NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 7/2026

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Was haben ein Juraprofessor, ein sanktionierter Anwalt, ein manipulierbares Rechtsdokument und eine Chrome-Erweiterung aus Kaiserslautern gemeinsam? Spoiler: Es geht um künstliche Intelligenz (KI).

Eine Studie der Stanford Law School sorgte Ende Mai für Gesprächsstoff: In Blindtests bevorzugten 16 Rechtsprofessoren die maschinell bzw. mit KI erzeugten Antworten gegenüber denen ihrer Kolleginnen und Kollegen und das ausgerechnet in Bereichen, in denen Abwägung und Urteilsvermögen gefragt sind, nicht bloß Faktenabruf. Die Pointe: Die Prüfer merkten es nicht einmal.

Gleichzeitig mehren sich die Gegenbeispiele. In den USA wurden zwei Anwälten Geldstrafen auferlegt, weil ihre Klageerwiderung mehr als zwei Dutzend gefälschte oder falsch dargestellte Zitate enthielt. Eine öffentlich zugängliche Datenbank dokumentiert weltweit bis April 2026 mehr als 1.300 solcher Fälle. Tendenz täglich steigend. Die KI kann also offenbar beides: überzeugend sein und komplett falsch liegen. Manchmal sogar gleichzeitig.

Und dann ist da noch die eher unheimliche Variante. Forschende zeigen mit dem sogenannten „Noroboto"-Angriff, wie ein manipulierter eingebetteter Font in einem Rechtsdokument dazu führen kann, dass ein menschlicher Leser „Maryland" sieht, während ein KI-System den Text als „Delaware" verarbeitet – mit potenziell erheblichen juristischen Konsequenzen.

Auf der anderen Seite des Spektrums: konstruktive Antworten. Das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) hat mit „Privacy Guardrail" eine Open-Source-Erweiterung für Chrome veröffentlicht, die personenbezogene und andere sensible Inhalte vollständig lokal im Browser erkennt, anonymisiert und nach der KI-Antwort wiederherstellt.

Der rote Faden dieser Monate lautet schlicht: KI ist im Rechtsbereich angekommen und zwar mit allem, was dazugehört: beeindruckende Fähigkeiten, blinde Flecken, neue Angriffsvektoren und der wachsende Bedarf an technischen wie rechtlichen Leitplanken.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: AiDesign, Adobe Stock

KI haftet nicht? – Zurechnung von KI-Falschaussagen

Ob Chatbot, KI-Übersicht oder halluzinierter Suchalgorithmus – drei Gerichtsentscheidungen in Deutschland ziehen eine klare Linie: Wer KI-Systeme im geschäftlichen Umfeld einsetzt, trägt die volle rechtliche Verantwortung für deren Ausgaben.

Mit Urteil vom 12. Mai 2026 hat der 4. Zivilsenat des Oberlandesgerichts (OLG) Hamm entschieden, dass ein Unternehmen für irreführende Qualifikationsangaben seines KI-Chatbots wettbewerbsrechtlich haftet. Im konkreten Fall hatte der Chatbot einer ästhetisch-medizinischen Klinik Facharztbezeichnungen ausgegeben, die die betreffenden Ärzte tatsächlich nicht führen dürfen. Die Verbraucherzentrale NRW obsiegte mit ihrer Unterlassungsklage. Der Senat stellte fest, dass KI-Chatbots rechtlich keine „Dritten" im Sinne des UWG sind, sondern als integraler Bestandteil der unternehmerischen Kommunikation dem Betreiber vollständig zugerechnet werden – unabhängig davon, ob der Fehler auf eine technische Fehlfunktion oder eine KI-Halluzination zurückzuführen ist. Wegen der grundsätzlichen Bedeutung der Zurechnungsfrage hat der Senat die Revision zum BGH zugelassen (Az. 4 UKl 3/25).

Parallele Linie bei Google und Grok

Die Entscheidung reiht sich in eine sich verdichtende Rechtsprechungslinie ein. Das Landgericht München I verurteilte Google mit Urteil vom 28. Mai 2026 zur Unterlassung falscher Aussagen in seiner Funktion „Übersicht mit KI" (AI Overview). Das Gericht stellte fest, dass durch diese KI-Funktion nicht nur Suchergebnisse Dritter wiedergegeben, sondern diese in eigenen Worten und nach eigener Gliederung zusammengefasst und ausgewertet präsentiert werden. Damit erzeuge die KI eigenständige, über einzelne Suchergebnisse hinausgehende Aussagen, die Google als deren Anbieter unmittelbar zuzurechnen seien. Eine pauschale Berufung auf die Privilegierung als Suchmaschinenanbieter ließ das Gericht nicht gelten (Az. 26 O 869/26). Bereits im Herbst 2025 hatte das Landgericht Hamburg in einem Verfahren gegen den Chatbot Grok von X eine vergleichbare Grundsatzentscheidung getroffen: Der Betreiber eines Chatbots haftet für unwahre oder ehrverletzende Tatsachenbehauptungen der KI, wenn diese Falschinformationen über einen Account in einem sozialen Netzwerk dauerhaft und öffentlich abrufbar sind. Die Tatsache, dass der Inhalt maschinell generiert wurde, ändere nichts an der rechtlichen Unzulässigkeit. Ein allgemeiner Disclaimer wie „KI kann Fehler machen" genüge nicht als Haftungsausschluss (Az. 324 O 461/25).

Einordnung für die Praxis

Die drei Entscheidungen betreffen zwar unterschiedliche KI-Systeme und Rechtsgebiete, haben aber denselben Grundsatz: KI-Ausgaben werden dem Betreiber wie eigene Äußerungen zugerechnet. Für Datenschutzbeauftragte und Compliance-Verantwortliche bedeutet dies, dass der Einsatz KI-gestützter Kommunikationssysteme nicht nur datenschutzrechtliche Risiken nach Art. 22 und Art. 5 Datenschutz-Grundverordnung (DS-GVO) erzeugt, sondern auch wettbewerbs- und persönlichkeitsrechtliche Haftungsrisiken, die im Rahmen von Risikoanalysen und KI-Governance-Konzepten zwingend zu berücksichtigen sind. Eine regelmäßige inhaltliche Überprüfung der KI-Ausgaben sowie klare interne Verantwortlichkeiten sind angesichts dieser Rechtsprechung keine Kür, sondern gebotene Sorgfaltspflicht.

Foto: magele-picture, Adobe Stock

Tätigkeitsbericht als Steuerungsinstrument für Datenschutzbeauftragte

Die französische Datenschutzbehörde CNIL hat jüngst eine Empfehlung samt Mustervorlage für den Tätigkeitsbericht des Datenschutzbeauftragten veröffentlicht. Die Empfehlungen decken sich weitgehend mit der deutschen Praxis – mit einer bemerkenswerten Ausnahme.

Obwohl weder die Datenschutz-Grundverordnung (DS-GVO) noch das Bundesdatenschutzgesetz (BDSG) einen Tätigkeitsbericht für betriebliche Datenschutzbeauftragte vorschreiben, empfiehlt die Commission nationale de l'informatique et des libertés (CNIL) diesen als zentrale Best Practice. Das entspricht auch der gelebten Praxis im deutschen Raum: Die in Art. 38 Abs. 3 DS-GVO verankerte Pflicht, unmittelbar an die höchste Managementebene zu berichten, bildet die natürliche Grundlage für einen strukturierten Jahresbericht. Auch das Kurzpapier Nr. 12 der Datenschutzkonferenz (DSK) unterstreicht, dass der Datenschutzbeauftragte (DSB) den Stand des Datenschutzniveaus analysiert und der Geschäftsleitung Verbesserungsvorschläge und Defizithinweise kommuniziert.

Inhaltlich empfiehlt die CNIL, den Bericht als strategisches Steuerungsinstrument zu nutzen: Er soll Verarbeitungstätigkeiten und Projekte diagnostizieren, rechtliche, finanzielle und reputationsbezogene Risiken bewerten sowie Maßnahmen zur Compliance dokumentieren – ergänzt durch Kennzahlen wie Betroffenenanfragen, Datenpannen oder erstellte Dokumentenvorlagen. Das entspricht dem deutschen Verständnis des Tätigkeitsberichts als Risiko- und Steuerungsdokument für die Geschäftsführung.

Einen Unterschied gibt es allerdings: Die CNIL empfiehlt, die Berichtsinhalte auch an Mitarbeitende und Arbeitnehmervertretungen weiterzugeben. Die CNIL sieht den Tätigkeitsbericht somit nicht nur als Managementinstrument, sondern auch als Mittel zur Sensibilisierung der Beschäftigten.

Ein Bericht könne:

- die Sichtbarkeit des Datenschutzbeauftragten erhöhen,
- laufende Datenschutzaktivitäten sichtbar machen,
- den Handlungsbedarf verdeutlichen.

Hierfür empfiehlt die CNIL, wesentliche Erkenntnisse aus dem Managementbericht in geeigneter Form mit den Mitarbeitenden und den Arbeitnehmervertretungen zu teilen.

Im deutschen Kontext dürfte in diesem Punkt zumindest Zurückhaltung geboten sein. Da der Tätigkeitsbericht typischerweise sensible Risikoeinschätzungen enthält, sollte eine Weitergabe an den Betriebsrat oder die Belegschaft stets in Abstimmung mit der Geschäftsführung erfolgen – andernfalls kann das Vertrauensverhältnis zwischen DSB und Leitung belastet werden.

Hinsichtlich Form und Rhythmus besteht Gestaltungsfreiheit: Der Bericht kann quartalsweise, halbjährlich oder jährlich erstellt werden. Die Mustervorlage der CNIL ist auch für deutsche DSB eine praxistaugliche Orientierungshilfe.

Foto: Suriyo, Adobe Stock

Datenpannenmanagement: LDI NRW identifiziert strukturelle Schwachstellen

Keine Datenpanne in zwei Jahren – klingt gut, ist aber verdächtig. Zu diesem Schluss kommt die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW) nach einer Befragung von 33 Kliniken zum Umgang mit Datenschutzvorfällen. Das Ergebnis zeigt ein gemischtes Bild: solide IT-Sicherheitsstandards auf der einen, mögliche Lücken im internen Meldewesen auf der anderen Seite.

Untersuchungsgegenstand und Methodik

Die LDI NRW befragte 23 Krankenhäuser der Landschaftsverbände Westfalen-Lippe und Rheinland sowie die zehn NRW-Universitätskliniken. Der Fokus auf Kliniken begründet sich mit der besonderen Sensibilität der dort verarbeiteten Gesundheitsdaten, bei denen Datenverluste besonders schwerwiegende Folgen haben können.

Positiv: Geringe Cyberangriffslast, proaktive Betroffeneninformation

Verglichen mit anderen Sektoren sind Kliniken wenig von Cyberangriffen betroffen – ein Befund, den die LDI NRW auf bereits implementierte IT-Sicherheitsstandards zurückführt. Die häufigsten Datenpannen waren Fehlversendungen und unbefugte Datenweitergaben. Bemerkenswert positiv ist, dass in 21 Prozent (2023) bzw. 13 Prozent (2024) der Fälle betroffene Personen auch dann informiert wurden, wenn keine rechtliche Benachrichtigungspflicht bestand. Dieser Ansatz wird von der Landesbeauftragten Bettina Gayk ausdrücklich begrüßt.

Kritisch: Null-Meldungen als Warnsignal

Zwölf der befragten Einrichtungen gaben an, in den Jahren 2023 und 2024 keine einzige Datenpanne verzeichnet zu haben. Die LDI NRW wertet dies als Hinweis auf unzureichende interne Meldeprozesse: Vorfälle dürften direkt mit Betroffenen geklärt worden sein, ohne die vorgeschriebenen internen Dokumentationspflichten zu erfüllen.
Für Datenschutzverantwortliche in Gesundheitseinrichtungen ist dies ein zentraler Hinweis: Auch Datenpannen mit lediglich geringem Risiko müssen intern dokumentiert werden. Die Dokumentation dient nicht nur der Erfüllung aufsichtsbehördlicher Anforderungen, sondern auch der Erkennung von Häufungen in bestimmten Bereichen und der gezielten Weiterentwicklung des Pannenmanagements.

Empfehlung der Aufsichtsbehörde

Die Landesbeauftragte Gayk empfiehlt regelmäßige Schulungen der Beschäftigten zu meldepflichtigen Sachverhalten und zu internen Meldewegen als wesentliche Maßnahme zur Verbesserung des Datenpannenmanagements.

Foto: MDABDUR, Adobe Stock

Praxisnahe Handreichung zum Datenpannenmanagement

Passend zur jüngsten Verwarnung der Berliner Verkehrsbetriebe (BVG) durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) eine strukturierte Handreichung zum Vorgehen bei Datenpannen veröffentlicht. Das nützliche Referenzdokument richtet sich an Datenschutzverantwortliche und bereitet die wesentlichen Pflichten kompakt und praxisorientiert auf.

Meldepflicht und Risikobewertung als Ausgangspunkt

Die Meldepflicht nach Art. 33 DS-GVO liegt stets beim Verantwortlichen – auch wenn der Vorfall beim Auftragsverarbeiter eingetreten ist. Dieser muss den Verantwortlichen so schnell wie möglich informieren; die Meldung an die zuständige Aufsichtsbehörde hat innerhalb von 72 Stunden zu erfolgen. Bei noch laufenden Untersuchungen ist eine schrittweise Meldung zulässig.

Entscheidend ist zunächst eine sorgfältige Risikobewertung anhand von Schadenschwere und Eintrittswahrscheinlichkeit. Ergibt die Bewertung kein Risiko für die Rechte und Freiheiten natürlicher Personen, entfällt die Meldepflicht: Die interne Dokumentationspflicht nach Art. 33 Abs. 5 DS-GVO bleibt jedoch in jedem Fall bestehen. Bei hohem Risiko tritt zusätzlich die Pflicht zur unverzüglichen Benachrichtigung der betroffenen Personen nach Art. 34 DS-GVO hinzu.

Was das ULD nach Eingang einer Meldung prüft

Das ULD prüft insbesondere,

- ob die Benachrichtigungspflicht erkannt und umgesetzt wurde,
- ob die Frist eingehalten oder eine Verzögerung begründet wurde,
- ob das Risiko angemessen bewertet wurde und
- ob geeignete technische und organisatorische Maßnahmen zur Behebung und Prävention getroffen wurden.

Ergänzend weist das ULD auf ein in der Praxis häufig übersehenes Verwertungsverbot hin: Inhalte, die im Rahmen einer Meldung oder Benachrichtigung zwingend mitzuteilen sind, dürfen in Straf- und Ordnungswidrigkeitenverfahren gegen Meldepflichtige grundsätzlich nicht verwendet werden.

Einordnung

Die Handreichung ergänzt die bestehenden DSK-Kurzpapiere sinnvoll und ist insbesondere für Organisationen hilfreich, die ihr internes Datenpannenmanagement, etwa im Nachgang zu aufsichtsbehördlichen Prüfungen, überarbeiten oder in Schulungsunterlagen einbetten möchten. Die im BVG-Fall festgestellten Defizite bei der AVV-Gestaltung, der Löschkontrolle und den Meldeprozessen illustrieren anschaulich, wie hoch die praktischen Anforderungen in diesem Bereich tatsächlich sind.

Benno Hoff - stock.adobe.com

19. GDD-Sommer-Workshop

für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

17.–19.08.2026 | Timmendorfer Strand

Praxisthemen:

- ✓ Aktuelle Entwicklungen im Datenschutz
- ✓ Der HR Bereich als Einfallstor für Hochrisiko KI: Herausforderung für Datenschutz und Compliance
- ✓ Aktuelles zu MS365 aus dem Ländle: der schwäbische Weg als Blaupause für die Republik?
- ✓ KI-Kompetenz konkret – Ein Konzept für KI-Schulungen im Unternehmen
- ✓ Screening, legal oder illegal?
- ✓ Die DS-GVO als „Waffe“ im Arbeitsrecht: Trends zu Auskunft und Schadensersatz im Beschäftigungsverhältnis

Jetzt anmelden: **www.datakontext.com/sommerworkshop**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

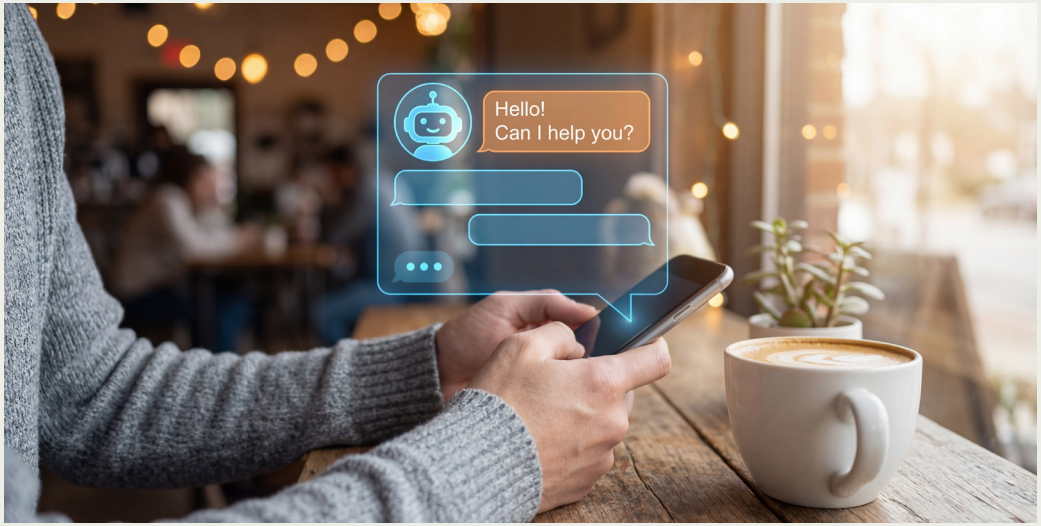

Foto: Anusa, Adobe Stock

LLM-gestützte Chatbots in der öffentlichen Verwaltung

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat mit „AI in a Nutshell 3 ⬇ “ eine praxisorientierte Kurzinformation zum datenschutzkonformen Einsatz von LLM-gestützten Chatbots in bayerischen Behörden veröffentlicht. In dem Dokument werden die relevanten Anforderungen entlang der drei Phasen Beschaffung, Implementierung und Nutzung strukturiert dargestellt.

Beschaffung: Vorabprüfung als Pflichtprogramm

Bereits im Vorfeld der Beschaffung ist umfassend zu klären, ob und in welchem Umfang eine Verarbeitung personenbezogener Daten überhaupt erforderlich ist. Dabei sind grundlegende Architekturentscheidungen zu treffen:

- Soll es ein offenes oder ein abgeschottetes System sein?
- Soll ein RAG-Subsystem angebunden werden?
- Soll ein vortrainiertes Modell oder eine cloudbasierte Infrastruktur genutzt werden?

Daneben ist frühzeitig zu prüfen, ob Auftragsverarbeitungsvereinbarungen nach Art. 28 Abs. 3 DS-GVO abzuschließen sind.

Implementierung: Dokumentation, Transparenz und technische Absicherung

Beim Einsatz von extern vortrainierten Chatbots ist eine angemessene Bewertung der Datenschutzkonformität des Systems erfolgen. Gegebenenfalls sind risikomindernde Maßnahmen zu ergreifen. Pflichtdokumente sind die Datenschutz-Folgenabschätzung und das Verarbeitungsverzeichnis. Gegenüber externen Nutzern ist zudem die Transparenzpflicht aus Art. 50 Abs. 1 KI-Verordnung (KI-VO) zu beachten: Personen müssen darüber informiert werden, dass sie mit einer Maschine interagieren.

Auf technischer Ebene empfiehlt der BayLfD die Minimierung unzulässiger Dateneingaben, die Deaktivierung des Nachtrainings mit Eingabedaten sowie die Deaktivierung der Chat-Historie. Bei behördeninterner Nutzung sollten zusätzlich Funktionsaccounts und Schnittstellen zur Datenminimierung eingesetzt sowie Dienstanweisungen und Beschäftigtenschulungen implementiert werden.

Nutzung: Laufende Kontrolle und Ausgabenprüfung

Im Betrieb sind die Datenschutzmaßnahmen regelmäßig zu überprüfen und bei Bedarf anzupassen. Chatbot-Ausgaben sind insbesondere hinsichtlich Diskriminierungsfreiheit, Richtigkeit, Vollständigkeit sowie etwaigem Personenbezug und der zugehörigen Rechtsgrundlage zu kontrollieren.

Das Dokument ergänzt die bereits im März 2026 veröffentlichte umfassende Orientierungshilfe des BayLfD zu KI-Projekten in der bayerischen Verwaltung ⧉ und bietet Datenschutzverantwortlichen eine kompakte Checkliste für alle Projektphasen.

Foto: hanohiki, Adobe Stock

Kontrollversagen bei Auftragsverarbeitung führt zur Verwarnung durch Aufsichtsbehörde

Auftragsverarbeitung ist kein Freifahrtschein. Wer personenbezogene Daten an Dienstleister auslagert, bleibt als Verantwortlicher in der Pflicht – für Löschkontrolle, Vertragsgestaltung und Incident Response gleichermaßen. Ein aktueller Fall aus Berlin illustriert eindrücklich, was passiert, wenn alle drei Bereiche gleichzeitig vernachlässigt werden.

Der Vorfall

Ein von der BVG beauftragter Dienstleister, der im Januar 2025 Briefe und E-Mails im Auftrag der BVG versandt hatte, wurde am 17. April 2025 erfolgreich angegriffen. Dabei waren rund 180.000 Kundendatensätze betroffen, darunter Namen, Anschriften, Vertrags- und Kundennummern sowie teilweise E-Mail-Adressen. Bankdaten und Passwörter waren laut BVG nicht betroffen.

Mehrfaches Versagen auf Seiten des Verantwortlichen

Die aufsichtsbehördliche Prüfung ergab drei voneinander unabhängige Verstöße:

Erstens hatte die BVG nicht kontrolliert, ob der Dienstleister die Kundendaten nach Auftragsabschluss tatsächlich gelöscht hatte, sondern sich allein auf die vertragliche Vereinbarung verlassen. Dies wurde als ein Verstoß gegen Art. 5 Abs. 2 i. V. m. Abs. 1 lit. c, e und f sowie Art. 32 Abs. 1 DS-GVO bewertet.

Zweitens überschritt die BVG die gesetzliche 72-Stunden-Meldefrist nach Art. 33 DS-GVO: Spätestens am 25. April 2025 lagen ausreichende Anhaltspunkte für einen meldepflichtigen Vorfall vor, die formelle Meldung erfolgte jedoch erst am 30. April 2025.

Drittens fehlte im Auftragsverarbeitungsvertrag ein konkretes Verfahren für den Umgang mit Datenschutzvorfällen, was einen Verstoß gegen Art. 28 Abs. 3 Satz 2 lit. f DS-GVO begründet.

Einordnung der Aufsichtsbehörde

Die Datenschutzbeauftragte Meike Kamp betonte, dass die Auslagerung von Datenverarbeitungen nicht zu Verzögerungen bei Untersuchungs- oder Meldeprozessen führen dürfe. Der Fall verdeutliche zudem das Risiko, das von unnötig lang gespeicherten Daten ausgeht. Eine konsequente Löschkontrolle hätte den Vorfall in diesem Ausmaß verhindert. Die BVG hat mittlerweile Maßnahmen angekündigt, um vergleichbare Vorfälle künftig zu vermeiden.

Foto: Wisnu, Adobe Stock

KI-Verordnung: Rat und Parlament einigen sich auf Vereinfachungen im Omnibus-Paket

Am 7. Mai 2026 haben sich das Europäische Parlament und der Rat auf eine vorläufige Einigung zum sogenannten „Digital Omnibus on AI" verständigt. Es ist damit die erste substanzielle Änderung der KI-Verordnung (EU) 2024/1689, bevor deren zentrale Hochrisiko-Pflichten überhaupt in Kraft getreten sind. Der Vorschlag ist Teil des Gesetzgebungspakets „Omnibus VII" im Rahmen der EU-Vereinfachungsagenda und zielt darauf ab, wiederkehrende Verwaltungskosten zu senken und Unternehmen zu entlasten.

Wesentliche Änderungen im Überblick

Die Neufassung von Art. 4 KI-VO stellt klar, dass Arbeitgeber lediglich angemessene Maßnahmen zur Förderung der KI-Kompetenz ihrer Beschäftigten ergreifen müssen. Ein bestimmtes individuelles Kompetenzniveau ist ausdrücklich nicht mehr zu gewährleisten. Für Datenschutzbeauftragte und Compliance-Verantwortliche ist dies insofern relevant, da damit bisherige Unsicherheiten über den Umfang organisatorischer Schulungspflichten damit erheblich reduziert werden.
Bei den Fristen für Hochrisiko-KI-Systeme sieht die Einigung Verlängerungen vor: Eigenständige KI-Systeme wie KI-gestützte Bewerber-Screening-Tools unterliegen den einschlägigen Vorschriften erst ab Dezember 2027, in Produkte eingebettete Systeme erst ab August 2028. Zudem werden regulatorische Erleichterungen, die bislang nur für kleine und mittlere Unternehmen (KMU) galten, auf kleine Unternehmen mit mittlerer Kapitalisierung ausgeweitet. Darüber hinaus schafft die Einigung mehr Spielraum für die Verarbeitung sensibler personenbezogener Daten zur Erkennung und Korrektur von algorithmischen Verzerrungen. Überschneidungen zwischen der KI-VO und branchenspezifischen Vorschriften, etwa im Maschinen- oder Medizinprodukterecht, sollen künftig durch klarere Abgrenzungen und Kommissionsleitlinien vermieden werden.

Governance und nächste Schritte

Die Zuständigkeiten zwischen dem EU AI Office und den nationalen Aufsichtsbehörden werden klarer abgegrenzt, um eine einheitlichere Anwendung der Vorschriften zu fördern. Der Ausschuss der ständigen Vertreter (AStV) II hat das Verhandlungsergebnis am 13. Mai 2026 gebilligt; die zuständigen EP-Ausschüsse stimmten am 2. Juni ab, das Plenum folgte in der darauffolgenden Juniwoche. Das Inkrafttreten ist für den 1. August 2026 vorgesehen.

Foto: Khalid Ghurafa, Adobe Stock

KI in der Justiz: Rahmen für den rechtskonformen Einsatz

Die Bundesregierung hat in einer Antwort auf eine Kleine Anfrage der AfD-Fraktion (BT-Drs. 21/5985, 18. Mai 2026 ⭳) umfassend zum Einsatz künstlicher Intelligenz in der deutschen Justiz Stellung genommen. Ausgangspunkt war die öffentliche Diskussion um KI-generierte Schriftsätze bei Sozialgerichten, die durch den Mangel an Fachanwälten für Sozialrecht begünstigt wird – mithin ein Bereich, in dem mit rund 1.600 zugelassenen Fachanwälten eine erhebliche Unterversorgung gegenüber anderen Rechtsgebieten besteht.

Laufende Pilotprojekte mit ersten Echtbetrieben

In mehreren Bundesländern laufen bereits konkrete KI-Projekte: Die Vorhaben „ALeKS“ (Niedersachsen/Bayern) und „JANO“ (Hessen/Baden-Württemberg) zielen auf Urteilsanonymisierung, Verfahrensstrukturierung und Datenextraktion. „JANO“ wurde im Dezember 2025 für die Zivilgerichtsbarkeit in den Echtbetrieb überführt und erzielt nach Angaben der Bundesregierung bereits höhere Trefferquoten als die manuelle Bearbeitung. Ergänzend soll das niedersächsische Projekt „MAKI“ den Umgang mit Massenverfahren erleichtern.

Regulatorischer Rahmen: EU-KI-VO als zentrale Rechtsgrundlage

Regulatorisch verortet die Bundesregierung den Justizeinsatz von KI im Hochrisikobereich gemäß EU-KI-Verordnung (2024/1689). Daraus resultieren verbindliche Anforderungen an das Risiko- und Qualitätsmanagement, die Datenqualität, die technische Dokumentation sowie die menschliche Aufsicht. Ergänzend wurde im Juni 2025 eine gemeinsame Bund-Länder-KI-Strategie für die Justiz verabschiedet, die unter anderem länderübergreifende Standards für das Risikomanagement und Leitlinien zur Daten-Governance vorsieht.
Verfassungsrechtlich bleibt die endgültige Entscheidungskompetenz ausschließlich bei den Richterinnen und Richtern – KI darf lediglich unterstützend wirken. Hinsichtlich datenschutzrechtlicher Fragestellungen sieht die Bundesregierung das europäische Datenschutzrecht grundsätzlich als ausreichend an, prüft jedoch weiteren gesetzgeberischen Handlungsbedarf.

Kompetenzaufbau und Finanzierung

Zur Qualifizierung von Richtern, Staatsanwälten und Justizpersonal ist die Entwicklung eines KI-Kompetenz-Frameworks geplant. Finanziell begleitet der Bund entsprechende Ländervorhaben im Rahmen der Digitalisierungsinitiative für die Justiz, die bis Ende 2026 läuft und nahtlos in den neuen „Pakt für den Rechtsstaat“ mit einer Laufzeit von drei weiteren Jahren übergehen soll.

Data Agenda Podcast Folge 94: KI-Reallabore, Kinder und Gesundheit. Was Digitalrechte und Medizinforschung verbindet.

Die unabhängige Expertenkommission „Kinder- und Jugendschutz in der digitalen Welt" hat am 24. Juni 2026 ihre Handlungsempfehlungen vorgelegt. Der Bericht trägt den Titel „Entwicklung stärken, Verantwortung übernehmen" und befasst sich insbesondere mit den Auswirkungen Künstlicher Intelligenz auf Kinder und Jugendliche.

Markus Beckedahl, der Gründer des Zentrums für Digitalrechte und Demokratie, diskutiert das „KI-Seepferdchen" (HE 12), die Gefahren durch AI Companions (HE 46), Anreize für eine vertrauenswürdige europäische Plattform- und Dateninfrastruktur (HE 50) sowie die Entwicklung kindgerechter KI im Sinne der digitalen Souveränität der EU (HE 48). Letztere soll und kann in KI-Reallaboren nach Art. 57 bis 59 KI-VO entwickelt werden.

Dies gilt auch für KI, die für die Medizin entwickelt werden soll. Prof. Dr. Dr. Felix Sahm, Direktor der Neuropathologie am Universitätsklinikum Heidelberg, berichtet über das Forschungsprojekt EuCanAI, in dem im Sinne der digitalen Souveränität der EU ein KI-Agent zur Verbesserung der Diagnostik und Behandlung von Hirntumoren entwickelt werden soll. Warum die Gesundheitsforschung dafür auf KI-Reallabore angewiesen ist, erläutert Lucia Burkhardt, Datenschutzjuristin und wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht der TH Köln.

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