von Videokonferenzen etc. – [LINK](#) –

### 2. Tätigkeitsbericht Baden-Württemberg für 2025

Der 41. TB für 2025 aus Baden-Württemberg liegt vor. – [LINK](#) -

### 3. Tätigkeitsbericht für 2025 aus Hamburg

Der HfDI hat den 34. Tätigkeitsbericht für 2025 vorgelegt. – LINK – Hervorzuheben sind die Ausführungen zu „Automatisierte Transkription und Protokollierung von Videokonferenzen“ nicht nur für Behörden, Seite 43 ff., und die „Weitergabe von Beschäftigtendaten in Konzernstrukturen“, Seite 71 f.

### 4. Tätigkeitsbericht Sachsen für 2025

Der Tätigkeitsbericht aus Sachsen für 2025 liegt vor. – LINK -

### 5. Tätigkeitsbericht aus Schleswig-Holstein 2025 (ULD)

Im Frühjahr veröffentlicht Frau Hansen einen Bericht über die Tätigkeit ihrer Behörde, des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Ein ständiger Dauerbrenner sind die Beschwerden über eine Videoüberwachung, z. B. in Sportvereinen, Reitanlagen und Kleingärten, in Taxis, in Restaurants und in Schwimmbädern. „Nicht jede Videoüberwachung ist datenschutzrechtlich unzulässig – offenbar denken dies aber viele Menschen.“. Das ULD informiert auf seiner Website, was für eine rechtskonforme Videoüberwachung zu beachten ist. - LINK –

### 6. Tätigkeitsbericht aus Hessen

Der 54. Tätigkeitsbericht des LfDI liegt vor. – LINK – Interessant die Ausführungen zu Forschungsdatentreuhänder, Patientenakten beim Ausscheiden eines Arztes aus einer Gemeinschaftspraxis, Streaming im Gesundheitsbereich etc.

### 7. Tätigkeitsbericht NRW

Der 31. Tätigkeitsbericht der LDI Nordrhein-Westfalen wurde veröffentlicht. – LINK – Highlight-Themen Social Media als Werbepattform einer Therapeutin oder der Influencer-Auftritt von Pflegepersonal.

### 8. Broschüre „Cybersicherheit im Gesundheitswesen 2025“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt in einer 4 seitigen Broschüre einen exemplarischen Einblick in die Gefährdungslage im Gesundheitssektor. Statistische Zahlen geben Aufschluss über Vorfälle in den Bereichen "Telematikinfrastruktur", "Leistungserbringer" sowie "Hersteller und Produkte". Im Fokus stehen das E-Rezept, die Sicherheit in der ambulanten Versorgung sowie vernetzte Medizinprodukte. - LINK -

## C. Urteile und Beschlüsse von Gerichten

### 1. Exzessiver Auskunftsantrag

Der EuGH hat mit Urteil C-526/24 vom 19-03-2026 umfangreiche Ausführungen gemacht, wann ein Auskunftsantrag als „exzessiv“ abgelehnt werden kann. Dies gilt insbesondere, wenn reine Geldinteressen im Vordergrund stehen. Die Hürden allerdings sind hoch.

## 2. Keine Verarbeitung von Diagnosen durch private Krankenversicherer

Mit Urteil des BVerwG vom 06.03.2026, Az. 6 C 7.24 hat dieses entschieden, dass private Krankenversicherungen nicht befugt sind, ohne Einwilligung – z. B. für ein Vorsorgeprogramm - der betroffenen Versicherten die Diagnosen auf deren zur Erstattung eingereichten Rechnungen zu analysieren.

## 3. Abtretung eines DSGVO Auskunftsanspruchs?

Der Auskunftsanspruch nach Art. 15 DSGVO ist nicht geschaffen worden, damit die betroffene Person eine (Haupt-)Forderung durchsetzen kann, sondern um sich der Verarbeitung ihrer Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können, ErwG 63 Satz 1 DSGVO.

Der BGH hat mit Urteil vom 24-02-2026, Az.: VI ZR 430/24 datenschutzrechtliche Auskunftsansprüche grundsätzlich als höchstpersönlich gewertet. Die gerichtliche Durchsetzung kann jedoch im Wege der gewillkürten Prozessstandschaft möglich sein, sofern eine wirksame Ermächtigung des Betroffenen sowie ein eigenes schutzwürdiges Interesse des Prozessstandschafters vorliegen. Entscheidend ist dabei, dass keine unzulässige Umgehung des Rechtsdienstleistungsgesetzes erfolgt und die Sachherrschaft beim materiell Berechtigten verbleibt.

## 4. Geschäftsführer können private Daten aus Handelsregister löschen lassen

Geschäftsführer können private Daten – wie Privatadresse und Unterschrift – aus dem Handelsregister löschen lassen, da diese keine obligatorischen Informationen sind, so der BGH mit Beschluss vom 18-02-2026, Az.: II ZB 2/25.

## 5. Umfang einer „Kopie“ im Rahmen eines Auskunftsantrags nach Art. 15 DSGVO

Das OGH, (Österreich) hat mit Urteil vom 18.03.2026, Az.: 6 Ob 170/25f die „Kopie“ nach Art 15 Abs 3 DSGVO so beschrieben, dass diese grundsätzlich eine vollständige und verständliche Reproduktion der personenbezogenen Daten zu sein hat – nicht automatisch eine Kopie des gesamten Dokuments. Ganze Dokumente oder Dokumentauszüge sind nur dann herauszugeben, wenn das zur Verständlichkeit oder zur wirksamen Ausübung der Betroffenenrechte erforderlich ist.

## 6. Verpflichtende Nutzung von Privatgeräten zur Authentifizierung 48.000 € Bußgeld

Beschäftigte mussten den Zugang zu dienstlich erforderlichen Accounts über ihr privates Smartphone als zweiten Faktor authentifizieren, dazu wurden dann die privaten Daten an Dritte weitergegeben. Eine Authentifizierung über die dienstliche E-Mail-Adresse wollte die Unternehmensleitung nicht. Die spanische Aufsichtsbehörde (AEPD) erkannte dafür keine Rechtsgrundlage. Verarbeitungen, die zwar nützlich, aber objektiv nicht erforderlich sind, um die vertraglich vereinbarte Dienstleistung zu erbringen werden nicht durch die DSGVO gedeckt. Dies gilt auch dann, wenn die Verarbeitung für andere geschäftliche Zwecke des Arbeitgebers erforderlich ist. - LINK -

- Hinzu kommt die arbeitsrechtliche Bewertung. Das Bundesarbeitsgericht hat in einem wegweisenden Urteil im Jahr 2021 (Az. 5 AZR 334/21) entschieden, dass Unternehmen die wesentlichen Arbeitsmittel zur Verfügung stellen müssen. Die Beschäftigten schulden grundsätzlich nur ihre Arbeitskraft, nicht ihre privaten Ressourcen.

### **7. Anonymisierung kann Umsetzung der Löschpflicht sein**

Die Löschpflicht aus Art. 17 DSGVO kann auch durch Anonymisierung der Daten umgesetzt werden. Die Anonymisierung stellt ein Minus zur Löschung dar und ist damit von Art. 17 DSGVO erfasst, so das OLG Dresden mit Urteil vom 03.02.2026, Az. 4 U 292/25.

### **8. Auskunftsanspruch gegen gerichtlichen Sachverständigen als Verantwortlicher**

Ein gerichtlicher Sachverständiger ist hinsichtlich der von ihm im Rahmen seiner Gutachtenerstellung verarbeiteten personenbezogenen Daten eigenständiger Verantwortlicher im Sinne der DSGVO. Betroffene können daher grundsätzlich einen Auskunftsanspruch nach Art. 15 DSGVO unmittelbar gegen den Sachverständigen geltend machen; diesem können jedoch Beschränkungen insbesondere aus prozessrechtlichen Vertraulichkeitsanforderungen sowie aus Rechten Dritter entgegenstehen, so das OLG Stuttgart, Urteil vom 25.02.2026 – 4 U 342/25.

### **9. Schadensersatz nach Hackerangriff**

Das LAG Hessen hat mit Urteil vom 10.2.2026, Az.: 12 SLa 709/25 die Frage von Schadensersatzansprüchen nach einem Hackerangriff beleuchtet: ein Anspruch auf immateriellen Schadensersatz nach Art. 82 Abs. 1 DSGVO besteht nach einem Hackerangriff nicht schon deshalb, weil personenbezogene Daten betroffen waren; erforderlich sind konkrete Anhaltspunkte für einen tatsächlichen oder zumindest hinreichend wahrscheinlichen Schaden. Und: der erfolgreiche Hackerangriff als solcher beweist noch nicht, dass die Verantwortliche unzureichende technische oder organisatorische Maßnahmen im Sinne der DSGVO getroffen hat. Für die Feststellung künftiger Schäden genügt nicht eine nur abstrakte Möglichkeit; es muss eine gewisse Wahrscheinlichkeit eines Schadenseintritts bestehen.

### **10. Auskunft vs. Sozialgeheimnis**

Das Landessozialgericht Niedersachsen-Bremen (LSG) hat entschieden, dass eine Krankenkasse nicht verpflichtet ist, Auskunft über Hinweisgeber zu einem möglichen Sozialleistungsmisbrauch zu erteilen. Hinsichtlich der Herausgabe von Sozialdaten verfüge die Behörde über ein Ermessen, das sie rechtmäßig ausgeübt habe. Die Belange des Sozialdatenschutzes sowie das berechnete Interesse von Hinweisgebern an der Wahrung ihrer Anonymität seien zu berücksichtigen. Etwas anderes gelte nur, wenn Anhaltspunkte dafür vorlägen, dass der Hinweisgeber wider besseres Wissen und in der Absicht der Rufschädigung gehandelt habe, oder der Behörde leichtfertig unzutreffende Informationen übermittelt worden seien. LSG Niedersachsen-Bremen, Beschluss vom 23. März 2026, Az.: L 16 KR 1/26

### 11. E-Mail Verschlüsselung

Bei Daten mit **normalem Risiko** reicht es aus, wenn die Informationen beim E-Mail-Versand transportverschlüsselt werden. Eine Ende-zu-Ende-Verschlüsselung ist hingegen nicht notwendig, so das VG Düsseldorf, Urt. v. 02.04.2026, 29 K 7351/23

### 12. Unerlaubter KI-Einsatz in einer Prüfung ist Täuschung

Das VG Kassel, hat mit Urteil vom 25-02-2026, Az.: 7 K 2134/24 KS ü 7 K 2515/25 KS die unerlaubte Nutzung von KI in einer Prüfung als Täuschung gewertet. Ein Ausschluss ist damit rechtmäßig.

## D. Beschäftigtendatenschutz – Artikel und Urteile

### 1. Leitfaden „Künstliche Intelligenz und Mitbestimmung“

Bitkom hat einen Leitfaden „Künstliche Intelligenz und Mitbestimmung“ veröffentlicht. -LINK -

### 2. Keine Anscheinsbeweis für den Zugang bei Einwurf-Einschreiben

Das LAG Hamburg beschäftigte sich in seiner Entscheidung vom 17.07.2025, Az.: 4 SLa 26/24 mit der Frage, ob ein Arbeitnehmer die Einladung zu einem BEM-Verfahren erhalten hatte. Das LAG verneint dies für ein Einwurf-Einschreiben. Bei Anwendung des neuen - digitalisierten - Zustellungsverfahrens bestünde anders als beim früheren Peel-Off-Label-Verfahren kein Beweis des ersten Anscheins für den Zugang der Einladung. Die Kündigung des Arbeitnehmers sei unwirksam. Es mangle am ordnungsgemäß durchgeführten BEM-Verfahren.

Die Entscheidung ist noch nicht rechtskräftig. Die Revision zum BAG ist zugelassen.

### 3. Versäumte Bearbeitung eines Whistleblower-Hinweises rechtfertigt Kündigung

Die versäumte Bearbeitung eines Whistleblower-Hinweises rechtfertigt die Kündigung des dafür verantwortlichen Mitarbeitenden, so das ArbG Offenbach mit Urteil vom 25-11-2025, Az.: 1 Ca 136/25.

### 4. Kein Dauerzugriffsrecht auf Zeiterfassungsdaten

Ein Gesamtbetriebsrat kann keinen dauerhaften elektronischen Zugriff auf personenbezogene Arbeitszeitdaten der Beschäftigten verlangen, weil ihm hierfür die Zuständigkeit fehlt und auch datenschutzrechtliche Gründe entgegenstehen. Dies ändert auch eine bestehende Betriebsvereinbarung nicht – so das LAG Köln, Beschluss v. 09.01.2026, Az: 9 TaBV 22/25. (Die Revision ist zugelassen)

## E. Kirchlicher Datenschutz

### 1. Arbeitshilfe Umsetzung KDG-Novelle

Die Konferenz der Diözesandatenschutzbeauftragten hat eine Arbeitshilfe zur Novellierung veröffentlicht. Highlights: Die Fax-Nutzung ist nunmehr nur noch in Ausnahmefällen erlaubt (!! ) und die Multi-Faktor-Authentifizierung wird obligatorisch. – LINK –

### 2. Die Löschung personenbezogener Daten durch die MAV

Jacob Jousen hat einen lesenswerten Artikel zur Löschung personenbezogener Daten durch die MAV geschrieben. – LINK – Felix Neumann von Art. 91 hat das Thema weiter auf den Punkt gebracht. – LINK –

### 3. Bußgeldkonzept der Kath. Datenschutzaufsicht Nord (Bezug: mangelhafte technisch-organisatorische Maßnahmen zur Vermeidung von unbefugten Patientendatenzugriffen)

Das Interdiözesane Datenschutzgericht hat ein Bußgeld der KDSA Nord mit folgender Begründung gekippt: „Als Ausgangspunkt ihrer Berechnung der Geldbuße hat die Antragsgegnerin in Anlehnung an die EDSA-Leitlinien einen Betrag von 10 Millionen Euro gewählt und den in § 51 Abs. 5 KDG genannten Betrag von 500.000 Euro lediglich als potentielle Kappungsgrenze angewendet. Dies stellt eine Ermessensüberschreitung des in § 51 Abs. 5 KDG vorgegebenen Ermessensrahmens dar. Denn § 51 Abs. 5 KDG ist nicht lediglich eine Kappungsgrenze, sondern ein Geldbußenrahmen, innerhalb dessen das Ermessen zur Höhe der Geldbuße auszuüben ist.“ (Beschluss IDSG 05/2024, Rn. 30).“ – LINK - Spannend auch der Hintergrund: das Bußgeld erfolgte, weil das Krankenhaus keine ausreichenden technisch-organisatorischen Maßnahmen getroffen hatte, um unbefugte Zugriffe auf abgeschlossene Behandlungsfälle zu verhindern. Vorliegend griffen Azubis im Rahmen eines Mitarbeiterexzesses auf solche zu und verwendeten die Daten.

### 4. Broschüre „Umgang mit Datenschutzverletzungen“

Das KDSZ Frankfurt und die KDSA Nord haben zusammen eine Broschüre „Umgang mit Datenschutzverletzungen“ veröffentlicht. – LINK – Inhalt ist eine Zusammenfassung, was Datenschutzverletzungen sind und wie sinnvoll damit umgegangen werden sollte. Ergänzt wird die Broschüre durch eine Liste typischer Datenpannen.

## F. Sonstiges

### 1. Google reCAPTCHA wird Auftragsverarbeiter

Bisher agierte Google bei der Nutzung der erhobenen Informationen zum Nutzerverhalten wie ein Verantwortlicher (DSGVO). Google entschied selbst darüber, wie und zu welchen Zwecken die Informationen verarbeitet werden. Zum 02. -April 2026 will Google auf Auftragsverarbeitung umstellen und die spezifischen Nutzungsbedingungen ändern. - LINK -

- Daraus folgt nicht per se Datenschutzkonformität. Weiterhin bleibt intransparent, welche Daten Google erhebt und nutzt. Auch wenn Nutzende mehr Rechte über die gesammelten Daten erhalten sollen.

## **2. Orientierungshilfe Gesundheitsdatennutzungsgesetz (GDNG)**

Der BayLDA hat eine Orientierungshilfe zum Gesundheitsdatennutzungsgesetz veröffentlicht. – [LINK](#) –

## **3. Grundschatz – Leitfaden zur Methodik**

Das BSI hat auf nur 45 Seiten die Grundlagen der Grundschatzmethodik dargestellt. – [LINK](#) -

## **4. Aktualisierte EVB-IT**

Es wurden aktualisierte Versionen der EVB-IT-Vertragsmuster veröffentlicht. – [LINK](#) -

## **5. Abschlussbericht zum Projekt Sicherheit von Praxisverwaltungssystemen (SiPra)**

Das BSI hat die Datenschutzkonformität und IT-Sicherheit von Arzt-Praxisverwaltungssystemen untersucht und in Punkt 5.2 gängige Schwachstellen beschrieben. – [LINK](#) – [LINK](#) –

## **6. Abschlussbericht zum Projekt Sicherheit von digitalen Pflegedokumentationssystemen (DiPS)**

Das BSI testete exemplarisch 3 Pflegedokumentationssysteme. Der Abschlussbericht vom 13.02.2026 liegt vor. - [LINK](#) -

Die Handlungsempfehlungen wurden zur Kommentierung bis 17.06.2026 veröffentlicht. - [LINK](#) -

## **7. FAQ zur allgemeinen digitalen Aufbewahrung**

Die Bundessteuerberaterkammer (BStBK) hat ihren FAQ-Katalog zur digitalen Aufbewahrung aktualisiert. Die Veröffentlichung behandelt handels- und steuerrechtliche Aufbewahrungspflichten nach Handelsgesetzbuch (HGB), Abgabenordnung (AO) sowie den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD). Dabei werden an mehreren Stellen datenschutzrechtlich relevante Fragestellungen aufgegriffen. – [LINK](#) –

## **8. C5:2026**

Der Cloud Computing Compliance Criteria Catalogue (C5) wurde aktualisiert. Das BSI bietet auch eine maschinenlesbare Version an. Weiterhin gibt es eine Kreuzreferenztafel, damit man Änderungen von dem früheren zum aktuellen C5-Katalog leichter überprüfen kann. - [LINK](#) –

## **9. Reisepass-Verifikation mit Persona im Auftrag von LinkedIn ... und alle kennen mich**

Eine Identitätsprüfung durch LinkedIn mittels Bereitstellung meines Reisepasses erfolgt stets durch den Dienstleister „Persona“, eine kalifornische Firma. Diese stellt laut ihrer Datenschutzerklärung alle

akribisch erfassten Daten 17 weiteren Unternehmen bereit, darunter Antropic, OpenAi, Groqcloud, AWS, Google Cloud etc. – LINK – Wer will das wirklich???

## **10. Staatliches Bedrohungsmanagement: Psychisch kranke Personen mit Risikopotential**

Wer ist gefährlich- und wer ist krank? Damit beschäftigt sich ein Heise-Artikel. – LINK – Thema ist die uneinheitliche, nicht regulierte Datenverarbeitung dieser Personengruppen.

## **G. Künstliche Intelligenz (KI)**

### **1. Verhaltenskodex zur Kennzeichnung und Kennzeichnungsanforderung von KI-generierten Inhalten**

Die EU-Kommission hat einen zweiten Entwurf des Verhaltenskodex zur Kennzeichnung und Kennzeichnungsanforderung von KI-generierten Inhalten veröffentlicht, um Anbietern und Betreibern zu helfen, die Kennzeichnungs- und Kennzeichnungsanforderungen für KI-generierte Inhalte gemäß Artikel 50 AI-Gesetz zu erfüllen. – LINK –

### **2. Rechtliche Anforderungen bei KI-Nutzung – Datenschutzbeauftragter gibt Antworten auf häufig gestellte Fragen**

Das LfDI Niedersachsen hat ein Papier "Rechtliche Anforderungen bei KI-Nutzung" veröffentlicht. – LINK -

### **3. Kennzeichnung KI-generierter Inhalte**

Die Wettbewerbszentrale hat einen Leitfaden veröffentlicht, der Orientierung bei der wettbewerbsrechts- und KI-verordnungskonformen Nutzung KI-generierter Inhalte geben soll. Im Fokus stehen Kennzeichnungspflichten nach Art. 50 KI-Verordnung der EU (KI-VO) 2024/1689, die ab dem 2. August 2026 vollumfänglich gelten. -LINK –

### **4. Orientierungshilfe „Datenschutz bei KI-Projekten in der bayerischen Verwaltung“**

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat eine Orientierungshilfe "Datenschutz bei KI-Projekten in der bayerischen Verwaltung" veröffentlicht. – LINK -

### **5. Whitepaper: Strategien für KI im Krankenhaus**

Künstliche Intelligenz wird im Krankenhaus häufig in einzelnen Pilotprojekten erprobt – etwa in der Dokumentation, der medizinischen Bildanalyse oder der Entscheidungsunterstützung. Der nachhaltige Nutzen bleibt jedoch oft begrenzt. Das Whitepaper des Fraunhofer IAIS zeigt: Die größten Hürden liegen weniger in der Technologie als vielmehr in fehlenden Datenstrategien, unklaren Zuständigkeiten, regulatorischer Unsicherheit und mangelnder Akzeptanz bei Mitarbeitenden. Download - LINK -

Sind die Inhalte von Links nicht aufrufbar und ist ein Link mit einem Zeilenumbruch dargestellt, kann durch Entfernen des Trennzeichens die Linkfunktion aktiviert werden. Keine Haftung für Vollständigkeit und Richtigkeit der Inhalte! Abmeldung des Newsletters jederzeit durch eine Rückmeldung per Email, Post oder Telefon.