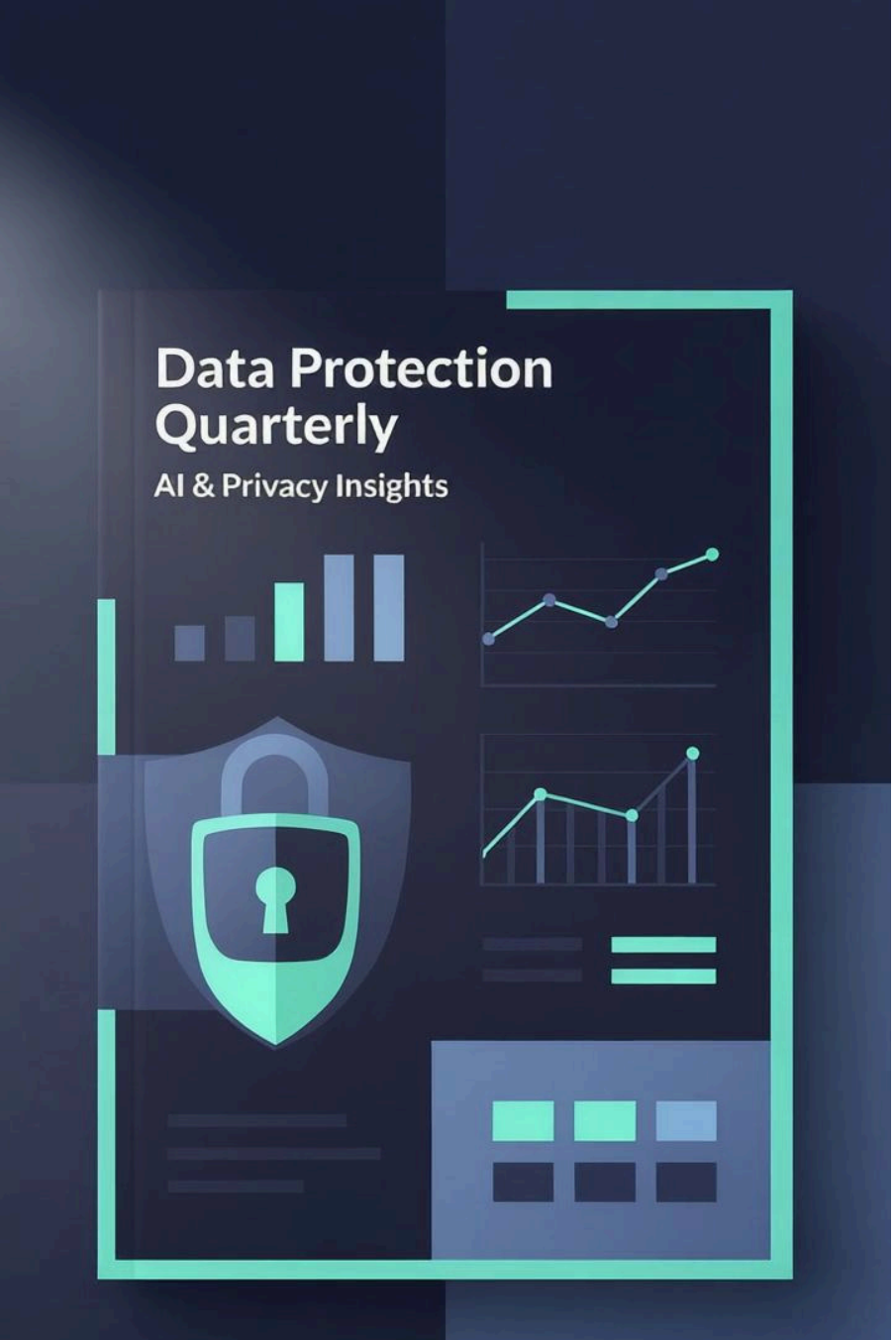


PRICOM

Individuell. Kompetent. Lösungsorientiert.

Update Q1 / 2026

IT-SICHERHEIT | DATENSCHUTZ | KI | DATA ACT

Alle wichtigen Entwicklungen zu IT-Sicherheit, Datenschutz, KI und Data Act Kompakt aufbereitet mit Tipps für die Unternehmenspraxis.

Business sichern, Risiken minimieren, Chancen nutzen.

Überblick: Die wichtigsten Themen

01

IT-Sicherheit

Ransomware und E-Mail-Hacking bleiben grösste Cyberbedrohungen — mit steigenden Meldezahlen.

KRITIS-Dachgesetz gilt seit 17. März 2026 mit Auswirkungen auf IT-Dienstleister.

02

Gerichte

EuGH stärkt Unternehmen gegen missbräuchliche Auskunftsersuchen.

BGH ermöglicht Chancen bei Rechtsgrundlage "Vertrag"

OLG verschärfen Haftung bei Cookies & Tracking.

03

Behörden

Hamburger DSB verstärkt Anforderungen an Interessenabwägung.

BayLDA: Fast 10.000 Beschwerden, Zulässigkeit GPS-Tracking, E-Mail-Postfächer

Dokumente schwärzen — technisch korrekt, nicht nur optisch.

04

Data Act & KI

Neue Zuständigkeiten, gestaffelte Fristen und Vereinfachungen auf dem Weg.

I. IT-SICHERHEIT

Ransomware & E-Mail-Hacking: Bedrohungslage 2025

BayLDA, 15. Tätigkeitsbericht 2025

> Das BayLDA meldete 2025 insgesamt **524 Ransomware-Fälle** und knapp **400 kompromittierte E-Mail-Accounts** — Tendenz weiter steigend.

- **Haupteinfallstore:** Phishing, fehlende Mehrfaktor-Authentifizierung und ungepatchte Software bleiben primäre Angriffsvektoren. Diese Schwachstellen sind bekannt — und dennoch weit verbreitet.
- **Multiplikatoreffekt kompromittierter Postfächer:** Ein gehacktes E-Mail-Konto sendet täuschend echte Phishing-Mails an Hunderte Kontakte weiter. Glaubwürdigkeit dieser Mails ist extrem hoch — der Schaden entsprechend gross.
- **Besonders betroffene Branchen:** Mittelstand, Fertigung und Zulieferer sind durch vernetzte Systeme besonders anfällig für Kaskadeneffekte. Supply-Chain-Angriffe auf IT-Dienstleister treffen deren gesamte Kundschaft gleichzeitig.
- **Medizinische Einrichtungen:** Bei Gesundheitseinrichtungen ist die Veröffentlichung von Patientendaten ein nicht reparierbarer Schaden — mit weitreichenden rechtlichen und reputativen Folgen.

Praxis-Tipp: Aktivieren Sie Mehrfaktor-Authentifizierung für alle E-Mail-Konten und Remote-Zugänge und stellen Sie sicher dass Offline-Backups im Ernstfall tatsächlich einsatzbereit sind. Das BayLDA stellt kostenlos eine Checkliste Cyberfestung bereit (lda.bayern.de). Wir beraten Sie gerne zur Umsetzung.

I. IT-SICHERHEIT

KRITIS-Dachgesetz: Seit 17. März 2026 in Kraft

> KRITIS-Dachgesetz schafft erstmals **bundeseinheitliche und sektorübergreifende Mindeststandards** für physischen Schutz kritischer Infrastrukturen.

11 Erfasste Sektoren

Energie, Transport, Finanz- und Versicherungswesen, Gesundheit, Trinkwasser & Abwasser, Abfallentsorgung, IT & Telekommunikation, Ernährung, Weltraum, Öffentliche Verwaltung

Pflichten und Schwellenwert

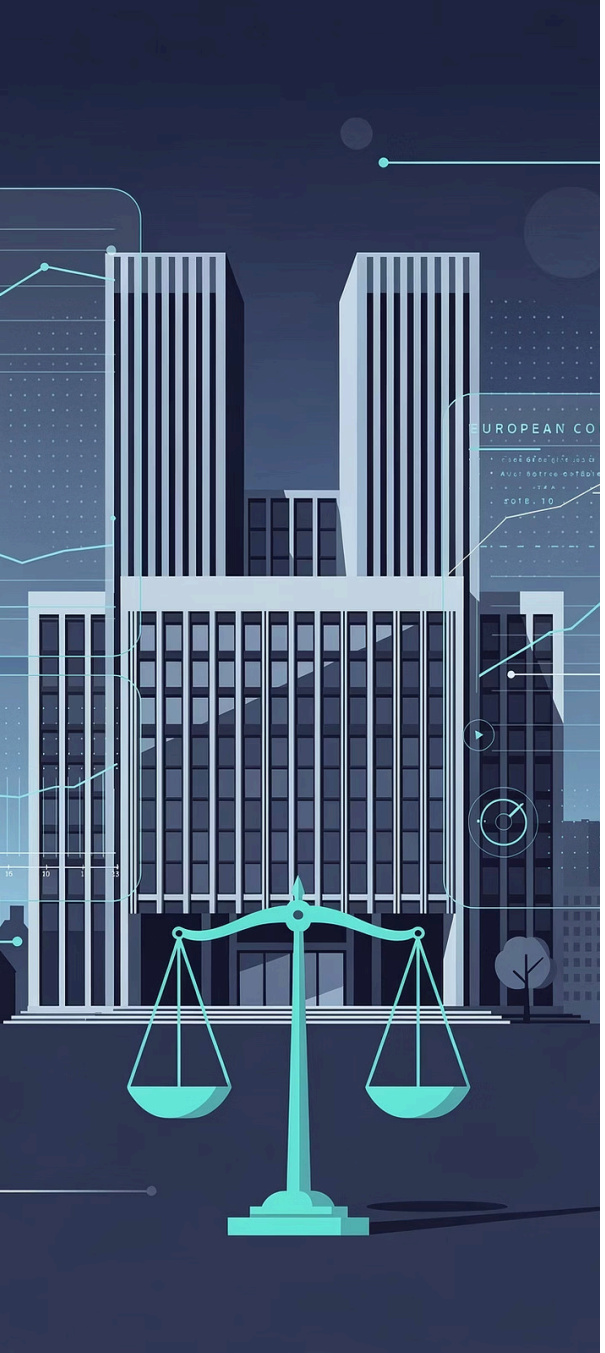
Betroffen sind Einrichtungen, die mehr als 500.000 Personen versorgen.

Die Pflichten umfassen: Risikoanalysen, physische Schutzmaßnahmen (Objektschutz, Notfallteams, Ausfallsicherheit) sowie eine Meldepflicht für Vorfälle.

Das Gesetz ergänzt — ersetzt nicht — die bestehenden NIS2/BSIG-Pflichten im IT-Bereich. Die Evaluierung erfolgt bereits nach 2 Jahren (statt ursprünglich geplanter 5 Jahre).

Einordnung für den Mittelstand

Praxis-Tipp: Für die meisten mittelständischen Unternehmen greift Schwelle nicht direkt. **Dennoch sollten Zulieferer und IT-Dienstleister solcher Betreiber die Anforderungen kennen: Erfahrungsgemäß werden sie vertraglich weitergereicht — oft in einem Umfang, der kaum erfüllbar ist.** Wir helfen Ihnen, Anforderungen realistisch umzusetzen, Verträge fair zu gestalten und Ihre Kundenbeziehungen zu sichern.



II. GERICHTE

Missbräuchliche Auskunftsersuchen können zurückgewiesen werden

- EuGH stärkt Unternehmen gegen wachsende Praxis missbräuchlicher Auskunftsanfragen (**DSGVO-Hopper**)
- **Auskunftsersuchen**, die nicht Datenschutzrechte wahrnehmen, sondern daraus Schadensersatzansprüche konstruieren oder andere datenschutzfremde Zwecke verfolgen, **können zurückgewiesen werden — auch schon beim ersten Ersuchen.**

EuGH, Urteil v. 19.3.2026 (Rs. C-526/24 — Brillen Rottler)

Was bedeutet das konkret?

Missbrauch ggf. beim ersten Ersuchen

Auskunftsersuchen ist missbräuchlich wenn es nicht Kontrolle der Datenverarbeitung dient, sondern ausschließlich um Voraussetzungen für Schadensersatzansprüche zu schaffen. Häufung von Anfragen ist keine Voraussetzung mehr.

Datenschutzfremde Zwecke

Gilt auch wenn Auskunftsersuchen primär anderen Zwecken dienen — z.B. in arbeitsrechtlichen Verfahren. Öffentlich zugängliche Informationen über systematisches Vorgehen des Antragstellers dürfen bei Missbrauchsprüfung berücksichtigt werden.

Schadensersatz nur bei konkretem Schaden

Für Schadensersatz muss tatsächlicher Schaden nachgewiesen werden — kein Schaden ohne konkreten Nachteil.

Hat der Betroffene den Schaden selbst herbeigeführt, scheidet Anspruch aus.

Wichtige Einschränkung & Praxis-Tipp: Hürde für eine Zurückweisung bleibt hoch — vorschnelle Ablehnung ist riskant, denn zu Unrecht zurückgewiesener Auskunftsanspruch kann Haftungsrisiken auslösen. Setzen Sie Prozesse auf, die auffällige oder strategisch motivierte Anfragen früh erkennen, dokumentieren und rechtlich einordnen. Wir prüfen für Sie, ob eine Zurückweisung im Einzelfall tragfähig ist.

II. GERICHTE

Offsite-Tracking — Wer das Pixel programmiert, haftet mit

OLG München, Endurteil v. 18.12.2025 (Az. 14 U 1068/25 e)

> Wer über eingebettete Tracking-Tools Nutzerdaten auch außerhalb der eigenen Plattform erhebt, muss das konkret rechtfertigen können — eine pauschale Datenschutzerklärung reicht nicht.

Offsite-Daten = DSGVO

Daten von fremden Websites/Apps via eingebettete Tools unterliegen vollständig der DSGVO, sobald eine Zuordnung zum Nutzerkonto möglich ist.

Personenbezug technischer IDs

IP-Adressen, Browser-IDs und Geräte-IDs sind personenbezogene Daten — auch wenn sie technisch aussehen.

Gemeinsame Verantwortlichkeit

Wer die Funktionalität des eingebetteten Tools mitbestimmt, ist gemeinsam Verantwortlicher nach Art. 26 DSGVO.

Datenminimierung

Großflächige, undifferenzierte Datenerhebung verstößt gegen Datenminimierung und Privacy by Default. Betroffene müssen ihre individuelle Betroffenheit nur plausibel darlegen.

Praxis-Tipp: Prüfen Sie, welche Tracking-Tools auf Ihrer Website oder App aktiv sind und ob diese auch außerhalb Ihrer Plattform Daten sammeln. Ihre Datenschutzerklärung muss konkret benennen, welche Daten zu welchem Zweck auf welcher Rechtsgrundlage verarbeitet werden. Wir unterstützen Sie bei der Überprüfung Ihres Tracking-Setups.

II. GERICHTE

Cookie-Haftung trifft auch Drittanbieter direkt

OLG Frankfurt, Urteil v. 11.12.2025 (Az. 6 U 81/23)

- Das Cookie-Verbot nach § 25 TDDDG gilt gegenüber jedermann —
- **Wer als Drittanbieter** (Analytics, Werbetechnologie, eingebettete Tools) **an der Cookie-Setzung auf fremden Websites mitwirkt, haftet selbst** als Anbieter.
- Eine vertragliche Regelung mit Websitebetreiber, die Cookies nur bei Einwilligung vorsieht, entlastet den Drittanbieter nicht.

Praxis-Tipp: Verlassen Sie sich nicht darauf, dass Ihr Drittanbieter die Einwilligung steuert. Stellen Sie technisch sicher, dass Cookies erst nach aktiver Zustimmung gesetzt werden — vor allem bei automatisch ladenden Drittskripten. Lassen Sie Ihr Consent-Management prüfen.

II. GERICHTE

Was ist eigentlich ein Vertrag im Sinne der DSGVO?

BGH (10.12.2025 – II ZR 132/24)

- Begriff **Vertrag** in Art. 6 (1) b DSGVO ist nicht nach nationalem Zivilrecht, sondern **europarechtlich auszulegen i**st.
- Maßgeblich ist, ob ein Rechtsverhältnis auf einer freiwilligen und selbstbestimmten Entscheidung beruht.
- BGH lässt für einen Vertrag ak„*all jene vertragsähnlichen Konstellationen*“ ausreichen, „*die gleichermaßen auf willentliche Entscheidungen des von der Verarbeitung Betroffenen zurückgehen*“.
- Im konkreten Fall liegt „Vertrag“ im Sinne der DSGVO vor, obwohl keine zwei korrespondierenden Willenserklärungen vorlagen.
- **Mitgliedschaften, Plattformnutzungen und ähnliche Rechtsverhältnisse** können als **Rechtsgrundlage nach Art. 6 Abs. 1 lit. b** DSGVO dienen, sofern die Datenverarbeitung zur Ausübung der damit verbundenen Rechte erforderlich ist.

Hinweis: Datenverarbeitungen können ggf. leichter auf *Vertrag* als Rechtsgrundlage gestützt werden als bisher.

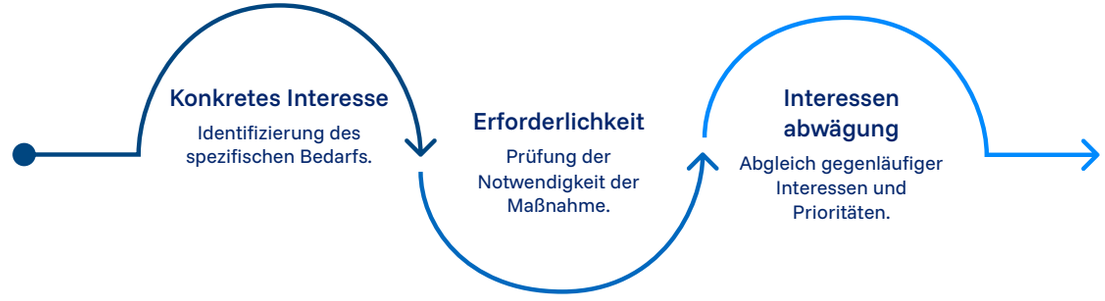
Praxis-Tipp: Prüfen Sie, ob Ihre bestehenden Rechtsgrundlagen und Datenschutzhinweise noch den aktuellen Anforderungen entsprechen - vor allem dort, wo Sie bisher auf berechtigtes Interesse ausgewichen sind, obwohl ein Vertragsverhältnis vorliegt.

III. BEHÖRDEN

Hamburger DSB: Dreistufiger Katalog zur Interessenabwägung

> Der HmbBfDI hat Fragenkatalog für die Prüfung des berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO) veröffentlicht.
>
> **Pauschale Interessenabwägungen dürften damit künftig nicht mehr als ausreichende Rechtsgrundlage gelten.**

HmbBfDI, veröffentlicht 08.01.2026



Tiefe und Umfang der Dokumentation richten sich nach Komplexität und Sensibilität der Verarbeitung — je sensibler, desto ausführlicher.

Eine pauschale Formulierung wie „zur Wahrung berechtigter Interessen" im Datenschutzhinweis reicht nicht mehr aus.

Praxis-Tipp: Wenn Sie Datenverarbeitungen auf berechtigtes Interesse als Rechtsgrundlage stützen, sollten Sie Ihre Interessenabwägungen auf Basis dieses Fragenkatalogs überarbeiten. Wir unterstützen Sie bei einer rechtssicheren Interessenabwägung

III. BEHÖRDEN

GPS-Tracking in Firmenfahrzeugen - Enge Grenzen, klare Pflichten

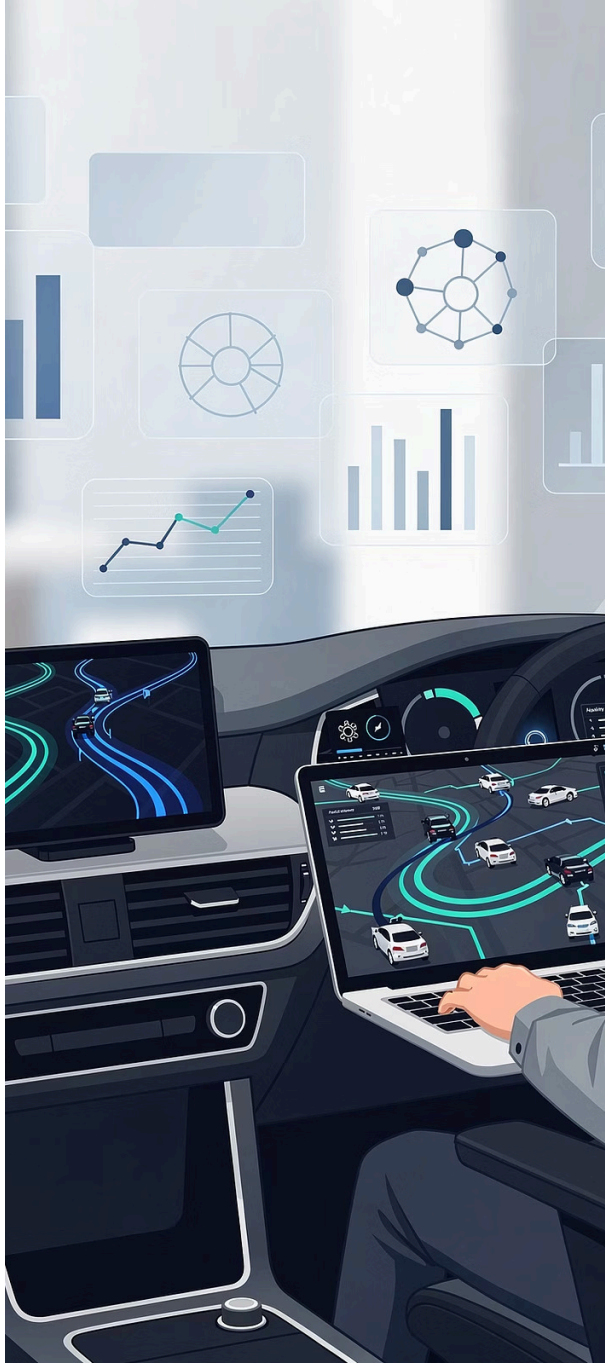
BayLDA, 15. Tätigkeitsbericht 2025

Grundsatz: GPS-Tracking ist nur ausnahmsweise zulässig

- GPS-Daten sind personenbezogen, sobald sie einem Fahrer zugeordnet werden können — das gilt nahezu immer. **Einwilligung taugt als Rechtsgrundlage im Arbeitsverhältnis in der Regel nicht** (fehlende Freiwilligkeit).
- Nicht zulässig: Routenkontrolle, Arbeitszeitüberprüfung oder abstrakte Diebstahlsprävention rechtfertigen GPS-Tracking grundsätzlich nicht.
- **Zulässig: Bei konkreter gesetzlicher Verpflichtung (z.B. Gefahrguttransporte) oder dokumentiertem Verdacht schwerer Pflichtverletzungen.**

⚠ **Hinweis:** Bei privater Fahrzeugnutzung ist Ortung in der Freizeit ausgeschlossen — Mitarbeiter müssen sie deaktivieren können.

Datenschutzfolgenabschätzung (DSFA) ist vor dem Einsatz zwingend.



III. BEHÖRDEN

E-Mail-Postfächer ausgeschiedener Mitarbeiter: Sofort handeln

BayLDA, 15. Tätigkeitsbericht 2025

Persönliche E-Mail-Postfächer ausgeschiedener Mitarbeitender müssen unverzüglich deaktiviert oder gelöscht werden. Monatelanger Weiterbetrieb ohne Abwesenheitsnotiz ist DSGVO-Verstoß — das BayLDA hat bereits Verwarnungen ausgesprochen.

- Ein kurzer Übergangszeitraum mit aktiver Abwesenheitsnotiz kann zulässig sein.
- Monatelange Weiterführung ohne Kennzeichnung: rechtswidrig — weder Art. 6 Abs. 1 b noch f DSGVO trägt das.
- Eingehende Mails Dritter werden ohne Wissen der Absender schutzlos verarbeitet.

Praxis-Tipp: Regeln Sie den Umgang mit Postfächern in einem Offboarding-Prozess: Wie lange bleibt das Postfach aktiv? Wer richtet die Abwesenheitsnotiz ein? Wann wird gelöscht? Wir helfen Ihnen, einen pragmatischen und datenschutzkonformen Prozess zu erstellen.

III. BEHÖRDEN

BayLfD: Dokumente technisch korrekt schwärzen - nicht nur optisch

BayLfD, Aktuelle Kurz-Information, März 2026

> Wer Dokumente mit geschwärzten Inhalten weitergibt, muss sicherstellen, dass die Schwärzung auch **technisch vollständig** ist — sonst können die Inhalte wiederhergestellt werden.

1 Das Problem bei PDFs

Bei PDF-Dokumenten reicht es nicht, Text schwarz einzufärben oder ein schwarzes Rechteck darüberzulegen — die Originaldaten bleiben im Dokument und lassen sich mit einfachen Mitteln sichtbar machen.

2 Korrekte Methoden

Geschwärzte Inhalte müssen technisch vollständig entfernt werden, z.B. durch spezialisierte Redaktionssoftware oder Umwandlung in ein gerastertes Bildformat ohne Textebene. Bei Papierdokumenten ist ein deckendes Schwärzungsverfahren mit anschließender Sichtkontrolle gegen Lichtquelle erforderlich.

3 Typische Fehlerquellen

Copy-Paste aus geschwärzten PDFs, Metadaten, Kommentarfelder und Dokumenteneigenschaften — all diese Bereiche können unbeabsichtigt sensible Informationen preisgeben.

Praxis-Tipp: Prüfen Sie, ob Schwärzungsmethode technisch vollständig und irreversibel ist. Bei **digitalen Dokumenten** gilt dabei der **Grundsatz "entfernen statt überdecken" - inklusive Metadaten und verborgenem Inhalt**. Und für **analoge Schwärzungen** gilt der **Grundsatz "überkleben oder ausschneiden, dann nur die Kopie herausgeben**".

III. BEHÖRDEN

BayLDA: EU-U.S. Data Privacy Framework — Kein gemeinsames Verständnis von HR-Daten

BayLDA, 15. Tätigkeitsbericht 2025

> Bei der Übermittlung von HR-Daten in die USA unter dem EU-U.S. DPF besteht nach wie vor **kein einheitliches Verständnis**, welche **Daten als „Human Resources Data" einzustufen sind** – mit erheblichen Folgen für die Rechtsgrundlage.

1

Besondere Anforderungen

Das DPF sieht für HR-Daten im Beschäftigungskontext besondere Anforderungen vor — u.a. müssen Arbeitnehmer effektive Rechtsmittel haben.

2

Unterschiedliches Begriffsverständnis

Unternehmen und US-Empfänger verstehen „HR-Daten" unterschiedlich weit — von Personalstammdaten bis hin zu Leistungsbeurteilungen, Krankmeldungen oder Gehaltsabrechnungen.

3

Lücken im Datenschutzniveau

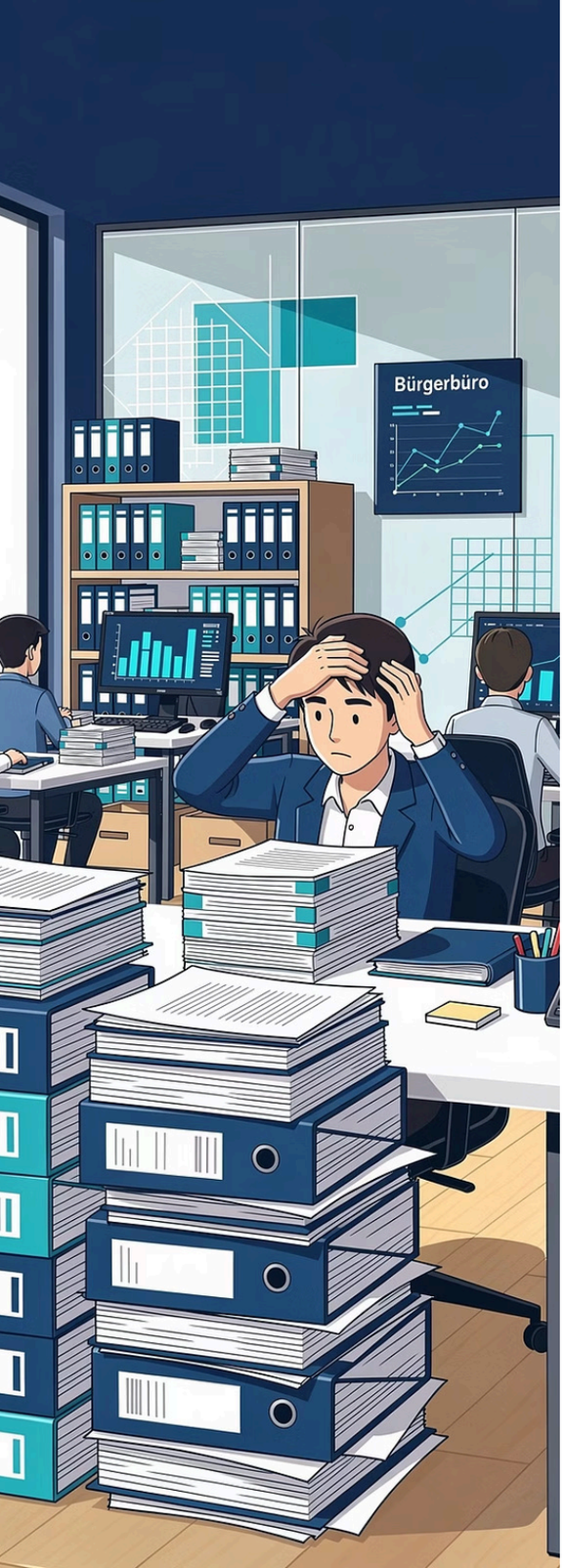
Ohne gemeinsames Begriffsverständnis drohen Lücken — der Angemessenheitsbeschluss greift nur, wenn die DPF-Zertifizierung des US-Empfängers die HR-Daten tatsächlich abdeckt.

4

Empfehlung des LDA

Vertraglich klarstellen, welche Datenkategorien als HR-Daten gelten — und dies mit dem US-Empfänger schriftlich fixieren.

Praxis-Tipp: Prüfen Sie, ob Ihr zertifizierter US-Empfänger HR-Daten explizit in seiner DPF-Zertifizierung ausweist – und definieren Sie im Auftragsverarbeitungsvertrag konkret, welche Datenkategorien darunter fallen.



III. BEHÖRDEN

Fast 10.000 Beschwerden beim BayLDA — ein Rekord mit Schattenseiten

BayLDA, 15. Tätigkeitsbericht 2025

Die Zahlen:

Das BayLDA verzeichnete 2025 knapp 10.000 Eingaben — 61 % mehr und Allzeithöchststand. Viele Beschwerden dienen erkennbar datenschutzfremden Zwecken. BayLDA fordert u.a. verwaltungsrechtliche Kosten für Beschwerden in Missbrauchsfällen.

Unsere Einschätzung:

Entwicklung ist auch Behörden anzulasten. Viele behördliche Anforderungen sind mit unternehmerischer Praxis unvereinbar. Wenn Orientierungshilfen praktisch nicht erfüllbare Erwartungen wecken überträgt sich das auch auf Betroffene. Datenschutz wird dann als sachfremder Hebel eingesetzt.

Anstatt Verwaltungskosten zu verlangen, sollten Behörden für praxisnahe, risikoorientierte Anforderungen und Empfehlungen sorgen, die Unternehmen tatsächlich umsetzen können.

IV. REGULIERUNG

Omnibus KI-Verordnung (AI Act)

EU-Rat beschliesst Position zu Vereinfachungen

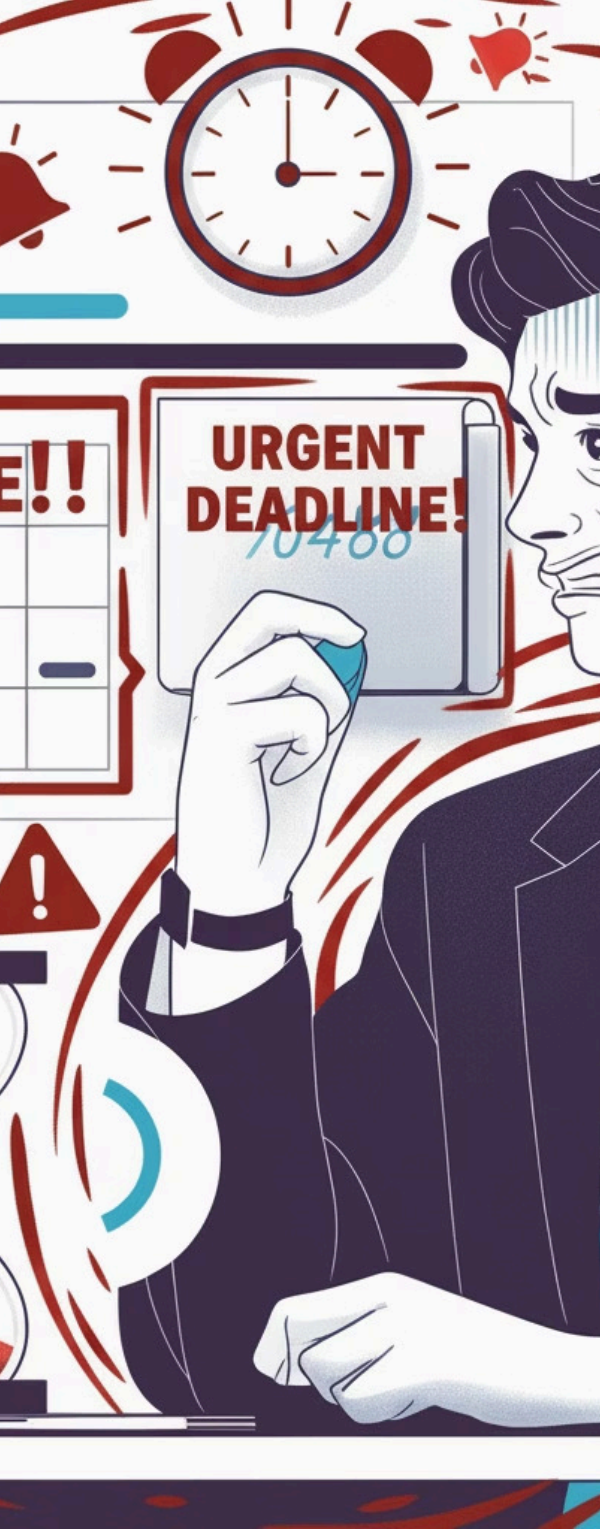
EU-Rat, Omnibus VII, März 2026

- **Neue feste Fristen:** Hochrisiko-KI Pflichten nach Anhang III gelten erst ab Dezember 2027, nach Anhang I ab August 2028
- **Reallabore:** Frist für KI-Sandbox-Umgebungen verschoben auf Dezember 2027
- **Weitere verbotene KI-Praktiken:** KI-gestützte Erstellung nicht-einvernehmlicher sexueller Inhalte und CSAM wird ausdrücklich verboten
- **AI Office:** Klarstellungen zu den Aufsichtskompetenzen des europäischen KI-Amts

Die gestaffelten Fristen geben Unternehmen mehr Planungssicherheit. Das ändert aber nichts daran, dass die Vorbereitungen jetzt laufen müssen — wer erst 2027 anfängt, wird die Fristen

Praxis-Tipp: Geringfügig verlängerte Fristen geben Unternehmen nur wenig Aufschub. Das ändert nichts daran, dass die Vorbereitungen jetzt laufen müssen — wer erst 2027 anfängt, wird die Fristen nicht einhalten können.

Wir helfen Ihnen KI-Systeme rechtskonform einzusetzen – mit Experten für KI-Compliance.



Data Act: Bundesnetzagentur wird zentrale Durchsetzungsbehörde

Deutscher Bundestag, 1. Lesung 16.01.2026, BT-Drs. 21/2998

Das nationale Durchführungsgesetz zum Data Act ist im parlamentarischen Verfahren.

Die lang fehlende Zuständigkeitsklarheit kommt: Die **Bundesnetzagentur** wird zentrale Anlaufstelle für Aufsicht und Durchsetzung — mit Zwangsgeldern bis zu **500.000 Euro**. Soweit personenbezogene Daten betroffen sind, liegt die Zuständigkeit bei der **BfDI**. Die Landesdatenschutzbehörden spielen insoweit keine Rolle.

Ob sich das zentralisierte Modell in der Praxis bewährt, wird sich zeigen.

Achtung: Viele Pflichten des Data Act gelten bereits. Weitere wie Access-by-Design gelten ab 12.09.2026. **Betroffene Unternehmen müssen handeln.**

Nutzen Sie unseren kostenlosen Anwendbarkeitscheck, Reifegrad - Analyse und To-Do Checkliste mit 100+ konkreten Maßnahmen von Strategie bis zur technischen Umsetzung. Sofort umsetzbar.

PRICOM – Pragmatische Experten für Datenschutz, KI-Compliance und datengetriebenes Business

Data Act Beratung: Chancen Nutzen & Risiken Minimieren | PRICOM

Strategische Data-Act-Beratung. Business sichern, neue Chancen nutzen. Pragmatisch und effizient für IoT, Cloud, XaaS, Datenzugang, Switching, Verträge. Kostenloser Anwendbarkeitscheck und...

Data, AI & IT-Security – We get it done

Datenschutz (externer DSB)

Effizienter und pragmatischer DSB - **ab 99€**

KI-Kompetenz Schulungen

Mit Zertifikat nach Art. 4 KI-VO **ab 1€/Nutzer** – effizient, kostengünstig, sofort 24/7 einsetzbar

KI-Kompetenz Akademie

KI-Compliance & AI Officer

Rechtssichere und erfolgreiche KI-Nutzung

IT-Security & Cybersicherheit

NIS2/BSIG, ISO 27001, ISO 42100, ISMS & Audits

NIS2 Geschäftsleitungsschulung

Data Act

Strategie bis Umsetzung mit kostenlosen Anwendbarkeitschecks, Reifegrad Analysen und Checklisten

Data Act Beratung

Business sichern, Risiken minimieren, Chancen nutzen.

Sprechen Sie unverbindlich und vertraulich mit uns.

Kontakt | LinkedIn | Website