NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
9/2025

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Manche werden nicht müde zu verkünden, welche große Fußfessel und welches Hindernis der Datenschutz (und mit ihm oftmals auch der Datenschutzbeauftragte) für die Innovation, die Digitalisierung und das Scheitern von Projekten darstellen:

- Datenschutz als „Aufwand" für Unternehmen
- Datenschutz als Innovationsbremse
- Datenschutz als Herausforderung für Digitalisierung

Da ist es Balsam für die Seele eines Datenschützers, auch mal zu lesen, welche positiven Effekte Datenschutzbeauftragte und gelebter Datenschutz auf Unternehmen und Unternehmenszahlen haben können. Jüngst veröffentlichte die CNIL eine Untersuchung zu den wirtschaftlichen Vorteilen eines Datenschutzbeauftragten in Unternehmen.

- **Förderung bei Ausschreibungen**
- Ein Datenschutzbeauftragter (DSB) wird als Zeichen für die Seriosität im Hinblick auf die Datenschutz-Grundverordnung (DS-GVO) gesehen. Befragte Unternehmen berichten von signifikant größeren Chancen, bei der Vergabe berücksichtigt zu werden, insbesondere, wenn der DSB aktiv konsultiert wird.
- **Reduktion von Sanktionen**
- DSB stärken die Compliance, schulen Mitarbeitende und wirken als zentrale Ansprechpersonen – dadurch verringern sich Bußgeldrisiken.
- **Schutz vor Datenverlusten**
- Durch Sensibilisierung sank die Phishing-Klickrate von 21 Prozent auf 5 Prozent, was potenzielle Schäden deutlich reduzierte.
- **Effizientere Datenverwaltung**
- Die Umsetzung DS-GVO-konformer Datenstrategien (Minimierung, Löschung, Speicherbegrenzung) senkte die Infrastrukturkosten – z. B. **400.000 Euro Ersparnis** bei Serverausgaben
- In **58 Prozent der Unternehmen**, in denen Compliance als strategischer Hebel verstanden wird, zeigen sich die genannten Vorteile besonders deutlich.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: NongAsimo, Adobe Stock

KI in der anwaltlichen Praxis: Chancen und rechtliche Rahmenbedingungen

Der Deutsche Anwaltverein (DAV) sieht im Einsatz von künstlicher Intelligenz (KI), insbesondere generativer KI (GKI), erhebliche Effizienzpotenziale für Kanzleien. In der Stellungnahme 32/2025 werden die wesentlichen berufsrechtlichen, datenschutzrechtlichen und urheberrechtlichen Aspekte beleuchtet, mit besonderem Fokus auf die Einhaltung der anwaltlichen Verschwiegenheitspflicht.

Berufsrecht: Gewissenhaftigkeit und Geheimnisschutz

Der DAV betont die Pflicht zur sorgfältigen Prüfung KI-generierter Inhalte (§ 43 Bundesrechtsanwaltsordnung (BRAO)). Eine ungeprüfte Weitergabe ist nur zulässig, wenn der Mandant dies ausdrücklich verlangt. Der Einsatz externer KI- und Cloud-Dienstleister ist nach § 43e BRAO grundsätzlich zulässig, sofern die Einbindung erforderlich ist und die Dienstleister vertraglich zur Verschwiegenheit verpflichtet werden. Dabei genügt es nicht, auf Standardlösungen zurückzugreifen. Anbieter müssen bewusst in die anwaltliche Tätigkeit eingebunden werden und es müssen technische Zugriffsbeschränkungen berücksichtigt werden. Eine pauschale Pflicht zur Verschlüsselung besteht allerdings nicht.

Datenschutz: Rechtskonforme Einbindung externer Systeme

Auch datenschutzrechtlich sei der KI-Einsatz gut beherrschbar. Die Datenverarbeitung kann regelmäßig auf Art. 6 Abs. 1 lit. b oder f DS-GVO gestützt werden, bei besonderen Kategorien personenbezogener Daten auf Art. 9 Abs. 2 lit. b oder f DS-GVO. KI-Anbieter gelten typischerweise als Auftragsverarbeiter (Art. 28 DS-GVO). Anwältinnen und Anwälte müssen dabei die Datenschutzprinzipien Datenminimierung, Zweckbindung, Dokumentation und Transparenz beachten. Drittstaatentransfers sind unter Beachtung der Art. 44 ff. DS-GVO sorgfältig zu prüfen, insbesondere bei US-Anbietern. Der DAV empfiehlt, dynamische Entwicklungen zu beobachten und möglichst auf Anbieter mit EU-Infrastruktur zurückzugreifen.
Die neue EU-Verordnung über Künstliche Intelligenz (KI-VO bzw. AI Act) ist seit 2025 schrittweise anwendbar. Der DAV kommt zu dem Ergebnis, dass typische Kanzlei-Anwendungen, etwa für Textgenerierung oder Dokumentenanalyse, meist als risikoarme Systeme einzustufen sind. Die Kennzeichnungspflichten gemäß Art. 50 KI-VO (z. B. bei Chatbots) und die Transparenzanforderungen für veröffentlichte KI-Inhalte (ab August 2026) sind gleichwohl zu beachten.

Fazit

Der DAV sieht keine grundsätzlichen rechtlichen Hürden für den KI-Einsatz in Kanzleien, wohl aber einen erheblichen Regelungs- und Prüfungsbedarf. Entscheidend sei ein informierter, kontrollierter Umgang mit KI-Anwendungen unter Beachtung berufs- und datenschutzrechtlicher Standards. Bei sorgfältiger Implementierung könne KI als zukunftsweisendes Instrument die anwaltliche Arbeit sinnvoll ergänzen.

Foto: woravut, Adobe Stock

Datenschutzrechtliche Anforderungen bei der Entgeltfortzahlung

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat sich in einem aktuellen Beitrag mit der datenschutzrechtlichen Zulässigkeit der Verarbeitung von Gesundheitsdaten im Zusammenhang mit sogenannten Fortsetzungserkrankungen beefasst. Arbeitgeber dürfen demnach Diagnosedaten oder vergleichbare Informationen nur verarbeiten, wenn diese zur Prüfung des Anspruchs auf Entgeltfortzahlung tatsächlich erforderlich sind.

Verarbeitung nur bei konkretem Anlass und unter engen Voraussetzungen

Hintergrund ist die gesetzliche Regelung, nach der Arbeitnehmerinnen und Arbeitnehmer im Krankheitsfall für maximal sechs Wochen eine Lohnfortzahlung erhalten. Wird dieselbe oder eine damit zusammenhängende Erkrankung innerhalb von sechs Monaten nach Wiederaufnahme der Arbeit erneut festgestellt, liegt eine Fortsetzungserkrankung vor. Dies kann dazu führen, dass sich die Zeiten addieren und der Anspruch auf Entgeltfortzahlung entfällt – es bestünde dann ein Anspruch auf Krankengeld.
Zur Prüfung, ob eine Fortsetzungserkrankung vorliegt, ist die Verarbeitung von Gesundheitsdaten grundsätzlich zulässig. Rechtsgrundlagen hierfür sind § 26 Abs. 3 Bundesdatenschutzgesetz (BDSG) i. V. m. Art. 9 Abs. 2 lit. b DS-GVO sowie ergänzend Art. 6 Abs. 1 lit. b DS-GVO, sofern die Prüfung arbeitsvertragliche Pflichten berührt. Entscheidend ist aber, dass konkrete Anhaltspunkte für eine Fortsetzungserkrankung vorliegen müssen. Ein bloßer Verdacht reicht nicht aus. Arbeitgeber haben zuvor mildere Mittel zu prüfen, etwa eine Abklärung über die Krankenkasse oder eine (datensparsame) Einschätzung durch den Betriebsarzt.

Technische und organisatorische Schutzmaßnahmen

Die pauschale Erhebung von Diagnosen oder die Speicherung chronischer Erkrankungen auf Vorrat ist unzulässig. Auch eine Einwilligung der betroffenen Person reicht in der Regel nicht aus, da sie im Arbeitsverhältnis regelmäßig nicht als freiwillig gilt.
Besondere Anforderungen gelten zudem für die technische und organisatorische Verarbeitung: Gesundheitsdaten sind strikt von der übrigen Personalakte getrennt zu verwahren. Sie dürfen nur so lange gespeichert werden, wie dies zur Prüfung des Entgeltfortzahlungsanspruchs notwendig ist. Eine Weitergabe an Dritte – etwa im Rahmen einer Rechtsverteidigung – ist nur bei zwingender Erforderlichkeit und unter Beachtung des Grundsatzes der Datenminimierung zulässig.
Die Entscheidung des Bundesarbeitsgerichts vom 18. Januar 2023 (Az. 5 AZR 93/22) bestätigt, dass Arbeitgeber vor der Verarbeitung sensibler Gesundheitsdaten zunächst alternative Möglichkeiten zur Sachverhaltsaufklärung ausschöpfen müssen.

OLG Frankfurt: Kein Datenzwang mehr beim Sparpreis-Ticket

Seit Oktober 2023 durfte die Deutsche Bahn „Spar"- und „Super-Sparpreis"-Tickets ausschließlich digital vertreiben. Beim Schalterkauf mussten Reisende zwingend entweder eine EMail-Adresse oder eine Handynummer angeben, um das Ticket elektronisch zu erhalten.

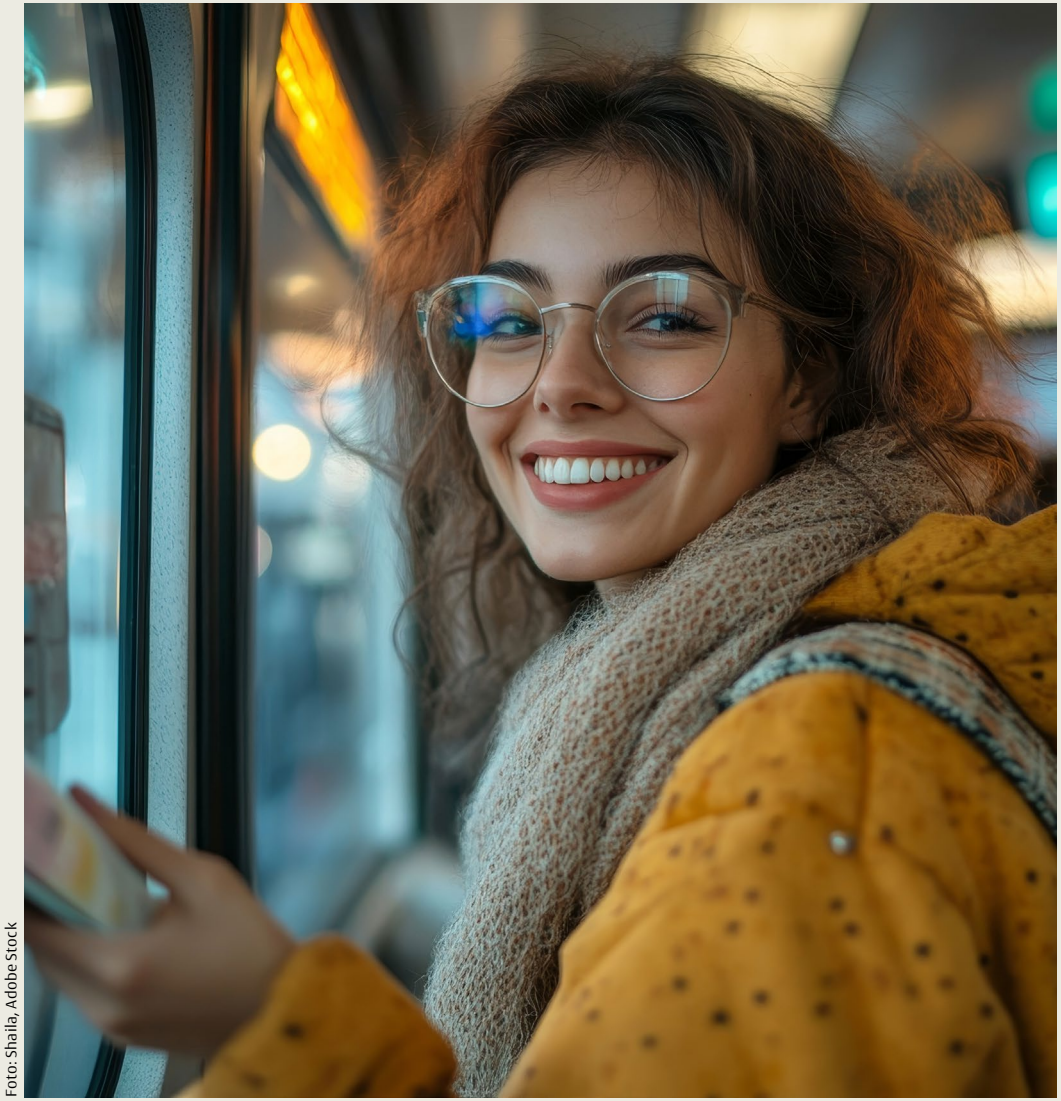

Foto: Shaila, Adobe Stock

Klage und rechtliche Bewertung

Der Verbraucherzentrale Bundesverband (VZBV) reichte Klage ein. Der 6. Zivilsenat des Oberlandesgerichts (Az. 6 UKl 14/24) befand, dass diese Pflichtangabe gegen Art. 6 und 7 DS-GVO verstößt: Die Einwilligung könne nicht als „freiwillig" gelten, da der digital vorgeschriebene Weg keine echte Wahl lasse – insbesondere bei einem marktbeherrschenden Unternehmen wie der Bahn. Zudem sei die Erhebung der Daten für den reinen Ticketkauf rechtlich irrelevant und diene vielmehr operativen und marketingbezogenen Zwecken.

Entscheidung und Konsequenzen

Das Oberlandesgericht (OLG) untersagte der Bahn, digitale Tickets an personenbezogene Daten zu knüpfen. Nutzer können Sparpreise nun wieder analog, also ohne Datenpreisgabe, am Schalter erwerben. Das Urteil ist unanfechtbar. Laut Unternehmenssprecherin wurde der analoge Ticketkauf bereits im Dezember 2024 angepasst. Zwar wird weiterhin empfohlen, eine E-Mail-Adresse anzugeben (z. B. zur Zustellung von Fahrplanänderungen), doch dies ist nicht mehr zwingend erforderlich.

Wesentliche Erkenntnisse für die Datenschutzpraxis

- **DS-GVO-Konformität:** Einwilligungen müssen freiwillig erfolgen – ein Zwangsmechanismus durch digitale Ticketvorgaben ist unzulässig.
- **Datensparsamkeit und Zweckbindung:** E-Mail-Adresse und Mobilfunknummer sind nicht erforderlich für die Vertragserfüllung (Beförderung). Eine Verarbeitung nur zu Marketingzwecken ist DS-GVO-rechtswidrig.
- **Marktstellung:** Bei marktbeherrschenden Anbietern können selbst mittelbare Zwangssituationen die Freiwilligkeit einer Einwilligung ausschließen.

12.–14.11.2025
hybrid: online
& in Köln

49. DAFTA

44. RDV-FORUM

Vom Datenschutzrecht zum Datennutzungsrecht – so bewährt sich der betriebliche Datenschutz

Jetzt anmelden:
www.datakontext.com/dafta-2025

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: PRASANNAPIX, Adobe Stock

KI-Richtlinie für Studium und Lehre

Die Universität Regensburg hat am 7. Mai 2025 neue Richtlinien für den Einsatz von Künstlicher Intelligenz (KI) in juristischen Haus-, Seminar- und Studienarbeiten ⭳ veröffentlicht. Sie definieren einen transparenten und verantwortungsvollen Umgang mit KI-Hilfsmitteln, wie sie etwa von ChatGPT oder vergleichbaren Tools generiert werden. Unterschiedliche Kategorien – z. B. normative Prüfungen, inhaltliche Unterstützung oder Visualisierung durch generative KI – sind klar gekennzeichnet. Die Verwendung solcher KI-bezogener Inhalte muss in einem Anhang detailliert offengelegt werden, während KI-basierte Rechtschreib- oder Grammatikprüfungen weiterhin als triviale Werkzeuge gelten.

Die Richtlinie stellt klar: Studierende tragen die volle Verantwortung für den Inhalt ihrer Arbeiten, einschließlich KI-gestützter Passagen. Halluzinierte oder nicht überprüfte Textpassagen gelten als eigene Leistung – mit potenziellen Abzügen oder Sanktionen. Zudem wird darauf hingewiesen, urheberrechtlich geschützte KI-Ausgaben sowie verwendete Prompts angemessen zu behandeln.

Klare Kennzeichnungspflicht und Eigenverantwortung

Die Regensburger Richtlinien erlauben den Einsatz von KI als geteiltes Hilfsmittel – jedoch stets mit wissenschaftlich korrekter Kennzeichnung. KI-basierte Inhalte müssen in einem gesonderten Anhang genannt werden, inklusive Angaben zur Tool-Art (z. B. Paraphrasierung, Struktur, Visualisierung). Unmarkierte KI-Inhalte können zur Abwertung führen. Rechtschreibkorrekturen oder Datenbank-Recherchen bleiben unbeanstandet und müssen nicht explizit ausgewiesen werden.

Haftung und inhaltliche Verantwortung der Studierenden

Die Richtlinien stellen klar: Die Verantwortung für sämtliche Arbeitsergebnisse liegt uneingeschränkt beim Studierenden. Halluzinationen von KI, beispielsweise erfundene Gerichtsurteile, werden wie bewusst falsch eingebrachte Inhalte bewertet. Auch urheberrechtliche Folgen durch KI-Inhalte oder Aufforderungs-Prompts liegen vollständig in der Verantwortung der Verfasser:innen.

Diese Richtlinien sorgen für klare Richtsätze im juristischen Studium der Universität Regensburg: KI darf eingesetzt werden, jedoch nur unter strenger Kennzeichnung und unter voller persönlicher Verantwortung. So fördert die Universität einen reflektierten, ethisch wie rechtlich abgesicherten Umgang mit generativer KI in Wissenschaft und Lehre.

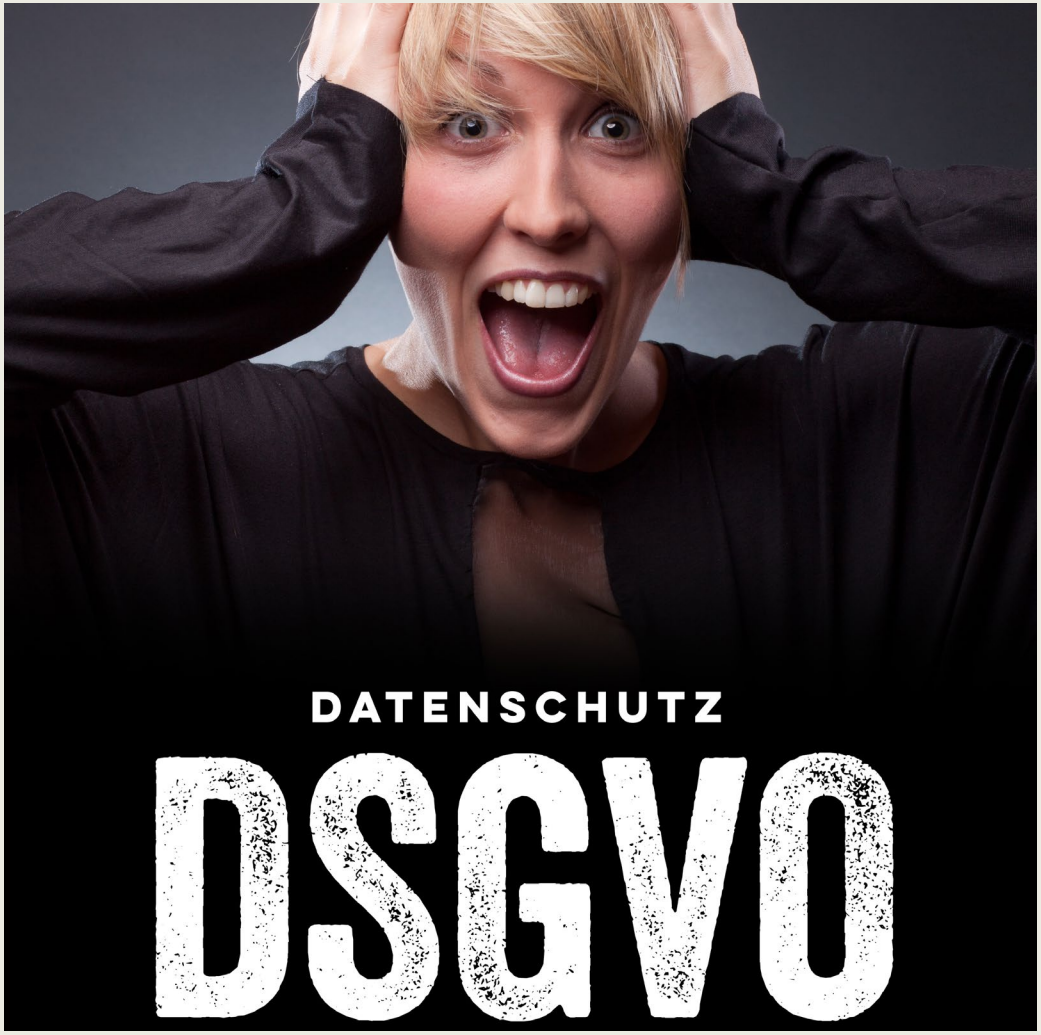

Foto: Bernulius, Adobe Stock

Datenschutz für Kleinstunternehmen und Soloselbstständige

Mit einer aktuellen Checkliste ⭳ unterstützt das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) Kleinstunternehmen und Soloselbstständige im stationären und digitalen Handel bei der datenschutzkonformen Umsetzung der DS-GVO. Die Orientierungshilfe richtet sich an Betriebe mit bis zu neun Beschäftigten und bietet eine praxisnahe Grundlage, um häufige Verarbeitungssituationen rechtssicher zu gestalten.

Die Checkliste gliedert sich in 15 thematische Bereiche und deckt zentrale Pflichten wie die Dokumentation von Verarbeitungstätigkeiten, die Wahl geeigneter Rechtsgrundlagen sowie den Umgang mit Betroffenenrechten ab. Auch typische Herausforderungen – etwa bei Videoüberwachung, Kundenkommunikation, Webshops oder der Nutzung digitaler Tools – werden adressiert. Die Anforderungen an Informationspflichten, Auftragsverarbeitungsverträge und Maßnahmen bei Datenschutzvorfällen sind klar umrissen.

Die Checkliste legt besonderes Augenmerk auf datenschutzrelevante Aspekte digitaler Anwendungen. So sind beim Einsatz von Hosting-Diensten, Cloud-Software oder KI-gestützten Tools zwingend Auftragsverarbeitungsverträge abzuschließen. Übermittlungen in Drittstaaten, insbesondere in die USA, bedürfen geeigneter Garantien – etwa durch das EU-US Data Privacy Framework. Für Webtracking und Onlinemarketing gilt: Der Einsatz entsprechender Technologien setzt eine wirksame Einwilligung voraus. Cookie-Banner müssen transparent, ablehnbar und widerrufbar gestaltet sein.

Auch wenn in den meisten Fällen keine Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht, betont das BayLDA die Notwendigkeit interner Abläufe – insbesondere für Auskunftsersuchen oder die Meldung von Sicherheitsvorfällen. Die Checkliste enthält zahlreiche Formulierungshilfen und praktische Hinweise, etwa zur Ausgestaltung von Datenschutzerklärungen und Informationspflichten im Geschäft oder im Web. Damit bietet sie eine kompakte, umsetzungsorientierte Unterstützung für kleine Handelsbetriebe mit hohen datenschutzrechtlichen Ansprüchen.

Foto: patpitchaya, Adobe Stock

Whitepaper zu Bias in KI-Systemen

Unter „Bias“ versteht man im Kontext künstlicher Intelligenz jede Form systematischer Verzerrung, die zu ungleichen oder unfairen Behandlungsergebnissen führt. Solche Verzerrungen können entstehen, wenn Trainingsdaten bestimmte Gruppen unterrepräsentieren, historische Vorurteile enthalten oder wenn Modelle aufgrund ihrer Architektur und Parametrierung bestimmte Muster bevorzugen. Die Folgen sind weitreichend: Neben der Beeinträchtigung von Fairness und Transparenz können Bias auch zu rechtlichen Problemen, Diskriminierung und Vertrauensverlust führen. Zudem bergen sie sicherheitsrelevante Risiken, etwa wenn fehlerhafte oder manipulative Ergebnisse Angriffsvektoren für Cyberattacken eröffnen.

Vor diesem Hintergrund hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 24. Juli 2025 ein Whitepaper veröffentlicht. Es bietet Entwickelnden, Anbietenden und Betreibenden von KI-Systemen eine praxisorientierte Einführung in die Ursachen, Erkennungsmethoden und Gegenmaßnahmen von Bias. Bias kann in allen Phasen des KI-Lebenszyklus entstehen – von der Datenerhebung über die Modellentwicklung bis hin zum operativen Einsatz. Häufige Ausprägungen sind historischer Bias, Repräsentations- und Evaluationsbias, Populationsbias sowie Automationsbias.

Methoden und Handlungsempfehlungen

In dem Whitepaper werden technische Verfahren zur Erkennung von Verzerrungen beschrieben, etwa qualitative und quantitative Datenanalysen, der Einsatz von Fairness-Metriken wie demografische Parität oder prädiktive Gleichheit sowie statistische Varianzanalysen. Zur Reduzierung werden Maßnahmen auf drei Ebenen empfohlen: In der **Präprozessierung** können Daten durch Sampling oder Reweighting angepasst werden, in der **Inprozessierung** kommen Techniken wie Regularisierung, Constraints oder Adversariales Learning zum Einsatz. In der **Postprozessierung** können Ergebnisse nachträglich korrigiert werden, wenn die Trainingsdaten oder Modelle nicht mehr verändert werden können.

Das BSI unterstreicht, dass der Umgang mit Bias nicht nur eine ethische Verantwortung bedeutet, sondern auch essenziell für die Cybersicherheit ist. Manipulativ ausgenutzte Verzerrungen können zu gravierenden Sicherheitsvorfällen führen. Daher empfiehlt die Behörde, ein kontinuierliches Bias-Monitoring mit klar definierten Verantwortlichkeiten, regelmäßigen Audits und dokumentierten Bias-Logbüchern zu etablieren. Interdisziplinäre Teams sollten technische, organisatorische und rechtliche Perspektiven einbeziehen, um sowohl die Sicherheit als auch die Rechtmäßigkeit von KI-Anwendungen nachhaltig sicherzustellen.

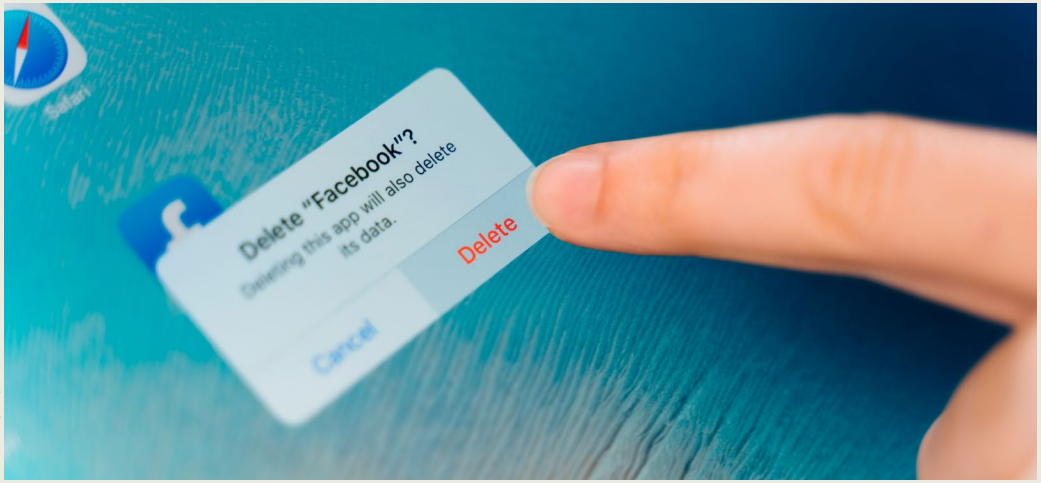

Foto: troyanphoto, Adobe Stock

Facebook-Fanpage der Bundesregierung zulässig

Das Verwaltungsgericht Köln hat im Verfahren des Bundespresseamts (BPA) gegen den Bescheid der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aus dem Februar 2023 entschieden und diesem in Teilen stattgegeben. Die BfDI hatte den Betrieb der Facebook-Fanpage der Bundesregierung untersagt – insbesondere wegen datenschutzrechtlicher Mängel bei Einwilligungen für Cookies. Die Klage von Meta Platforms Ireland Ltd. wies das Gericht in drei von vier Punkten als unzulässig ab.

Das Verfahren basiert auf der EuGH-Rechtsprechung („Wirtschaftsakademie“ 2018, C-210/16): Fanpage-Betreiber sind als Mit-Verantwortliche nach Art. 26 DS-GVO für Datenverarbeitungen (z. B. durch Insights-Funktionen) verantwortlich. Diese gemeinschaftliche Verantwortlichkeit ist durch weitere Urteile des Europäischen Gerichtshofs (EuGH) („Zeugen Jehovas“, „Fashion ID“) bekräftigt.
Die BfDI wertet das Urteil als „Schritt weiter“, auch wenn es nicht vollumfänglich den Erwartungen entspricht. Die BfDI kündigt an, die Urteilsbegründung eingehend zu prüfen. Es soll entschieden werden, ob Rechtsmittel beim Oberverwaltungsgericht Münster eingelegt werden. Parallel dazu verfolgen viele Behörden das Verfahren intensiv, um ihre eigene Social-Media-Strategie datenschutzkonform zu gestalten. Ähnliche Verfahren in Deutschland (z. B. Sachsen) und anderen EU-Staaten sind noch anhängig.

Foto: erika8213, Adobe Stock

Geschlechtliche Vielfalt als Datenschutzthema

Im Rahmen der Pride Week 2025 weist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit auf datenschutzrechtliche Aspekte im Umgang mit geschlechtlicher Vielfalt hin. Das am 1. November 2024 in Kraft getretene Selbstbestimmungsgesetz ermöglicht es Personen, ihren Geschlechtseintrag im Personenstandsregister selbst zu bestimmen oder keinen Eintrag vorzunehmen. Diese rechtliche Neuerung hat Auswirkungen auf die Verarbeitung personenbezogener Daten, insbesondere in Bezug auf die Datenrichtigkeit gemäß Art. 5 Abs. 1 lit. d) DS-GVO.

Datenrichtigkeit und Berichtigungsanspruch

Datenverarbeitende Stellen wie Behörden, Unternehmen und Dienstleister sind verpflichtet, personenbezogene Daten korrekt zu erheben und zu speichern. Wenn sich die Geschlechtsidentität einer Person ändert oder sie keinen Geschlechtseintrag wünscht, haben Betroffene gemäß Art. 16 DSGVO einen Anspruch auf Berichtigung ihrer Daten. Dabei ist die Eintragung im Personenstandsregister maßgeblich, wie § 10 des Gesetzes über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG) festlegt.

Die Abfrage des Geschlechts darf nur erfolgen, wenn sie für die Vertragserfüllung „objektiv unerlässlich“ ist. Dies bestätigte der Europäische Gerichtshof am 9. Januar 2025 im Zusammenhang mit dem Verkauf von Bahnfahrkarten. Demnach ist die Angabe des Geschlechts für die Beförderungsleistung nicht erforderlich.

Praktische Umsetzung

Datenverarbeitende Stellen sollten ihre Systeme so anpassen, dass sie neben den Kategorien „weiblich“ und „männlich“ auch „divers“ oder „kein Geschlecht“ erfassen können. Anreden in Korrespondenz sollten geschlechtsneutral gestaltet werden. Diese Maßnahmen tragen dazu bei, die Rechte von trans*, inter* und nicht-binären Personen zu wahren und Diskriminierung zu vermeiden.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit betont, dass die Achtung geschlechtlicher Vielfalt im Einklang mit den datenschutzrechtlichen Anforderungen steht und zur Förderung der Gleichberechtigung beiträgt.

DATA AGENDA PODCAST

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

(Quelle: TH Köln/Schmülgen)

Folge #**74:**	Einblicke und Ausblicke: So arbeitet das Bundesministerium für Digitales und Staatsmodernisierung
Folge #**73:**	Die Stimme des Urheberrechts – Grenzen der KI aus Sicht der Kreativbranche
Folge #**72:**	KI in der Anwaltskanzlei – Werkzeug oder Kollege?
Folge #**71:**	Meta und KI – Was ist zu tun?
Folge #**70:**	„Mini DS-GVO" im Omnibus – bekommt das EU-Datenschutzrecht ein Facelifting?
Folge #**69:**	Faire Bedingungen für Digitale Märkte: Die Rolle des Bundeskartellamts und seine Bezugspunkte zum Datenschutz
Folge #**68:**	Begleitmusik des Datenrechts – Die Entwürfe zur Durchführung von Data Act und KI-VO
Folge #**67:**	Zukunftsperspektiven für KI-Haftung und ePrivacy
Folge #**66:**	Update KI-VO: Leitlinien der Kommission zu verbotenen Praktiken
Folge #**65:**	Justizbehörde gegen den Hass im Netz – Wie die ZAC NRW Onlinekriminalität bekämpft
Folge #**64:**	Datenrecht 2025: Koordinierter Zukunftsoptimismus
Folge #**63:**	Datenschutz in der Onlinewirtschaft – Datennutzungsrecht und Einwilligungsverwaltung

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:
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