NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 8/2026

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Die Koalition verkauft es als „Modernisierung“: Wer genauer hinschaut, erkennt in Randnummer 14 des Koalitionsbeschlusses vor allem eines: einen weiteren Anlauf, den Datenschutz zur Wachstumsbremse umzudeuten, die es zu lösen gilt.

Besonders bemerkenswert ist die geplante Herausnahme „risikoarmer Datenverarbeitungen“ aus dem Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO). Wer entscheidet künftig, was „risikoarm“ ist? Datenschutz lässt sich nicht nach Unternehmensgröße bemessen, sondern nach Risiko für die betroffene Person. Diese Grundunterscheidung droht hier verwischt zu werden.

Ein kohärentes Datengesetzbuch klingt zunächst vernünftig. Rechtsklarheit ist ein legitimes Anliegen, das auch die Berufsgruppe der Datenschutzbeauftragten seit Jahren einfordert. Entscheidend wird jedoch sein, ob „Vereinfachung“ tatsächlich Klarheit schafft oder ob unter diesem Etikett materielle Standards abgesenkt werden. Die Formulierung „soweit dies sachgemäß ist“ lässt hier bewusst viel Interpretationsspielraum – zulasten der Betroffenenrechte, wenn die Ausgestaltung einseitig wirtschaftspolitisch geprägt wird.

Am deutlichsten wird die Schieflage bei der angekündigten Reduzierung betrieblicher Datenschutzbeauftragter (DSB) in kleinen und mittleren Unternehmen (KMU). Der DSB ist keine bürokratische Auflage, sondern die zentrale Schnittstelle, die Datenschutz im Unternehmensalltag überhaupt erst operationalisiert – als interne Frühwarnfunktion, Ansprechpartner für Betroffene und Beschäftigte sowie als Bindeglied zur Aufsicht. Wer diese Position schwächt, spart nicht an Bürokratie, sondern an Kontrolle. Gerade kleinere Unternehmen, die häufig über die geringsten internen Compliance-Ressourcen verfügen, verlieren damit eine wichtige Absicherung – mit dem Risiko, im Ernstfall unvorbereitet dazustehen.

Die Berufsgruppe der Datenschutzbeauftragten sollte sich frühzeitig in den anstehenden Gesetzgebungsprozess einbringen, bevor aus politischen Absichtserklärungen vollendete Tatsachen werden.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Photobank, Adobe Stock

Koalitionsausschuss beschließt „Vereinfachung“ des Datenschutzrechts

Im Rahmen des am 2. Juli 2026 vorgestellten Reformpakets „Ein Programm für Aufschwung und Beschäftigung“ haben CDU/CSU und SPD unter Punkt 14 weitreichende Änderungen im Bereich Datenschutz angekündigt. Unter der Überschrift „Moderner Datenschutz für mehr Wachstum“ kündigt die Koalition an, den nationalen Datenschutz zu vereinfachen und die in der DS-GVO angelegten Öffnungsklauseln und Spielräume künftig konsequenter auszuschöpfen.

Ausnahmen auf EU-Ebene geplant

Auf europäischer Ebene setzt sich die Bundesregierung dafür ein, bestimmte Konstellationen aus dem Anwendungsbereich der DS-GVO herauszunehmen. Konkret betroffen wären:

- nicht-kommerzielle Tätigkeiten, etwa im Vereinswesen,
- kleine und mittlere Unternehmen sowie
- risikoarme Datenverarbeitungen – als Beispiel wird die Führung von Kundenlisten durch Handwerksbetriebe genannt.

Datengesetzbuch und Zuständigkeitsbündelung

Zur Herstellung von mehr Rechtsklarheit und einer einheitlichen Auslegungspraxis soll ein Datengesetzbuch geschaffen werden. Dieses soll das Datenrecht als kohärentes Regelwerk harmonisieren und – soweit sachgerecht – vereinfachen, bei gleichzeitiger Wahrung des Datenschutzniveaus und Förderung der Datennutzung. Angekündigt wird zudem eine spürbare Verschlankung datenschutzrechtlicher Verfahren sowie eine Vereinfachung und Bündelung der Aufsichtsstrukturen; namentlich genannt wird eine Zuständigkeitskonzentration beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

Gesetzliche Verankerung der DSK, weniger betriebliche DSB

Die Datenschutzkonferenz (DSK) soll erstmals gesetzlich verankert werden, um die Erarbeitung gemeinsamer Standards der Aufsichtsbehörden zu institutionalisieren. Parallel dazu strebt die Koalition an, die Zahl der in kleinen und mittleren Unternehmen erforderlichen betrieblichen Datenschutzbeauftragten zu reduzieren.

Einordnung

Für die betriebliche und behördliche Datenschutzpraxis handelt es sich zunächst um eine politische Absichtserklärung; konkrete Gesetzentwürfe – etwa zum angekündigten Datengesetzbuch oder zur Neuregelung der DSB-Bestellpflicht – liegen noch nicht vor. Insbesondere die geplanten Ausnahmen vom Anwendungsbereich der DS-GVO dürften nicht kurzfristig umsetzbar sein.

50. DAFTA

12.–13. November 2026

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

Hybrid: Online & in Köln

45 RDV-FORUM

11. November 2026

Jetzt anmelden: **www.dafta.de**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: InfiniteFlow, Adobe Stock

Datenschutzverstoß beim Online-Recruiting

Informationspflicht bei Datenerhebung aus Drittquellen

Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, sondern aus Drittquellen wie öffentlich einsehbaren Profilen, greift die strengere Informationspflicht des Art. 14 DS-GVO statt der milderen Regelung des Art. 13 DS-GVO. Verantwortliche müssen der betroffenen Person dann von sich aus mitteilen, woher die Daten stammen, zu welchem Zweck sie verarbeitet werden und auf welcher Rechtsgrundlage dies geschieht – unabhängig davon, ob danach gefragt wird. Bei Nutzung der Daten zur Kontaktaufnahme muss dies gemäß Art. 14 Abs. 3 lit. b DS-GVO spätestens mit der ersten Mitteilung an die betroffene Person erfolgen. Die Vorschrift hat besonderes Gewicht, weil Betroffene bei Erhebung aus Drittquellen oft gar nichts von der Verarbeitung wissen und ihre Rechte erst wahrnehmen können, wenn sie überhaupt davon erfahren.

Öffentlich zugänglich heißt nicht frei verwendbar

Ein zweiter, häufig missverstandener Punkt betrifft die Reichweite öffentlich zugänglicher Daten: Die bloße Sichtbarkeit von Kontaktdaten auf einer Plattform begründet keine stillschweigende Zustimmung zu deren werblicher Nutzung. Die faktische Zugänglichkeit von Daten ist strikt von ihrer rechtmäßigen Verwendbarkeit zu trennen. Art. 6 Abs. 1 DS-GVO verlangt für jede Verarbeitung, auch zu Werbezwecken, eine eigenständige Rechtsgrundlage. Maßgeblich ist dabei der Kontext, in dem die Daten ursprünglich bereitgestellt wurden: Wer ein Profil zu einem klar umrissenen, nicht-kommerziellen Zweck veröffentlicht, muss nicht mit Kontaktaufnahmen zu fremden geschäftlichen Zwecken rechnen. Diese berechtigte Erwartungshaltung ist im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zu berücksichtigen.

Konkreter Fall

Genau diese beiden Aspekte adressiert ein Fall aus dem Tätigkeitsbericht 2025 der LDA Brandenburg: Eine auf IT-Fachkräfte spezialisierte Personalvermittlungsagentur hatte Name und E-Mail-Adresse eines Nutzers von dessen Profil auf einer Plattform für den Austausch zu Softwareprojekten übernommen und ihn unaufgefordert mit Stellenangeboten kontaktiert. Die Landesbeauftragte für Datenschutz und Akteneinsicht (LDA) stellte fest, dass weder eine Einwilligung noch überwiegende berechtigte Interessen des Verantwortlichen vorlagen, da der Nutzer die Plattform erkennbar privat nutzte. Zudem fehlten in den Werbe-E-Mails sämtliche nach Art. 14 DS-GVO erforderlichen Angaben zu Herkunft, Zweck und Rechtsgrundlage der Datenverarbeitung. Wegen dieser und weiterer Verstöße – unter anderem gegen die Frist zur Beantwortung eines Auskunftsersuchens nach Art. 12 Abs. 3 DS-GVO – sprach die Behörde gemäß Art. 58 Abs. 2 lit. b DS-GVO eine Verwarnung aus.

Foto: emwe studio, Adobe Stock

Ransomware-Angriff: Mangelhafte Datensicherung führt zu Totalverlust

Der aktuelle Tätigkeitsbericht 2025 der LDA dokumentiert einen abgeschlossenen Fall (S. 47), der die Grenzen rein formaler Backup-Konzepte verdeutlicht: Eine Arztpraxis meldete der Aufsichtsbehörde nach Art. 33 DS-GVO eine Datenschutzverletzung infolge eines Ransomware-Angriffs. Betroffen waren rund 75 Gigabyte medizinischer und administrativer Daten von über 8.000 Patientinnen und Patienten. Ein Datenabfluss konnte durch einen hinzugezogenen IT-Dienstleister zwar ausgeschlossen werden, die Verschlüsselung führte jedoch zu einem vollständigen und irreversiblen Datenverlust.

Ursache: Fehlerhafte Umsetzung der 3-2-1-Backup-Regel

Im Rahmen der Anhörung stellte die Landesbeauftragte für Datenschutz und Akteneinsicht fest, dass die Praxis zwar grundsätzlich nach der dem Stand der Technik entsprechenden 3-2-1-Regel sichern wollte – drei Kopien auf mindestens zwei unterschiedlichen Speichermedien, davon eine räumlich getrennt aufbewahrt – in der praktischen Umsetzung waren jedoch sämtliche als Sicherungsmedien genutzten Festplatten dauerhaft parallel am produktiven IT-System angeschlossen. Dadurch konnte die Schadsoftware auch auf die Backup-Datenträger zugreifen und diese mitverschlüsseln. Eine unverschlüsselte, isolierte Kopie zur Wiederherstellung existierte im Ergebnis nicht.

Bewertung durch die Aufsichtsbehörde

Die LDA wertete dies als Verstoß gegen Art. 32 Abs. 1 lit. b und c DS-GVO: Weder die Verfügbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten noch eine zeitnahe Wiederherstellbarkeit nach dem Vorfall waren gewährleistet. Die Behörde sprach gegenüber der Praxis eine Verwarnung gemäß Art. 58 Abs. 2 lit. b DS-GVO aus und erteilte konkrete Hinweise zur Verbesserung der Datensicherungsmaßnahmen.

Praxisrelevanz

Der Fall macht deutlich: Allein die organisatorische Festlegung eines Backup-Konzepts genügt nicht den Anforderungen des Art. 32 DS-GVO – entscheidend ist dessen tatsächliche, technisch korrekte Umsetzung. Eine physisch oder logisch getrennte, vom Produktivsystem isolierte Sicherungskopie ist essenziell, um auch bei Ransomware-Angriffen eine Wiederherstellung der Daten zu gewährleisten.

Foto: Amith, Adobe Stock

Datenschutz, Informationssicherheit und KI als integriertes Prüffeld der Internen Revision

Der DIIR-Arbeitskreis „Datenschutz & Data Governance“ hat seinen bewährten Leitfaden „Interne Revision und Datenschutz“ sowie die begleitende „Checkliste zur Prüfung der Datenschutzorganisation“ grundlegend überarbeitet und als Version 3.0 veröffentlicht. Beide Dokumente reagieren auf die erheblich veränderten regulatorischen und technologischen Rahmenbedingungen der letzten Jahre.

Erweiterter Themenrahmen: KI und Informationssicherheit neu integriert

Datenschutz ist längst kein isoliertes Rechtsthema mehr. Cyberrisiken, hybride IT-Landschaften, datengetriebene Geschäftsmodelle und der zunehmende Einsatz von KI-Systemen erfordern ein integriertes Verständnis und die Verzahnung von Datenschutz, Informationssicherheit und Data Governance. Der Leitfaden trägt dem Rechnung, indem er diese Themen erstmals systematisch zusammenführt. Datenschutz schützt dabei die Privatsphäre natürlicher Personen, während Informationssicherheit auf die Verfügbarkeit, Integrität und Vertraulichkeit aller Unternehmensdaten zielt. Beide Disziplinen überschneiden sich insbesondere bei den technischen Schutzmaßnahmen nach Art. 32 DS-GVO und den Anforderungen der ISO 27001.

Bezug zu den Global Internal Audit Standards

Auch die Global Internal Audit Standards tragen der Relevanz dieser Themen Rechnung, insbesondere in den Standards 5.2 (Schutz von Informationen) und 10.3 (Technologische Ressourcen). Standard 5.2 betont die Verantwortung der Internen Revision, Prüfungsinformationen angemessen zu schützen und damit sowohl den Anforderungen des Datenschutzes als auch des Informationsschutzes über den gesamten Prüfungsprozess hinweg Rechnung zu tragen.

Relevanz für den betrieblichen Datenschutzbeauftragten

Der Leitfaden widmet der Rolle des Datenschutzbeauftragten (DSB) ein eigenes Kapitel (mit Ausführungen zu seiner Stellung im Unternehmen, seinen Aufgaben und dem internationalen Kontext). Für DSB ist die Publikation in zweifacher Hinsicht bedeutsam: Einerseits definiert sie, wie die Interne Revision datenschutzkonform prüfen soll, was unmittelbar die Zusammenarbeit zwischen DSB und Revisionsabteilung betrifft. Andererseits liefert die begleitende Checkliste einen strukturierten Prüf- und Orientierungsrahmen, der auch für die eigene Überwachungsfunktion des DSB nach Art. 39 DS-GVO nutzbar ist. Die Einhaltung der DS-GVO-Grundsätze obliegt dem Verantwortlichen und muss anhand einer entsprechenden Dokumentation nachgewiesen werden können. Das legt nahe, dass im Unternehmen ein Datenschutzmanagementsystem etabliert sein sollte, das die Einhaltung der Schutzziele der DS-GVO gewährleistet. Beide Dokumente sind kostenlos über die DIIR-Website abrufbar.

Foto: STOATPHOTO, Adobe Stock

Social Media: LfDI aktualisiert Handlungsrahmen

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) Rheinland-Pfalz hat seinen Handlungsrahmen für die Nutzung von Social Media durch öffentliche Stellen in aktualisierter Fassung veröffentlicht. Das Dokument trägt der gewachsenen Realität Rechnung, dass Plattformen wie Facebook, TikTok oder X längst zu regulären Kommunikationskanälen von Behörden geworden sind – und schafft dafür klare datenschutzrechtliche Leitplanken.

Nutzungskonzept als Pflichtvoraussetzung

Insbesondere müssen Behörden ein Nutzungskonzept erstellen, das darlegt, weshalb der Verzicht auf Social-Media-Angebote zu einer Beeinträchtigung ihrer Aufgabenerfüllung führen würde. Der LfDI beabsichtigt, diese Konzepte stichprobenartig zu überprüfen. Daneben sind im Konzept Zweck, Art und Umfang der Datenverarbeitungen zu beschreiben sowie die redaktionelle und technische Betreuung der Präsenzen zu regeln.

Cross-Media-Gebot: Kein Zwang zur Plattformnutzung

Ein weiteres zentrales Element ist das Cross-Media-Gebot: Behörden müssen alternative Informations- und Kommunikationswege betreiben und auf diese hinweisen, sodass sich keine Bürgerin und kein Bürger zur Nutzung eines Social-Media-Angebots gezwungen sieht. Die Nutzung sozialer Plattformen darf demnach nur eine Option unter mehreren sein und nicht der einzige Zugangsweg zu behördlichen Informationen.

Gemeinsame Verantwortlichkeit und Rechtsgrundlagen

Öffentliche Stellen, die eine Fanpage betreiben, gelten seit der Entscheidung des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 (C-210/16) als Verantwortliche im Sinne der DS-GVO und müssen die damit verbundenen Informations- und Nachweispflichten erfüllen. Sie sind daher verpflichtet, nach Art. 26 DS-GVO einen Vertrag über die gemeinsame Verantwortlichkeit mit dem jeweiligen Plattformbetreiber zu schließen. Ergänzend stellte das Bundesverwaltungsgericht klar, dass Aufsichtsbehörden bei Verstößen direkt gegen den Fanpage-Betreiber vorgehen können.
Der aktualisierte Handlungsrahmen berücksichtigt auch die jüngste Rechtsprechung zur Frage des KI-Trainings durch Plattformbetreiber und bietet damit eine zeitgemäße Orientierungshilfe für behördliche Datenschutzbeauftragte, die öffentliche Stellen bei der Einrichtung oder Überprüfung ihrer Social-Media-Präsenzen beraten.

Foto: Calado, Adobe Stock

LG Freiburg stärkt Auskunftsrecht von (Wett-) Spielern

Das Landgericht (LG) Freiburg hat in einem Teilurteil den datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DS-GVO in einem Kontext bestätigt (LG Freiburg, Teilurteil vom 29. Mai 2026 – 8 O 203/24): Ein Spieler klagte gegen zwei maltesische Online-Glücksspielanbieter auf vollständige Auskunft über seine Spiel- und Zahlungshistorie – als Vorstufe zur Rückforderung verlorener Einsätze von geschätzt 100.000 Euro. Das Gericht gab dem Auskunftsbegehren weitgehend statt.

Auskunftsanspruch gilt unabhängig vom verfolgten Zweck

Die Beklagten hatten eingewandt, das Auskunftsersuchen sei rechtsmissbräuchlich, weil es nicht dem Schutz personenbezogener Daten, sondern allein der Vorbereitung einer Rückforderungsklage diene und damit ein „Spielen ohne Risiko" ermögliche. Das LG folgte dieser Argumentation nicht. Unter Verweis auf die gefestigte Rechtsprechung des EuGH (C-307/22, FT/BW) und des Bundesgerichtshofs (BGH) stellte das Gericht klar, dass der Auskunftsanspruch keiner Begründung bedarf und auch dann besteht, wenn der Antragsteller damit Ziele verfolgt, die nicht in den Erwägungsgründen der DS-GVO aufgeführt sind. Selbst ein etwaiger Rechtsmissbrauch beim nachgelagerten Leistungsanspruch lässt den vorgeschalteten datenschutzrechtlichen Auskunftsanspruch unberührt.

Spielhistorie und Zahlungsdaten als personenbezogene Daten

Das Gericht bestätigte, dass Spielhistorien und Transaktionsdaten personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO darstellen. Sie enthalten Informationen über wirtschaftliche Verhältnisse und Zahlungsmodalitäten des Nutzers und sind diesem über sein verifiziertes Nutzerkonto eindeutig zuordenbar. Der Anbieter ist als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO zur Auskunft verpflichtet.

Format der Auskunft: Maschinenlesbar auf Verlangen

Praxisrelevant ist die Aussage des Gerichts zum Dateiformat der bereitzustellenden Datenkopie. Auf Grundlage von Art. 15 Abs. 3 S. 3 DS-GVO und dem Transparenzgrundsatz aus Art. 12 Abs. 1 DS-GVO bejahte das LG einen Anspruch auf Übermittlung in einem strukturierten, gängigen und maschinenlesbaren Format – konkret CSV oder Excel. Eine PDF-Datei, die lediglich ein nicht maschinenlesbares Bild enthält, erfülle den Auskunftsanspruch nicht. Entscheidend sei, dass betroffene Personen die Daten effektiv lesen und weiterverarbeiten können. Die Wahl des Formats dürfe nicht allein dem Verantwortlichen überlassen bleiben.
Das Urteil verdeutlicht, dass Art. 15 DS-GVO auch in zivilrechtlichen Auseinandersetzungen als eigenständiges, zweckneutrales Instrument eingesetzt werden kann. Prozesse zur Bearbeitung von Auskunftsersuchen müssen nicht nur inhaltlich vollständig, sondern auch technisch so gestaltet sein, dass die Daten in einem lesbaren, maschinenlesbaren Format bereitgestellt werden können: Andernfalls besteht das Risiko, dass der Anspruch als nicht erfüllt betrachtet werden kann.

Foto: CrazyCloud, Adobe Stock

Prüfkompetenzen des DSB bezüglich des Betriebsrats

Das Landesarbeitsgericht Hamburg (LAG Hamburg, Beschluss vom 27. Januar 2026 – 4 TaBV 3/25) hat in einem Beschluss klargestellt, dass die Interne Revision einer Rundfunkanstalt die Gesamtschwerbehindertenvertretung nicht im Rahmen der regulären Revisionsjahresplanung prüfen darf. Die anlasslose, systematische Kontrolle der Amtstätigkeit, insbesondere auf Zweckmäßigkeit, verstößt gegen das Behinderungsverbot des § 179 Abs. 2 Sozialgesetzbuch (SGB) IX. Der Arbeitgeberin wurde aufgegeben, den bereits erstellten Revisionsbericht zu vernichten und künftige Regelprüfungen zu unterlassen.

Der Sachverhalt

Die Revision einer Rundfunkanstalt hatte die Gesamtschwerbehindertenvertretung im Rahmen ihrer Jahresplanung geprüft und dabei unter anderem die Beratungspraxis, die Zielformulierungen anhand von SMART-Kriterien sowie die interne Kommunikation bewertet. Das Gericht sah darin eine unzulässige inhaltliche Kontrolle der Amtstätigkeit, auch deshalb, weil der Bericht mehreren Führungskräften zugeleitet und der Gesamtschwerbehindertenvertretung eine Maßnahmenliste übermittelt wurde, die Rechtfertigungsdruck erzeugte.

Relevanz für den betrieblichen Datenschutzbeauftragten

Das Gericht befasste sich explizit mit der Frage, ob die Revision mit dem betrieblichen Datenschutzbeauftragten (DSB) vergleichbar sei und verneinte dies klar. Der DSB sei kraft Gesetzes weisungsunabhängig (Art. 38 Abs. 3 DS-GVO), zur Verschwiegenheit verpflichtet und unterliegt nach § 79a BetrVG besonderen Geheimhaltungspflichten gegenüber dem Arbeitgeber hinsichtlich des internen Meinungsbildungsprozesses des Betriebsrats. Diese institutionelle Unabhängigkeit unterscheide ihn strukturell von einer Revision, die dem Intendanten unterstellt ist.
Gleichwohl zieht das Gericht eine für Datenschutzbeauftragte bedeutsame Grenze: Auch der DSB ist nicht befugt, die Amtstätigkeit von Interessenvertretungen auf Zweckmäßigkeit hin zu kontrollieren. Seine datenschutzrechtliche Prüfkompetenz endet dort, wo die weisungsfreie Amtsführung der Vertretungsorgane beginnt. Diese Abgrenzung ist praxisrelevant, etwa bei der Prüfung von IT-Systemen oder Kommunikationskanälen, die Betriebsräte oder Schwerbehindertenvertretungen nutzen.
Für DSB ergibt sich daraus eine wichtige Orientierung: Datenschutzrechtliche Kontrolle gegenüber Arbeitnehmervertretungen ist auf die Einhaltung datenschutzrechtlicher Vorgaben beschränkt. Eine inhaltliche Beurteilung der Amtsführung ist weder zulässig noch von der gesetzlichen Aufgabenzuweisung gedeckt.

Foto: kaliel, Adobe Stock

Kein automatisches Beweisverwertungsverbot bei DS-GVO-Verstößen

Der EuGH hat in einem viel beachteten Urteil (EuGH, Urteil v. 18.06.2026, C-484/24) klargestellt, dass Gerichte personenbezogene Daten auch dann als Beweismittel verwerten dürfen, wenn eine Prozesspartei diese zuvor unter Verstoß gegen datenschutzrechtliche Vorgaben erlangt hat. Die Entscheidung erging auf Vorlage des Landesarbeitsgerichts Niedersachsen, das Zweifel daran hatte, ob es selbst beim Umgang mit möglicherweise rechtswidrig beschafften Beweisdaten gegen die DS-GVO verstoße.

Sachverhalt und Vorlagefrage

Im Ausgangsfall forderte ein Haustechnikunternehmen von einer ehemaligen Mitarbeiterin Schadensersatz. Der Arbeitgeber hatte sich über den Browserverlauf, einen Familienordner auf dem Server und eine manipulierte SIM-Karte Zugriff auf das persönliche Passwort der Frau verschafft, um deren private eBay-Verkäufe zu dokumentieren.

Kernaussagen des Urteils

Der EuGH stellt klar, dass die Verarbeitung personenbezogener Daten durch Gerichte grundsätzlich der DS-GVO unterliegt. Die Aufnahme von Beweisen in die Akten oder deren Auswertung stellt eine Verarbeitung im Sinne der Verordnung dar. Als Rechtsgrundlage kommt Art. 6 Abs. 1 lit. c DS-GVO in Betracht, da die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (nämlich der Entscheidung über Zulässigkeit und Würdigung von Beweismitteln) erforderlich ist.
Ein generelles Beweisverwertungsverbot ordne die DS-GVO hingegen nicht an. Die Zulässigkeit und Würdigung von Beweisen bleibe grundsätzlich Sache des nationalen Prozessrechts, das jedoch mit dem Unionsrecht vereinbar sein müsse. Entscheidend sei nach Auffassung des EuGH die Abwägung mit dem Recht auf ein faires Verfahren aus Art. 47 Charta der Grundrechte der Europäischen Union (GrCh). Zudem müssten Gerichte den Grundsatz der Datenminimierung beachten und seien gehalten, etwa Anonymisierungen zu prüfen, bevor Daten offengelegt werden.

Praktische Konsequenzen

Die Entscheidung trennt klar zwischen zwei rechtlich eigenständigen Ebenen: der datenschutzrechtlichen Zulässigkeit der ursprünglichen Datenerhebung und der prozessualen Frage der Verwertbarkeit. Wer Beweise rechtswidrig beschafft, riskiert weiterhin datenschutzrechtliche Sanktionen und Schadensersatzansprüche nach Art. 82 DS-GVO sowie aufsichtsbehördliche Maßnahmen. Für die Praxis empfiehlt sich daher eine sorgfältige Vorabprüfung jeder Datenerhebung sowie im Prozess eine konsequente Beschränkung auf tatsächlich erhebliche Informationen.

Foto: HNFOTO, Adobe Stock

Neuer BfDI: Bundestag wählt Prof. Dr. Moritz Hennemann

Der Deutsche Bundestag hat Prof. Dr. Moritz Hennemann zum neuen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gewählt. Er wurde von der Unionsfraktion vorgeschlagen und erhielt 391 Ja-Stimmen bei 122 Nein-Stimmen und 77 Enthaltungen. Vor seiner Ernennung muss ihn noch der Bundespräsident offiziell berufen; das Bundesdatenschutzgesetz schreibt hierfür umfassende Qualifikationen im Datenschutzrecht sowie die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst vor.

Nachfolge und Übergang

Hennemann folgt auf Louisa Specht-Riemenschneider, die im März 2026 aus gesundheitlichen Gründen ihren Rücktritt angekündigt hatte – mit dem ausdrücklichen Hinweis, das Amt dürfe angesichts seiner Bedeutung auch nicht für kurze Zeit unbesetzt bleiben. Specht-Riemenschneider wird die Amtsgeschäfte noch bis zum 30. September 2026 weiterführen, um einen geordneten Übergang zu gewährleisten. Sie begrüßte die Wahl ihres Nachfolgers ausdrücklich und würdigte ihn als klugen und engagierten Kollegen.

Profil und fachliche Ausrichtung

Hennemann ist seit 2023 Professor für Zivilrecht, Informationsrecht, Medienrecht und Internetrecht an der Universität Freiburg. Sein wissenschaftliches Werk umfasst neben zahlreichen Beiträgen zur DS-GVO auch Analysen zu Datennutzungsgesetzen wie dem Data Act und dem Data Governance Act. Er gilt als Vertreter eines wirtschafts- und innovationsorientierten Datenschutzverständnisses, das Daten verstärkt als ökonomisches Gut begreift: eine Haltung, die er mit seiner Vorgängerin unter dem Begriff „Datenrealpolitik“ teilt.
Die Reaktionen aus der Digitalwirtschaft fallen erwartungsgemäß positiv aus. Bitkom-Präsident Ralf Wintergerst erhofft sich eine zeitgemäße und innovationsfördernde Interpretation des Datenschutzes und mahnt, insbesondere mit Blick auf künstliche Intelligenz dränge die Zeit, da die USA und China ihren Vorsprung weiter ausbauten.

Kritische Stimmen

Nicht unumstritten ist Hennemanns Kandidatur in der Zivilgesellschaft. Expertise zum Thema Informationsfreiheit, das neben dem Datenschutz zum Kernaufgabenfeld des BfDI gehört, hat der Jurist bislang nicht vorzuweisen. Zudem hatte er Ende 2025 das sogenannte Digital-Omnibus-Gesetzespaket der EU begrüßt, das von Datenschutzbehörden und Zivilgesellschaft als Einschränkung der KI-Verordnung und der DS-GVO kritisiert wird. Ein transparentes Ausschreibungsverfahren für die Nachbesetzung fand nicht statt.

DATA AGENDA PODCAST

(Quelle: TH Köln/Schmülgen)

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

Folge #**95**

Ein „KI-Seepferdchen“ für alle – Befähigung und Schutz in der digitalen Welt

Sebastian Gutknecht

Jörg Schieb

Bild: © BzKJ/bundesfotz/ Uwe Völkner

Data Agenda Podcast Folge 95: Ein „KI-Seepferdchen“ für alle – Befähigung und Schutz in der digitalen Welt

Das „KI-Seepferdchen“ wurde von der unabhängigen Expertenkommission „Kinder und Jugendschutz in der digitalen Welt“ im Juni 2026 als Maßnahme vorgeschlagen. Es geht darum, Kinder schon im Grundschulalter mit den Möglichkeiten und Risiken von KI in Form von Chatbots vertraut zu machen. Die Vermittlung von KI-Kompetenz ist eine Rechtspflicht auch für Schulen und Schulträger. Die Expertenkommission legt ein Konzept vor, das von Bund und Ländern kurzfristig umgesetzt werden kann. Sebastian Gutknecht, Direktor der Bundeszentrale für Kinder- und Jugendmedienschutz (BZKJ), und Rolf Schwartmann sind Mitglieder der Kommission. Sie berichten dem Technikjournalisten Jörg Schieb darüber, wie das „KI-Seepferdchen“ ins Werk gesetzt werden kann und worauf es jetzt ankommt.
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