

NEWS BOX

DATENSCHUTZ



INHALTSVERZEICHNIS

- 2 Editorial
- 3 Umgang mit E-Mail-Postfächern bei Abwesenheit oder Ausscheiden von Beschäftigten
- 4 Auskunftsrecht nach Art. 15 DS-GVO gegenüber Rechtsanwält:innen
- 5 Kein Auskunftsverweigerungsrecht juristischer Personen gegenüber Aufsichtsbehörden
- 6 Datenschutzrechtliche Bewertung eines sog. Lettershop-Verfahrens
- 8 BayLfD baut Informationsangebot zu KI und Datenschutz aus
- 9 Bafin wird Marktüberwachungsbehörde für KI-Systeme im Finanzsektor
- 10 Transparenz- und Anonymisierungsmängel bei KI-gestütztem Inkasso
- 11 Bußgeldverfahren wegen „Mitarbeiterexzessen“ im Gesundheits- und Polizeibereich
- 12 FAQ zum Datenschutz bei Inkassounternehmen
- 13 Kein Löschungsanspruch nach dem Bewerbungsverfahren
- 14 Neues Arbeitspapier: Vernichtung und Entsorgung von Datenträgern
- 16 Impressum

AUSGABE

9/2026



Levent Ferik

EDITORIAL

KI, KI und nochmals KI

Wer den druckfrischen Jahresbericht 2025 der Berliner Beauftragten für Datenschutz und Informationsfreiheit durchscrollt, kommt an einer Beobachtung kaum vorbei: Künstliche Intelligenz (KI) ist in der Aufsichtspraxis endgültig im Tagesgeschäft angekommen. Bereits ein Blick ins Inhaltsverzeichnis zeigt ein eigenes Kapitel „Künstliche Intelligenz“ mit fünf Unterpunkten – von der KI-Rechtsgrundlage im Berliner E-Government-Gesetz über Anonymisierungsfragen beim KI-Training bis zur beantragten App-Store-Sperre von DeepSeek. Schon in den ersten Kapiteln des Berichts – Vorwort, DSK-Vorsitzbericht – taucht das Kürzel „KI“ gebetsmühlenartig auf: Gründung eines eigenen DSK-Arbeitskreises Künstliche Intelligenz, eine Orientierungshilfe zu technisch-organisatorischen Maßnahmen bei KI-Systemen, eine weitere zu Retrieval-Augmented-Generation-Systemen, dazu Diskussionen um die geplante KI-VO-Reform im Digital-Omnibus-Verfahren. Wer mag, kann sich beim Lesen ein Bingo-Feld basteln.

Bemerkenswert ist dabei weniger die schiere Häufigkeit als die thematische Streubreite. KI taucht im Bericht nicht nur dort auf, wo man sie erwartet – etwa bei der Bewertung von Sprachmodellen oder Chatbots –, sondern zieht sich quer durch nahezu alle Sachgebiete: im Beschäftigtendatenschutz beim Einsatz von KI-Assistenzsystemen wie dem haus eigenen „BärGPT“, im Bildungsbereich beim Einsatz

von KI in Schulen, im Wirtschaftsrecht bei der Frage, ob Kundenanfragen ungefragt zu Trainingszwecken verwendet werden dürfen, im Verbraucherschutz bei Widerspruchsrechten gegen KI-Training – und selbst im digitalpolitischen Grundsatzstreit um die Zentralisierung der Datenschutzaufsicht schwingt die KI-Frage mit. Auch die Aufsichtsbehörde selbst ist längst nicht mehr nur Prüferin, sondern eigene Anwenderin: In dem Bericht wird die datenschutzrechtliche Begleitung eines KI-Assistenten für die eigene Verwaltung mit derselben Selbstverständlichkeit geschildert wie ein Bußgeldfall.

Man muss diesen Befund nicht dramatisieren – die Datenschutzaufsicht war schon immer dort, wo neue Verarbeitungstechnologien auftauchen, von der Videoüberwachung bis zum Smart Meter. Aber die schiere Dichte, mit der sich Aufsichtsbehörden inzwischen mit Sprachmodellen, Trainingsdaten und Anonymisierungsfragen befassen, macht deutlich: KI ist kein Sonderthema mehr für eine Handvoll Spezialist:innen, sondern fester Bestandteil des Beratungsalltags – quer durch Wirtschaft, Verwaltung, Bildung und Gesundheitswesen. Wer als Datenschutzbeauftragte:r im Jahr 2026 noch glaubt, das Thema mit einer einzigen Richtlinie abhaken zu können, dürfte sich grundlegend irren.



Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com



Umgang mit E-Mail-Postfächern bei Abwesenheit oder Ausscheiden von Beschäftigten

Der Umgang mit personalisierten E-Mail-Konten ausgeschiedener oder länger abwesender Mitarbeitender zählt zu den häufig nachgefragten Beratungsthemen im Beschäftigtendatenschutz. Im Zentrum steht die Frage, ob und unter welchen Voraussetzungen Arbeitgeber:innen auf betroffene Postfächer zugreifen dürfen.

Prävention durch klare Prozesse

Verantwortliche sollten datenschutzrechtlichen Konflikten bereits durch organisatorische Weichenstellungen vorbeugen. Zu prüfen ist zunächst, ob personalisierte Postfächer überhaupt erforderlich sind oder ob Funktionsadressen – etwa buchhaltung@verantwortlicher.de – ausreichen,

die auch nach Ausscheiden einzelner Beschäftigter fortgeführt werden können. Bei personalisierten Postfächern empfiehlt sich die Anweisung, zukunftsrelevante Inhalte grundsätzlich außerhalb des persönlichen Kontos abzulegen, ergänzt durch Abwesenheitsassistenten bei Abwesenheit und eine Abschaltung bzw. Zugangsverweigerung bei dauerhaftem Ausfall. Von sogenannten Catch-all-Postfächern, die nicht zuordenbare E-Mails sammeln, ist abzuraten, da hierdurch personenbezogene Daten ohne Rechtsgrundlage verarbeitet werden können.

Vorgehen beim Ausscheiden

Vor ihrem Ausscheiden sollten Beschäftigte private E-Mails löschen. Betriebliche Nachrichten sind an die Vertretung oder die Nachfolge weiterzuleiten oder zu löschen, sofern sie nicht mehr benötigt werden. Ist dies, etwa bei einer fristlosen Kündigung, nicht mehr möglich, sollte eine benannte Person (z. B. ein Betriebsratsmitglied, ein:e Datenschutzbeauftragte:r oder eine von den Betroffenen bestimmte Person) das Postfach ausschließlich zur Aussortierung betrieblicher Inhalte einsehen und offensichtlich private Nachrichten unverzüglich löschen.

Zugriff durch die Geschäftsführung

Eine Kenntnisnahme oder Weiterleitung durch die Geschäftsführung ist nur dann zulässig, wenn die private Nutzung des dienstlichen Postfachs ausdrücklich untersagt war. Jede E-Mail ist auf ihren geschäftlichen oder privaten Charakter zu prüfen – häufig bereits erkennbar am Header oder an der Betreffzeile. Ergibt sich der private Charakter erst nach dem Öffnen, ist diese Nachricht sofort ohne weitere Kenntnisnahme zu schließen. Die betroffene Person ist über die Maßnahme zu informieren. Ist die private Nutzung generell gestattet, empfiehlt sich der Abschluss einer Betriebs- bzw. Dienstvereinbarung. In jedem Fall gilt: Der Umfang zulässiger privater Nutzung sollte schriftlich festgelegt sein, ebenso der Prozess zur Abwicklung personalisierter Postfächer nach Beendigung des Beschäftigungsverhältnisses.



Auskunftsrecht nach Art. 15 DS-GVO gegenüber Rechtsanwält:innen

Beschwerden über unbeantwortete oder unvollständig beantwortete Auskunftersuchen gegenüber Kanzleien und Einzelanwält:innen gehören zu den regelmäßig auftretenden Fallkonstellationen der Aufsichtspraxis. Im Fokus steht zumeist die Frage der Reichweite des Auskunftsrechts betroffener Personen gegenüber Berufsheimnisträger:innen.

Grundsatz: DS-GVO gilt auch für Rechtsanwält:innen

Rechtsanwält:innen unterliegen als Verantwortliche im Sinne der Datenschutz-Grundverordnung (DS-GVO) grundsätzlich uneingeschränkt deren Vorgaben und müssen geeignete Maßnahmen zur Erfüllung von

Informations- und Auskunftspflichten treffen. Besteht ein Mandatsverhältnis, können Mandant:innen ihre Betroffenenrechte daher regelmäßig ohne Einschränkung geltend machen.

Einschränkung außerhalb des Mandatsverhältnisses

Fehlt ein Mandatsverhältnis, kann die Auskunft nach der bereichsspezifischen Regelung des § 29 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) verweigert werden, sofern dadurch Informationen offenbart würden, die aufgrund einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen überwiegender berechtigter Interessen Dritter, geheim zu halten sind. Als einschlägige Geheimhaltungsvorschrift kommt dabei etwa § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO) in Betracht.

Entscheidend ist jedoch, dass bereits der Wortlaut („soweit“) einen generellen Ausschluss des Auskunftsrechts verbietet. Rechtsanwält:innen müssen vielmehr im jeweiligen Einzelfall prüfen, ob und in welchem Umfang die Auskunftserteilung geheimhaltungsbedürftige, der anwaltlichen Verschwiegenheitspflicht unterfallende Tatsachen berühren würde. Keine Geheimhaltungspflicht besteht dagegen bei offenkundigen Tatsachen oder in Konstellationen ohne schutzwürdiges Geheimhaltungsinteresse. Der Auskunftsanspruch entfällt somit nur insoweit, als nicht offenkundige, dem anwaltlichen Geheimnisschutz unterliegende Informationen betroffen sind. Im Übrigen ist gegebenenfalls eine Teilauskunft zu erteilen.

Praxishinweis zur Bearbeitung

Auskunftersuchen sind grundsätzlich innerhalb der Monatsfrist des Art. 12 Abs. 3 DS-GVO zu beantworten. Wird die Auskunft ganz oder teilweise verweigert, ist dies der antragstellenden Person unverzüglich, spätestens jedoch innerhalb eines Monats mitzuteilen. Unter Bezugnahme auf die einschlägigen Rechtsvorschriften ist die Verweigerung zu begründen und die Person ist auf die Möglichkeit von Aufsichtsbeschwerde und gerichtlichem Rechtsbehelf hinzuweisen.



Kein Auskunftsverweigerungsrecht juristischer Personen gegenüber Aufsichtsbehörden

Das Verwaltungsgericht (VG) Berlin (VG Berlin, Urteil vom 9. Oktober 2025, VG 1 K 607/22) hat in einem noch nicht rechtskräftigen Urteil die aufsichtsbehördlichen Auskunftsbefugnisse nach Art. 58 Abs. 1 lit. a DS-GVO bestätigt und konkretisiert.

Ausgangsfall: Adressvermietung ohne Rechtsgrundlage

Hintergrund war die Verwarnung eines Buchverlags, der Kundendaten ohne Einwilligung und ohne sonstige gesetzliche Grundlage zu Werbezwecken an Geschäftskunden vermietet hatte. Im Rahmen der Verwarnung wurde das Unternehmen verpflichtet, Angaben zum Umfang der Datenvermietung in bestimmten Folgequartalen zu machen. Nach Verweigerung dieser Auskunft erging ein Auskunftsheranziehungsbescheid mit angedrohtem Zwangsgeld von 500 Euro. Die dagegen gerichtete Klage blieb erfolglos.

Reichweite der Auskunftsbefugnis bestätigt

Das Gericht stellte klar, dass die Auskunftsbefugnis nach Art. 58 Abs. 1 lit. a DS-GVO nicht an einen Verdacht gebunden ist, sondern sich aus der allgemeinen Überwachungs- und Durchsetzungsaufgabe der Aufsichtsbehörden ergibt. Sie besteht danach auch dann fort, wenn ein Verstoß bereits feststeht – etwa um dessen Ausmaß oder die Beteiligung weiterer Akteure aufzuklären.

Zentral ist zudem die Aussage des Gerichts zur Selbstbelastungsfreiheit: Dieser verfassungsrechtlich verankerte Grundsatz knüpft an die Menschenwürde und das allgemeine Persönlichkeitsrecht an und kommt daher nur natürlichen Personen zugute. Juristische Personen bilden ihren Willen durch Organe, unterliegen im Ordnungswidrigkeitenrecht nur eingeschränkter Verantwortlichkeit und können sich nicht strafbar machen. Eine gegen sie verhängte Geldbuße enthalte keinen Schuldvorwurf im personalen Sinne. Sie können sich folglich nicht auf ein Auskunftsverweigerungsrecht berufen.

Bleibt ein Unternehmen bei fortgesetzter Weigerung, kommen neben Zwangsgeldern auch Bußgelder wegen Verstoßes gegen die Kooperationspflicht aus Art. 31 DS-GVO in Betracht. Die unterlegene Klägerin hat die Zulassung der Berufung beantragt, sodass eine obergerichtliche Klärung noch aussteht.



Datenschutzrechtliche Bewertung eines sog. Lettershop-Verfahrens

In ihrem Jahresbericht 2025 (Ziffer 2) [↗](#) setzt sich die Berliner Beauftragte für Datenschutz und Informationsfreiheit kritisch mit einem Urteil des Verwaltungsgerichts Berlin zur gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO im sogenannten Lettershop-Verfahren auseinander. Gegenstand des Verfahrens war eine Verwarnung gegen ein werbendes Unternehmen, das über eine Adresshändlerin Zielgruppen anhand sozioökonomischer Merkmale wie Wohnort und Kaufkraft für den Versand von Werbeschreiben auswählen ließ.

Gericht verneint gemeinsame Verantwortlichkeit

Das VG Berlin hob die Verwarnung auf und verneinte eine gemeinsame Verantwortlichkeit von Auftraggeber und Adresshändlerin. Zwar bestimme das beauftragende Unternehmen im eigenen wirtschaftlichen Interesse den Verarbeitungszweck mit, auf die Verarbeitungsmittel – von der Anreicherung der Adressdaten bis zur Versendung – nehme es jedoch keinen Einfluss; diese lägen vollständig bei der Adresshändlerin. Die bloße Vorgabe einer Zielgruppe genüge nicht als Mitbestimmung der Mittel im Sinne von Art. 4 Nr. 7 DS-GVO. Ob überhaupt eine tragfähige Rechtsgrundlage für die Verarbeitung vorlag, ließ das Gericht ausdrücklich offen. Das Urteil ist nicht rechtskräftig.

Aufsichtsbehörde hält an gemeinsamer Verantwortlichkeit fest

Die Berliner Beauftragte teilt diese Rechtsauffassung nicht und hat Berufung eingelegt, die vom Gericht ausdrücklich zugelassen wurde. Nach ihrer Bewertung legen beide Seiten Zweck und wesentliche Mittel der Verarbeitung gemeinsam fest: Das auftraggebende Unternehmen initiiere die Verarbeitung durch die Entscheidung, eine bestimmte Zielgruppe zu bewerben, und lege damit faktisch fest, wessen Daten verarbeitet werden und zwar unabhängig davon, ob es Zugriff auf die konkreten personenbezogenen Daten hat. Unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofs (EuGH) betont die Behörde, dass eine Entscheidungsmacht über Zwecke und Mittel auch ohne eigenen Datenzugriff bestehen könne. Eine künstliche Aufspaltung des Verarbeitungsprozesses dürfe nicht dazu führen, dass die wirtschaftlich profitierende und initiiierende Partei aus der datenschutzrechtlichen Verantwortung entlassen werde.

Angesichts der grundsätzlichen Bedeutung für die Auslegung von Art. 26 DS-GVO im gesamten Adresshandelsbereich bleibt die obergerichtliche Klärung dieser praxisrelevanten Frage abzuwarten.



Eine
Jubiläumsbühne
für den
Datenschutz.



50. DAFTA

12.-13. November 2026

Künstliche Intelligenz – Werkzeug oder Partner? Herausforderungen für den Datenschutz!

45 RDV-FORUM

11. November 2026

Hybrid:
Online &
in Köln

Jetzt anmelden: www.dafta.de



BayLfD baut Informationsangebot zu KI und Datenschutz aus

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) erweitert kontinuierlich sein Angebot zur datenschutzkonformen Gestaltung von KI-Einsatzszenarien in der bayerischen Verwaltung. Hintergrund ist die zunehmende Nutzung von KI-Anwendungen durch öffentliche Stellen, welche bei der Verarbeitung personenbezogener Daten datenschutzrechtliche Anforderungen auslöst. Zentrales Referenzdokument bleibt die Orientierungshilfe „Datenschutz bei KI-Projekten in der bayerischen Verwaltung“ [↗](#), die den rechtlichen Rahmen aus KI-Verordnung sowie unionalem und nationalem Datenschutzrecht zusammenführt.

Reihe „AI in a nutshell“ wächst weiter

Ergänzend zur umfassenden Orientierungshilfe veröffentlicht der BayLfD kompakte Praxispapiere [↗](#) zu einzelnen Einsatzszenarien aus seiner Prüf- und Beratungstätigkeit. Mittlerweile liegen sechs Ausgaben vor, unter anderem zu Themen wie Anbindung von RAG-Subsystemen, KI-gestützte Übersetzungstools, LLM-Chatbots, Recherche-Unterstützung, Schreibassistenten und KI-basierte Textzusammenfassung. Besonders praxisrelevant ist die vierte Ausgabe zu KI-Systemen zur Recherche-Unterstützung [↘](#), die typischerweise Sprachmodelle mit Anbindung an behördeninterne Dokumentensammlungen, Fachdatenbanken oder Register kombinieren. Das Papier benennt konkrete Prüfpunkte entlang von Implementierung und Nutzung. Dazu zählen die erforderliche Freigabe solcher Systeme durch die einsetzende Stelle, KI-Kompetenzschulungen nach Art. 4 KI-VO, die Deaktivierung eines „Nachtrainings“ mit Eingabedaten sowie die Minimierung von Nutzerdaten – etwa durch eine restriktive Speicherung der Prompthistorie. Bei der Nutzung mahnt der BayLfD insbesondere die Vermeidung personenbezogener Eingaben ohne Rechtsgrundlage sowie eine sorgfältige Prüfung der Ausgaben auf Richtigkeit an, da KI-Systeme auch Halluzinationen – etwa erfundene Gerichtsentscheidungen oder Quellen – als faktisch präsentieren können. Ergänzend verweist das Papier auf die Kennzeichnungspflicht für KI-generierte Inhalte nach Art. 50 KI-Verordnung (KI-VO), die entfällt, sobald Ausgaben redaktionell überarbeitet und fachlich geprüft werden. Abgerundet wird das Angebot durch einschlägige Beiträge aus den Tätigkeitsberichten sowie durch Verweise auf Stellungnahmen des Europäischen Datenschutzausschusses und auf Positionspapiere der Datenschutzkonferenz, darunter die Hambacher Erklärung zur Künstlichen Intelligenz.



Bafin wird Marktüberwachungsbehörde für KI-Systeme im Finanzsektor

Mit Inkrafttreten des Gesetzes zur Durchführung der europäischen KI-Verordnung (KI-Marktüberwachungs- und Innovationsförderungsgesetz, KI-MIG) am 29. Juli 2026 übernimmt die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) [die](#) Marktüberwachung für KI-Systeme, die in direktem Zusammenhang mit einer regulierten Finanztätigkeit stehen. Die neue Zuständigkeit betrifft nach § 2 Abs. 3 KI-MIG von der Bafin oder der Europäischen Zentralbank (EZB) beaufsichtigte Finanzunternehmen, Emittenten signifikanter vermögenswertreferenzierter Token sowie die Versorgungsanstalt des Bundes und der Länder. Für Datenschutzbeauftragte in Finanzunternehmen ergibt sich damit eine zusätzliche Aufsichtsschnittstelle neben der etablierten DS-GVO-Aufsicht.

Umfang der Marktüberwachung

Die Bafin prüft künftig, ob KI-Systeme die verbotenen Praktiken nach Art. 5 KI-VO einhalten, ob die Transparenzpflichten nach Art. 50 KI-VO erfüllt werden – etwa bei Chatbots in der Kundenkommunikation – und ob Unternehmen gemäß Art. 4 KI-VO Maßnahmen zur Förderung der KI-Kompetenz ihres Personals ergreifen. Ab dem 2. Dezember 2027 kommen die Anforderungen an Hochrisiko-KI-Systeme hinzu, worunter nach Anhang III Nr. 5 lit. b und c KI-VO insbesondere Systeme zur Kreditwürdigkeitsprüfung sowie zur Risikobewertung und Preisbildung in der Lebens- und Krankenversicherung fallen. KI-Anwendungen ohne unmittelbaren Finanzmarktbezug, beispielsweise im Personalmanagement, verbleiben in der Zuständigkeit der Bundesnetzagentur. Bei Verstößen gegen die KI-Verordnung kann die Bafin Bußgelder verhängen.

Gestaffeltes Inkrafttreten

Bestimmte KI-Praktiken sind bereits seit dem 2. Februar 2025 untersagt, insbesondere Systeme zur Auswertung besonders schützenswerter Informationen mit diskriminierendem Potenzial. Die ersten Transparenzpflichten gelten ab dem 2. August 2026, die Anforderungen an Hochrisiko-KI-Systeme ab Dezember 2027.

Praxisrelevanz für die Governance

Die Bafin empfiehlt Finanzunternehmen, sich frühzeitig mit den neuen Anforderungen auseinanderzusetzen und sie in ihre bestehenden Governance-, Risiko- und Compliance-Strukturen zu integrieren, bspw. etwa durch Anknüpfung an das nach EU-Verordnung 2022/2554 (Digital Operational Resilience Act, DORA) bereits vorgesehene IKT-Asset-Inventar. Da sich datenschutz- und KI-rechtliche Anforderungen bei KI-gestützten Verarbeitungen personenbezogener Daten regelmäßig überschneiden, ist die neue Aufsichtszuständigkeit der Bafin auch für die Abstimmung von Datenschutz- und KI-Compliance in Finanzunternehmen unmittelbar relevant.



Transparenz- und Anonymisierungsmängel bei KI-gestütztem Inkasso

In ihrem Jahresbericht 2025 schildert die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) die Ergebnisse einer Vor-Ort-Prüfung bei einem Inkassounternehmen, das Schuldnerdaten mittels KI und Verhaltensforschung analysiert, um Ansprachekanal, Tonalität und Kontaktzeitpunkt zu optimieren. Über die reine Forderungseinziehung hinaus wurden die Daten zudem zum Training und zur Optimierung der eingesetzten KI-Modelle verwendet. Dabei stellte die Behörde mehrere Verstöße gegen die DS-GVO fest, die exemplarisch für Risiken beim Einsatz von KI in datenintensiven Geschäftsprozessen stehen.

Transparenzdefizit bei Zweckänderung

Da die Schuldnerdaten nicht bei den Betroffenen selbst erhoben wurden, richtete sich die Informationspflicht nach Art. 14 DS-GVO. Der

mit der ersten Zahlungsaufforderung versandte Datenschutzhinweis enthielt jedoch keinen Hinweis auf die zweckändernde Weiterverarbeitung zu KI-Trainingszwecken. Dieser fand sich erst in der verlinkten Datenschutzerklärung der Website. Nach Auffassung der BlnBDI genügt dies nicht den Anforderungen an Mehrebenen-Datenschutzhinweise: Wesentliche, für Betroffene nicht ohne Weiteres erwartbare Verarbeitungszwecke müssen bereits auf der ersten Informationsebene, hier: im ursprünglichen Schreiben, benannt werden, insbesondere da keine Kundenbeziehung zum Unternehmen bestand.

Vermeintliche Anonymisierung als Scheinlösung

Besondere praktische Relevanz hat der technische Befund der Prüfung: Das Unternehmen hatte in der Analyseumgebung direkte Identifikatoren wie Namen, Adressen, Aktenzeichen und IBAN gelöscht und die Daten als anonym eingestuft. Die technische Prüfung der BlnBDI ergab jedoch, dass eine Re-Identifizierung eines Großteils der Betroffenen weiterhin möglich war – über gespeicherte Hash-Werte von Namen, Adressen und Geburtsdaten sowie über Informationen aus aufbewahrungspflichtigen Geschäftsbriefen. Dieser Fall verdeutlicht, dass das Entfernen offensichtlicher Identifikatoren allein keine wirksame Anonymisierung im Sinne der DS-GVO begründet, solange eine Re-Identifizierung mit vertretbarem Aufwand möglich bleibt.

Auswirkungen auf die Interessenabwägung

Die BlnBDI stellte zudem klar, dass ein bestehendes Transparenzdefizit auch die Berufung auf ein überwiegendes berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DS-GVO gefährden kann: Fehlen wesentliche Informationen bereits auf erster Ebene, können Betroffene ihr Widerspruchsrecht faktisch nicht ausüben. Dies ist im Rahmen der Interessenabwägung zu berücksichtigen. Die Behörde gibt an, die festgestellten Verstöße aufgrund der hohen Zahl betroffener Personen zur Prüfung eines Bußgeldverfahrens an ihre Sanktionsstelle abzugeben.



Bußgeldverfahren wegen „Mitarbeiterexzessen“ im Gesundheits- und Polizeibereich

Die BlnBDI berichtet in ihrem Jahresbericht 2025  über eine Vielzahl von Bußgeldverfahren wegen sogenannter Mitarbeiterexzesse – Fälle, in denen Beschäftigte personenbezogene Daten, auf die sie im Rahmen ihrer dienstlichen Tätigkeit berechtigten Zugriff hatten, unbefugt zu privaten Zwecken verarbeiteten. Betroffen waren insbesondere der Gesundheits- und der Polizeibereich. Die Fälle verdeutlichen die datenschutzrechtliche Verantwortungsverteilung bei missbräuchlichem Datenzugriff durch Beschäftigte.

Verantwortungszurechnung beim Mitarbeiterexzess

Wenn Beschäftigte Daten weisungsgemäß im Rahmen ihrer Tätigkeit verarbeiten, wird dies datenschutzrechtlich dem Arbeitgeber als

Verantwortlichem zugerechnet. Nutzen sie hingegen dienstlich zugängliche Daten zu eigenen, privaten Zwecken, werden sie selbst zu Verantwortlichen – mangels beruflichem Anlass fehlt es dann regelmäßig an einer Rechtsgrundlage. Solche Verstöße stellen keine eigenen Pflichtverletzungen des Arbeitgebers dar. Bei Kenntnissnahme ist dieser jedoch unverzüglich zur Meldung nach Art. 33 Abs. 1 DS-GVO verpflichtet und muss durch geeignete technisch-organisatorische Maßnahmen sowie regelmäßige Schulungen das Risiko unbefugter Zugriffe minimieren.

Fälle aus dem Gesundheitsbereich

Im Berichtszeitraum verhängte die BlnBDI mehrere Bußgelder gegen Beschäftigte im Gesundheitswesen, darunter gegen einen Mitarbeiter, der private Filmaufnahmen aus einer Klinik weiterleitete, sowie gegen einen Arzt, der ohne erkennbaren dienstlichen Grund die Gesundheitsdaten einer unterstellten Beschäftigten sowie den Infektionsstatus seines erkrankten Assistenzarztes im Krankenhausinformationssystem abrief. In einem weiteren Fall nutzte ein Rezeptionist einer psychiatrischen Ambulanz die E-Mail-Adresse einer Patientin für eine private Kontaktaufnahme.

Unbefugte POLIKS-Abfragen bei der Polizei

Auch im Polizeilichen Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS) registrierte die BlnBDI wiederholt dienstlich nicht veranlasste Abfragen – etwa zur Einflussnahme auf ein eigenes Ermittlungsverfahren, zur unbefugten Kontrolle einer Kollegin oder zur gezielten Bloßstellung eines Anzeigenerstatters gegenüber dessen Vorgesetzten. Bereits die unberechtigte Abfrage allein verletzt das Recht auf informationelle Selbstbestimmung und stellt unabhängig von einer Weiterverwendung einen eigenständigen Verstoß dar. Zur besseren disziplinarrechtlichen Aufarbeitung solcher Fälle hat die BlnBDI gemeinsam mit dem Justizariat und den Disziplinarstellen der Polizei ein einheitliches Verfahren zur gegenseitigen Information und Aktenübersendung etabliert.



FAQ zum Datenschutz bei Inkassounternehmen

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) hat einen umfassenden FAQ-Beitrag zum Datenschutz bei der Forderungseinzahlung durch Inkassounternehmen [veröffentlicht](#). Der Beitrag bündelt die wesentlichen Rechtsgrundlagen und die Aufsichtspraxis für die Datenweitergabe zwischen Gläubiger:innen, Inkassounternehmen sowie Auskunftsteilen und kann auch in der Beratungspraxis von Datenschutzbeauftragten in Unternehmen mit Forderungsmanagement relevant werden.

Rechtsgrundlagen der Datenverarbeitung

Die Übermittlung von Schuldnerdaten an Inkassounternehmen bedarf keiner Einwilligung, sondern stützt sich je nach vertraglicher Konstellation auf Art. 6 Abs. 1 lit. b oder lit. f DS-GVO. Verarbeitet werden dürfen

dabei nur die zur Forderungsdurchsetzung erforderlichen Daten – regelmäßig Name, Anschrift, weitere Kontaktdaten sowie Grund, Höhe und Fälligkeit der Forderung. Auch beim Bestreiten einer Forderung besteht in der Regel weiterhin ein berechtigtes Interesse an der Datenverarbeitung, solange nicht von vornherein erkennbar ist, dass keine Forderung bestand, etwa bei sogenannten Abo-Fällen.

Löschung, Aufbewahrung und Auskunftsteilen

Ein Löschanspruch nach Art. 17 Abs. 1 lit. a DS-GVO scheitert regelmäßig, solange der Inkassovorgang läuft oder die Daten zur Rechtsverteidigung erforderlich sind (Art. 17 Abs. 3 lit. e DS-GVO). Auch nach Abschluss greifen häufig handels- und steuerrechtliche Aufbewahrungspflichten nach § 257 Handelsgesetzbuch (HGB) und § 147 Abgabenordnung (AO), sodass lediglich eine Verarbeitungseinschränkung nach Art. 18 DS-GVO erfolgt. Für die Übermittlung an Wirtschaftsauskunftsteilen wie die Schufa verweist die BlnBDI auf den DSK-Beschluss vom 23. März 2018 [↗](#), der fünf Fallgruppen mit Indizwirkung für eine zulässige Einmeldung definiert, wie etwa rechtskräftige Titel, unbestrittene Forderungen nach zweifacher Mahnung oder ausdrückliche Anerkenntnisse. Betroffene müssen vorab über die mögliche Einmeldung informiert worden sein.

Sonderfälle: Identitätsbetrug und E-Mail-Kommunikation

Bei glaubhaft vorgetragener Identitätsverwechslung muss das Inkassounternehmen die Forderungseinzahlung aussetzen und darf keine weiteren Mahnungen oder Auskunftseinmeldungen vornehmen, bis der Sachverhalt geklärt ist. Für die Kommunikation per E-Mail verweist die BlnBDI auf die Anforderungen der BSI-Richtlinie TR 03108-1 [↗](#) und die DSK-Orientierungshilfe zur E-Mail-Verschlüsselung [↗](#). Bei besonderen Datenkategorien nach Art. 9 DS-GVO ist eine Ende-zu-Ende-Verschlüsselung erforderlich; Betroffene können der E-Mail-Kommunikation zudem widersprechen.



Kein Löschungsanspruch nach dem Bewerbungsverfahren

Das Bundesverwaltungsgericht (BVwG) hat mit Erkenntnis vom 8. Juli 2026 (W137 2333649-1 [↗](#)) eine Beschwerde wegen Verletzung des Rechts auf Löschung nach Art. 17 DS-GVO abgewiesen und damit einen praxisrelevanten Fall zur Speicherung von Bewerbungsunterlagen entschieden.

Sachverhalt

Ein Bewerber hatte seiner Bewerbung Schriftsätze beigelegt, mit denen er die Verarbeitung seiner Daten ausschließlich auf den Bewerbungsprozess beschränken und eine sofortige Löschung nach Abschluss des Verfahrens erzwingen wollte. Nach der Absage speicherte das Unternehmen den Lebenslauf jedoch noch sieben Monate zur Abwehr möglicher Ansprüche nach dem Gleichbehandlungsgesetz und gab die Daten an eine beauftragte Rechtsanwaltskanzlei weiter. Der Bewerber sah darin eine zweckwidrige Verarbeitung und forderte die Löschung nach Art. 17 Abs. 1 lit. d DS-GVO.

Rechtliche Würdigung

Das Gericht bestätigte die Rechtsauffassung der Datenschutzbehörde: Die Verarbeitung war auf Art. 6 Abs. 1 lit. f DS-GVO (berechtigtes Interesse) gestützt zulässig, da alle drei kumulativen Voraussetzungen – berechtigtes Interesse, Erforderlichkeit und Überwiegen gegenüber den Interessen des Betroffenen – erfüllt waren. Ausschlaggebend war insbesondere, dass der Bewerber selbst bereits in seiner Bewerbung rechtliche Schritte angedroht hatte und ihm die Aufbewahrungspraxis im Kontext möglicher Gleichbehandlungsansprüche bekannt sein musste. Zudem stellte das Gericht klar, dass einseitige „Datenschutzbestimmungen“ eines Bewerbers, die gesetzliche Aufbewahrungspflichten vertraglich aushebeln sollen, keine Bindungswirkung entfalten. Eine „implizite Zustimmung“ durch bloße Verarbeitung scheidet aus. Da keine unrechtmäßige Verarbeitung vorlag, griff auch die Ausnahme des Art. 17 Abs. 3 lit. e DS-GVO (Verteidigung von Rechtsansprüchen) zugunsten des Unternehmens und der beauftragten Kanzlei.

Praxisrelevanz

Die Entscheidung bestätigt, dass Bewerbungsunterlagen nach Absage befristet zur Abwehr von Ansprüchen, etwa nach dem GIBG (Gleichbehandlungsgesetz in Österreich), aufbewahrt werden dürfen, sofern die Speicherfrist verhältnismäßig ist und im Bewerbungsprozess entsprechend informiert wurde. Einseitige Löschungsverlangen von Bewerbern, die gesetzliche Aufbewahrungspflichten unterlaufen sollen, entfalten keine rechtliche Bindungswirkung.

Auch wenn österreichische Gerichtsentscheidungen für deutsche Stellen keine Bindungswirkung entfalten, beruht die Entscheidung auf unionsweit einheitlich geltenden DS-GVO-Vorschriften und einschlägiger EuGH-Rechtsprechung. Die Wertung lässt sich daher ohne Weiteres auf die deutsche Rechtslage übertragen, insbesondere auf die Aufbewahrung von Bewerbungsunterlagen zur Abwehr von Ansprüchen nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) (§ 15 Abs. 4 AGG). Sie dient deutschen Verantwortlichen als zusätzliche Orientierung bei der Dokumentation ihrer Interessenabwägung.



Neues Arbeitspapier: Vernichtung und Entsorgung von Datenträgern

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat am 1. Mai 2026 ein Arbeitspapier zur datenschutzkonformen Vernichtung und Entsorgung von Datenträgern [↓](#) veröffentlicht. Es richtet sich zwar an bayerische öffentliche Stellen, liefert aber auch privaten Verantwortlichen praxisrelevante Orientierung zu den geltenden technischen Normen und organisatorischen Anforderungen.

Rechtsgrundlage und Normenlage

Verantwortliche sind nach Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DS-GVO verpflichtet, bei der Vernichtung von Datenträgern ein dem Risiko angemessenes Schutzniveau sicherzustellen. Bei besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO sind erhöhte Anforderungen zu beachten. Praktisch bedeutsam ist, dass die nationale Norm DIN 66399 im Jahr 2023 ersatzlos zurückgezogen wurde. An ihre Stelle tritt die inhaltlich weitgehend gleiche internationale Norm ISO/IEC 21964 (Teile 1 bis 3), die der BayLfD als maßgebliches Referenzwerk empfiehlt. Ergänzend bleibt die europäische DIN EN 15713:2024-07 zu Verfahrensregeln der sicheren Vernichtung anwendbar. Beide Regelwerke sind zwar keine Rechtsnormen, konkretisieren aber den „Stand der Technik“ im Sinne des Art. 32 DS-GVO und können bei dokumentierter Einhaltung als Compliance-Nachweis dienen.

Schutzklassen und Sicherheitsstufen

Die ISO/IEC 21964-1 definiert drei Schutzklassen und sieben Sicherheitsstufen. Für personenbezogene Daten ist mindestens Schutzklasse 2 (Sicherheitsstufe 3) erforderlich, für sensible Daten nach Art. 9 DSGVO sowie Personal-, Sozial- und Steuerdaten mindestens Schutzklasse 3 (Sicherheitsstufe 4). Teil 2 der Norm ordnet diese Stufen sechs Datenträgerkategorien zu (Papier, Film, optische, magnetische, Festplatten- und elektronische Datenträger); Teil 3 beschreibt drei mögliche Prozessvarianten – Eigenvernichtung, Vernichtung vor Ort durch Auftragsverarbeiter oder externe Vernichtung nach Abholung.

Handlungsempfehlung

Der BayLfD empfiehlt allen Verantwortlichen ein dokumentiertes Entsorgungs- und Vernichtungskonzept mit klaren Zuständigkeiten, der Festlegung der Schutzklassen, gesicherten Sammelstellen, Auftragsverarbeitungsverträgen bei externer Vergabe sowie der regelmäßigen Einholung und Prüfung von Vernichtungsnachweisen. Bei der Einbindung externer Dienstleister ist zudem die Orientierungshilfe „Auftragsverarbeitung [↓](#)“ des BayLfD zu beachten.



DATA AGENDA PODCAST



(Foto: TH Köln/Schmülgen)

Der **Experten-Talk** mit
Prof. Dr. Schwartmann

Folge #96

Legal AI zwischen
Vollkornbrot und Burger:
Warum
generative KI nicht
alles ist



Michael
Grupp



Sascha
Kremer



Eva-Maria
Pottkämper

Data Agenda Podcast Folge Folge 96: Legal AI zwischen Vollkornbrot und Burger: Warum generative KI nicht alles ist

„Es kommt darauf an.“ Das ist eine Lieblingsantwort von Juristen. Sie ist oft unbefriedigend, aber ebenso oft richtig.

Bei der Frage, ob und wofür man in der Rechtsberatung ein digitales Hilfsmittel einsetzt – etwa ein sogenanntes deterministisches Expertensystem, das sich mit Vollkornbrot vergleichen lässt, oder eine generative KI, die eher einem „AI-Burger“ entspricht –, kommt es ganz besonders auf den Zweck und den Einsatzbereich an.

Darum geht es in diesem Podcast mit Michael Grupp und Eva-Maria Pottkämper von Bryter sowie Rechtsanwalt Sascha Kremer, der Legal-Tech-Produkte in seiner Praxis einsetzt. Wir diskutieren außerdem, warum für die Justiz andere Maßstäbe beim Einsatz von KI gelten als in der Rechtsberatung.

Kleiner Spoiler: Ja – die Verfassung macht den Unterschied. Auch DSGVO und KI-Verordnung folgen dem differenzierenden Ansatz der Juristerei. Für die Frage, was erlaubt ist, gilt daher einmal mehr: „Es kommt darauf an.“

Zum Podcast bitte [hier](#)  klicken.

Weitere Folgen unter DataAgenda.de/podcast 

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30

Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Stefan Waldeisen
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299



Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen?
Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter



Datenschutz-Awareness nachhaltig stärken

Interaktive E-Learning-Kurse mit echter Moderation statt KI-Stimme

Unsere E-Learning-Kurse:

- ✓ Von GDD-Expert/innen entwickelt
- ✓ TV-Studio-Qualität mit professioneller Moderation
- ✓ vollanimierte Lerneinheiten, Study Buddy, Micro-Learning
- ✓ Barrierefrei nach BFSG
- ✓ Full-Service: Onboarding inklusive

Jetzt kostenfrei testen: www.datakontext.com/elearning

UNIVADO

 DATAKONTEXT