NEWS BOX DATENSCHUTZ



INHALTSVERZEICHNIS

2 Editorial
3 Datenübertragbarkeit: Gescannte PDF-Tabellen sind nicht maschinenlesbar
4 KI-Chatbots: Art. 9 DS-GVO gilt auch für ungefragt eingegebene sensible Daten
4 DSK aktualisiert Kurzpapier Nr. 20 zur Einwilligung
5 EDSA-Leitlinien für Bußgeld werden aktualisiert
6 Einwilligung zugunsten von „Partnern“ ist zu unbestimmt
7 Smart Glasses: Wer aufnimmt, ist verantwortlich
8 Standortdaten: 403 Millionen Euro Bußgeld gegen Google
9 Verlorene Papierakte: DS-GVO greift, Schadensersatz aber nicht
10 408.000 Euro Bußgeld wegen fehlenden Datenschutzes durch Technikgestaltung
12 Impressum

AUSGABE
11/2026



Levent Ferik

Waffengleichheit oder Papierflut?

4.022 Beschwerden in einem Jahr, rund 70 Prozent mehr als im Vorjahr. So lautet die Bilanz des Landesbeauftragten für den Datenschutz Niedersachsen für das Jahr 2025. Ein Grund dafür: KI-Chatbots liefern bei der Recherche zu Datenschutzverstößen gleich die passende Musterbeschwerde mit. Aus Ärger wird mit wenigen Klicks ein förmliches Verfahren. Und dieses Phänomen beschränkt sich längst nicht auf die Datenschutzaufsicht.

Zunächst ist das eine gute Nachricht. Behördendeutsch war lange eine Hürde, die vor allem jene nahmen, die die Sprache der Verwaltung beherrscht oder sich Beratung leisten konnten. KI übersetzt Bescheide, erklärt Fristen und hilft, Anliegen zu formulieren. Das schafft ein Stück Waffengleichheit. Die Datenschutzgrundverordnung (DS-GVO) hat Betroffenenrechte bewusst ohne Formvorgaben und ohne Anwaltszwang angelegt. Dass sie nun genutzt werden, sollte niemand beklagen.

Die Kehrseite: Was ohne Mühe entsteht, entsteht in Massen. Aus einem Satz Unmut werden drei Seiten Schriftsatz, mit Normzitaten, Fristsetzungen und mitunter erfundenen Aktenzeichen. Jedes Schreiben muss gelesen und beschieden werden – ob es mit Sorgfalt oder per Knopfdruck entstand. KI-Slop droht Ämter und Gerichte, die schon heute überlastet sind, weiter zu lähmen. Leidtragende wären ausgerechnet jene mit berechtigten Anliegen. Höhere Hürden wären trotzdem die falsche Antwort. Für offenkundig unbegründete oder exzessive Anträge gibt es mit Art. 12 Abs. 5 DS-GVO bereits ein Instrument. Gefragt sind vielmehr eine KI-gestützte Eingangstriage, effiziente Prozesse für Standardfälle und vor allem verständliche Kommunikation. Wer klar schreibt, nimmt manchem KI-Schreiben den Anlass. Das gilt für Behörden ebenso wie für Unternehmen, auf die ebenfalls mehr Auskunftsersuchen und Widersprüche zukommen werden.

KI hat die Schwelle zum Rechtsstaat gesenkt. Jetzt muss der Rechtsstaat beweisen, dass er auch jenseits dieser Grenze handlungsfähig bleibt.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com



Foto: dizain, Adobe Stock

Datenübertragbarkeit: Gescannte PDF-Tabellen sind nicht maschinenlesbar

Das Oberlandesgericht (OLG) Stuttgart hat mit Teilurteil vom 31.07.2026 (Az. 5 U 271/24) die Anforderungen an das Format einer Datenkopie präzisiert. Entscheidend ist, ob die betroffene Person Auskunft nach Art. 15 DS-GVO oder die Herausgabe ihrer Daten nach Art. 20 DS-GVO verlangt.

Sachverhalt

Ein Spieler verlangte von einem in Malta ansässigen Anbieter von Online-Sportwetten und virtuellen Automatenspielen seine vollständige Zahlungs- und Spielhistorie. Er wollte damit im Rahmen einer Stufenklage Rückzahlungsansprüche beziffern. Der Anbieter übermittelte einen 62-seitigen Kontoauszug als PDF, der lediglich einen Papierausdruck abbildete. Markieren, Kopieren oder Durchsuchen war nicht möglich. Das LG Stuttgart hatte die Klage noch abgewiesen, da ein PDF ein gängiges elektronisches Format sei.

Weiter auf DataAgenda lesen



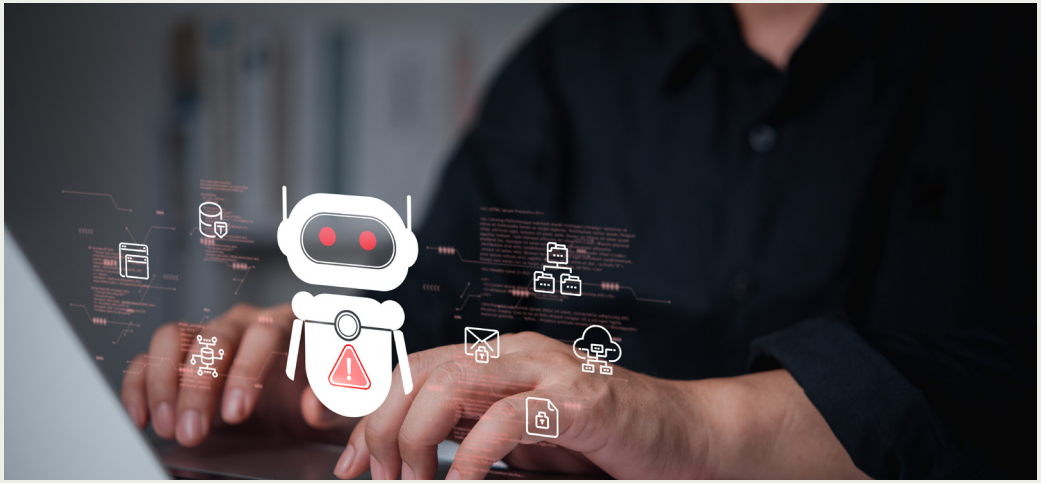


Foto: khunkornStudio, Adobe Stock

KI-Chatbots: Art. 9 DS-GVO gilt auch für ungefragt eingegebene sensible Daten

Das Landgericht (LG) Köln hat mit Urteil vom 17.09.2026 (Az. 33 O 120/24) einer Unterlassungsklage des Verbraucherzentrale Bundesverbands (vzbv) gegen die Snap Group Limited in vollem Umfang stattgegeben. Im Mittelpunkt steht der in Snapchat integrierte KI-Chatbot „My AI“, der bereits Nutzenden ab 13 Jahren offensteht.

Weiter auf DataAgenda lesen



Foto: Gilang, Adobe Stock

DSK aktualisiert Kurzpapier Nr. 20 zur Einwilligung

Die Datenschutzkonferenz (DSK) hat ihr Kurzpapier Nr. 20 zur Einwilligung nach der DS-GVO überarbeitet und mit Stand vom 23.09.2026 veröffentlicht. Beschlossen wurde es auf der 3. Zwischenkonferenz, auf der auch das Kurzpapier Nr. 2 zu Aufsichtsbefugnissen und Sanktionen aktualisiert wurde. Das Papier orientiert sich an den EDSA-Leitlinien 05/2020 und fasst die Anforderungen an eine wirksame Einwilligung nach Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 DS-GVO zusammen.

Weiter auf DataAgenda lesen



Foto: Stefan Klein/imageBROKER, Adobe Stock

EDSA-Leitlinien für Bußgeld werden aktualisiert

Der Europäische Datenschutzausschuss (EDSA) hat die Leitlinien 04/2026 angenommen und zur öffentlichen Konsultation gestellt. Sie regeln, wann Aufsichtsbehörden ein Bußgeld statt oder neben anderen Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO verhängen sollen. Die Leitlinien 04/2022 zur Berechnung der Bußgeldhöhe bleiben daneben bestehen, die bisherigen Leitlinien der Artikel-29-Datenschutzgruppe zu diesem Thema werden ersetzt.

Fünf Schritte bis zur Geldbuße

Die ersten drei Schritte prüfen die rechtlichen Voraussetzungen: Ist der Verstoß bußgeldbewehrt, kann der Adressat belangt werden und liegt Verschulden vor? Für Fahrlässigkeit genügt nach Ansicht des EDSA, dass der Verantwortliche den Verstoß hätte erkennen müssen. Existieren EDSA-Leitlinien zu der Frage, ist ein Rechtsirrtum stets vermeidbar. Verantwortliche haften zudem für das Handeln aller Personen, die in ihrem Namen tätig werden.

Im vierten Schritt wird anhand der Kriterien des Art. 83 Abs. 2 DS-GVO geprüft, ob ein geringfügiger Verstoß vorliegt. Dann genügt in der Regel eine Verwarnung. Anderenfalls spricht eine starke Vermutung für ein Bußgeld. Im fünften Schritt wird schließlich geprüft, ob das Bußgeld wirksam, verhältnismäßig und abschreckend ist.

Was mildernd wirkt und was nicht

Für die Praxis sind die Aussagen zu den Zumessungskriterien besonders aufschlussreich:

- Keine früheren Verstöße und die gesetzlich geschuldete Kooperation wirken nicht mildernd, denn Rechtstreue ist der Normalfall.
- Freiwillige Abhilfemaßnahmen vor Beginn der Ermittlungen und eine nicht verpflichtende Selbstanzeige können mildernd wirken.
- Wirtschaftliche Vorteile aus dem Verstoß sprechen deutlich gegen einen geringfügigen Fall.

Verantwortliche sollten Abhilfemaßnahmen frühzeitig ergreifen und dokumentieren. Stellungnahmen zum Entwurf sind bis zum 13.11.2026 möglich.

Einwilligung zugunsten von „Partnern“ ist zu unbestimmt

Eine Einwilligung in Direktwerbung durch nicht näher bezeichnete „Partner“ reicht nicht aus, damit ein Drittunternehmen die Daten für eigene Werbung nutzen darf. Das hat Generalanwalt Dean Spielmann in seinen Schlussanträgen vom 17.09.2026 in der Rechtssache C-317/25 (Groupe Canal+) vorgeschlagen.



Foto: Fabio Balbi, Adobe Stock

Sachverhalt

Die Canal+-Gruppe hatte 2021 elektronische Werbung an rund 3,9 Millionen Personen versandt. Die Kontaktdaten stammten von Internetanbietern, deren Nutzer bei der Anmeldung in eine Weitergabe an „Partner“ eingewilligt hatten. Die französische Aufsichtsbehörde CNIL sah darin keine wirksame Einwilligung und verhängte eine Geldbuße von 600.000 Euro. Der Conseil d’État legte dem EuGH die Frage vor, wie genau eine solche Empfängerkategorie bestimmt sein muss.

Kernaussagen

Nach Auffassung des Generalanwalts ist eine Einwilligung nur dann informiert, wenn die betroffene Person den Verantwortlichen identifizieren kann. Der Begriff „Partner“ sei dafür zu vage. Die Beschreibung müsse so genau sein, dass Betroffene vernünftigerweise damit rechnen können, von dem konkreten Unternehmen kontaktiert zu werden. War der Verantwortliche bei der ursprünglichen Einwilligung nicht erkennbar, muss er selbst eine neue Einwilligung einholen. Eine Abmeldemöglichkeit in der ersten Werbenachricht ersetzt die fehlende vorherige Einwilligung nicht.

Die Schlussanträge binden den Gerichtshof nicht, folgt er ihnen aber, hätte das erhebliche Folgen für den Adresshandel, die Co-Registrierung und die Lead-Generierung. Unternehmen, die Werbeadressen von Dritten beziehen, sollten prüfen, ob die zugrunde liegenden Einwilligungstexte sie als Empfänger konkret benennen.

Smart Glasses: Wer aufnimmt, ist verantwortlich

Wer mit einer KI-Brille filmt oder fotografiert, ist datenschutzrechtlich selbst Verantwortlicher. Das stellt der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) in einem Prüfbericht vom 10.09.2026 zur Ray-Ban Meta AI Glasses fest. Die Datenschutzkonferenz hat sich der Bewertung auf ihrer Zwischenkonferenz angeschlossen.



Foto: Aleksandr Fedosov, Adobe Stock

LED reicht nicht

Die Brille zeigt Aufnahmen über eine kleine LED an. Nach dem Bericht ist sie in vielen Umgebungen kaum erkennbar, leicht abzukleben und leuchtet bei Nutzung des KI-Assistenten schwach oder gar nicht. Das bloße Aufleuchten der LED genügt nicht, um Betroffene zu informieren. Es sind zusätzliche Hinweise nötig, etwa Piktogramme oder eine direkte Ansprache. Eine Gesichtserkennung hat die Behörde bislang nicht festgestellt. Die technischen Strukturen dafür seien aber angelegt.

Haushaltsausnahme greift selten

Die Ausnahme für rein private Tätigkeiten nach Art. 2 Abs. 2 lit. c DS-GVO entfällt, sobald Aufnahmen in sozialen Netzwerken veröffentlicht werden, Unbeteiligte gezielt erfasst werden oder Daten an Meta für das KI-Training gehen. Für das Training werden Nutzende sogar gemeinsam mit Meta verantwortlich. Das Fazit fällt deutlich aus: Erkennbare Aufnahmen von Personen außerhalb des engen Freundes- und Familienkreises sind bis auf seltene Ausnahmen unzulässig.

Smart Glasses werden auch im Arbeitsalltag auftauchen, bei Beschäftigten, Besuchern oder im Kundenkontakt. Unternehmen sollten den Einsatz frühzeitig regeln, etwa in einer Nutzungsrichtlinie oder in einer Betriebsvereinbarung. Sensible Bereiche sollten davon ausdrücklich ausgenommen sein.

Standortdaten: 403 Millionen Euro Bußgeld gegen Google

Die irische Datenschutzbehörde (Data Protection Commissioner, DPC) hat am 21.09.2026 ein Bußgeld von 403 Millionen Euro gegen Google Ireland verhängt. Gegenstand ist die Verarbeitung von Standortdaten über die Kontoeinstellungen „Location History“, „Web & App Activity“ und „Location Accuracy“ im Zeitraum von Mai 2018 bis Februar 2020. Das Verfahren ging auf Beschwerden europäischer Verbraucherverbände zurück, darunter der Europäische Dachverband Bureau Européen des Unions de Consommateurs (BEUC).

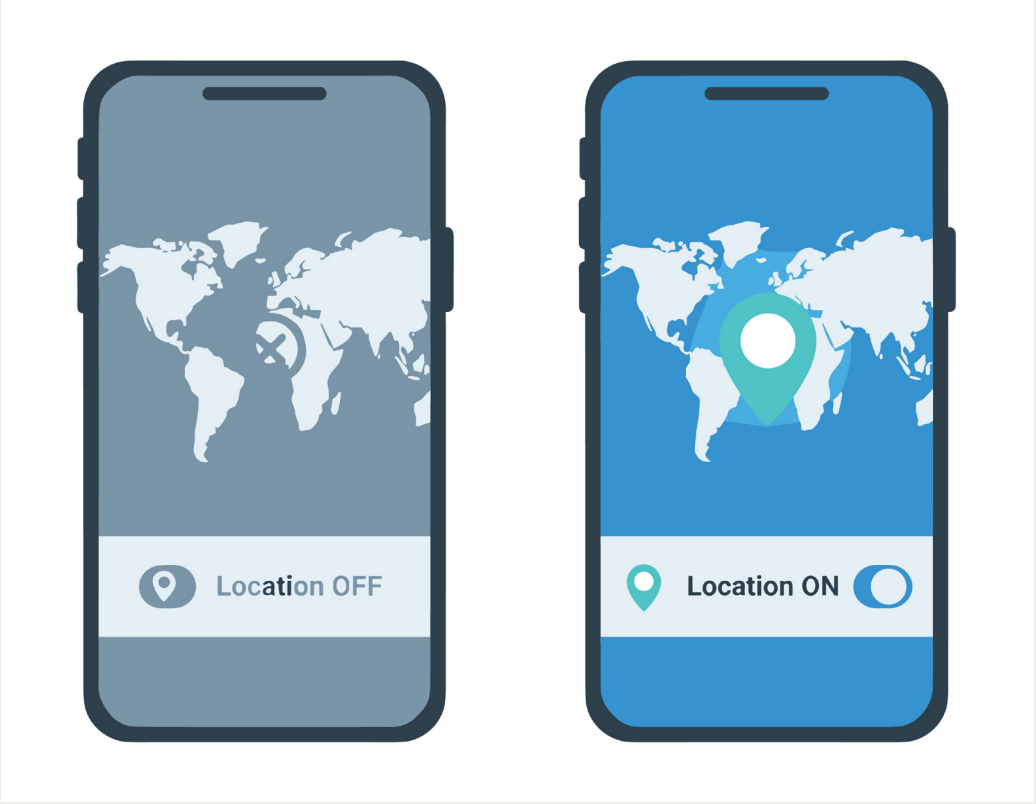


Foto: Mimi, Adobe Stock

Die Verstöße

Bei „Location History“ und „Web & App Activity“ sieht die DPC Verstöße gegen die Grundsätze der Rechtmäßigkeit und Fairness, gegen die Transparenzpflichten und gegen die Speicherbegrenzung. Bei „Location Accuracy“ konnte Google nicht nachweisen, dass die Verarbeitung den Grundsätzen entspricht, und verletzte damit die Rechenschaftspflicht. Auch hier fehlte es an Transparenz. Google muss die Verarbeitung innerhalb von sechs Monaten in Einklang mit der DS-GVO bringen.

Die Behörde betont, dass Standortdaten tiefe Einblicke in das Privatleben erlauben. Nutzerinnen und Nutzer hätten nicht erkennen können, dass ihr Aufenthaltsort für Werbung und für Rückschlüsse auf ihre Interessen genutzt wurde.

Die Entscheidung betrifft zwar einen Konzern, die Prüfmaßstäbe gelten aber allgemein. Wer Standortdaten verarbeitet, sollte transparent und für Laien verständlich über alle Verwendungszwecke informieren, insbesondere über Werbung und Profilbildung. Außerdem sind klare Löschfristen erforderlich, und die Rechtmäßigkeit muss dokumentiert sein. Gerade bei Einstellungen, die über mehrere Dienste hinweg wirken, reicht ein allgemeiner Hinweis nicht aus.



Foto: bazou, Adobe Stock

Verlorene Papierakte: DS-GVO greift, Schadensersatz aber nicht

Auch Papierakten können unter die DS-GVO fallen. Wenn eine solche Akte verschwindet, begründet das aber nicht automatisch einen Anspruch auf Schmerzensgeld. Das hat das LG Magdeburg mit Urteil vom 25.06.2026 (Az. 10 O 1894/25) entschieden. Das Urteil ist rechtskräftig.

Sachverhalt

Bei einem Fachaufsichtsbesuch in der JVA Burg fiel auf, dass ein Ordner mit der Einsatzakte für Geiselnahmen und andere Gewaltlagen verschwunden war. Darin befand sich eine Personalübersicht mit Namen, Privatadressen und privaten Telefonnummern aller Bediensteten. Die JVA informierte die Betroffenen nach Art. 34 DS-GVO. Ein Bediensteter, der täglich mit Strafgefangenen arbeitet, fürchtete um seine Sicherheit und verlangte Schmerzensgeld.

Papierakte als Dateisystem

Das Gericht stellte zunächst klar, dass die DS-GVO nicht danach unterscheidet, ob Daten digital oder auf Papier verarbeitet werden. Entscheidend sei, dass sie nach bestimmten Kriterien geordnet und gezielt auffindbar sind. Eine systematische Personalübersicht in einer Einsatzakte ist deshalb ein Dateisystem nach Art. 4 Nr. 6 DS-GVO.
Anwendbar war die DS-GVO im konkreten Fall dennoch nicht. Die Akte diente ausschließlich der Gefahrenabwehr im Strafvollzug, sodass die Ausnahme nach Art. 2 Abs. 2 lit. d DS-GVO greift. Maßgeblich sei der Zweck der Verarbeitung, nicht der Personenkreis. Die Ausnahme gilt daher auch für Daten von Beschäftigten.

Kein Schaden ohne tatsächlichen Kontrollverlust

Auch der Anspruch nach dem einschlägigen Landesrecht scheiterte. Das bloße Verschwinden der Akte begründe nur die abstrakte Möglichkeit, dass Dritte Kenntnis erlangen. Unter Verweis auf den Bundesgerichtshof (VI ZR 10/24) genügt ein solches hypothetisches Risiko nicht für einen immateriellen Schaden. Zudem traf das Land kein Verschulden, denn die Akte lag in einem verschlossenen Raum mit beschränktem Zugang. Papierakten gehören in das Verarbeitungsverzeichnis und in das Konzept der technischen und organisatorischen Maßnahmen. Wer Zugriffsbeschränkungen nachweisen kann, steht bei Haftungsfragen deutlich besser da.



Foto: Best Design, Adobe Stock

408.000 Euro Bußgeld wegen fehlenden Datenschutzes durch Technikgestaltung

Die spanische Datenschutzbehörde (Agencia Española de Protección de Datos, AEPD) hat gegen die CaixaBank Geldbußen von insgesamt 510.000 Euro festgesetzt (Verfahren PS-00028-2025). Die Bank hatte bei der Abwicklung von Erbfällen standardmäßig mehr Daten verlangt als erforderlich und die Erben unzureichend informiert. Da sie die Geldbuße freiwillig vorab bezahlte, ermäßigte sich der Betrag um 20 Prozent auf 408.000 Euro.

Sachverhalt

Nach dem Tod eines Kunden verlangte eine Filiale von den drei Erben eine vollständige notarielle Urkunde über die Annahme, Teilung und Zuweisung des Nachlasses, bevor sie das Guthaben auszahlte. Die Urkunde enthielt das gesamte Nachlassverzeichnis mit Vermögenswerten und Bewertungen sowie Daten der Witwe, die mit den Bankprodukten nichts zu tun hatten. Die Erben hatten dagegen angeboten, eine private Erklärung über die Verteilung des Kontoguthabens vorzulegen.

Fehler im Standardprozess

Die Bank verteidigte sich damit, vollständige Urkunden nie zwingend verlangt zu haben. Teilkopien seien möglich, Schwärzungen jederzeit zulässig, und notarielle Urkunden böten mehr Rechtssicherheit. Die AEPD folgte dem nicht. Der interne Erbschaftsleitfaden der Bank sehe die vollständige Urkunde als Regelfall vor. Dass im konkreten Fall eine Alternative angeboten wurde, konnte die Bank nicht belegen. Weil der Mangel systematisch im Prozess angelegt war, wertete die Behörde den Sachverhalt nicht als bloßen Verstoß gegen die Datenminimierung, sondern als Verstoß gegen Art. 25 DS-GVO. Dafür setzte sie ein Bußgeld in Höhe von 500.000 Euro fest. Weitere 10.000 Euro entfielen auf einen Verstoß gegen Art. 13 DS-GVO. Die Datenschutzhinweise der Bank enthielten keine Informationen zur Verarbeitung im Erbfall. Der allgemeine Verweis auf eine Online-Datenschutzerklärung genügte nicht, zumal die Erben in der Filiale vorsprachen. Das Wissen der Erben, dass ein Erbfall bearbeitet wird, ersetzt die Information nach Art. 13 DS-GVO nicht. Den Vorwurf eines Verstoßes gegen Art. 30 DS-GVO stellte die Behörde ein. Die Bank muss binnen sechs Monaten Abhilfe nachweisen.

Bedeutung für die Praxis

Die Entscheidung zeigt, dass Art. 25 DS-GVO vor allem standardisierte Abläufe in den Blick nimmt. Wer Nachweise anfordert, sollte bereits in Leitfäden und Checklisten festlegen, welche Angaben tatsächlich erforderlich sind. Für Verarbeitungen, die keine eigenen Kunden betreffen, wie hier die Erben, braucht es eigene Datenschutzhinweise.

DATA AGENDA PODCAST



(Quelle: TH Köln/Schmülgen)

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

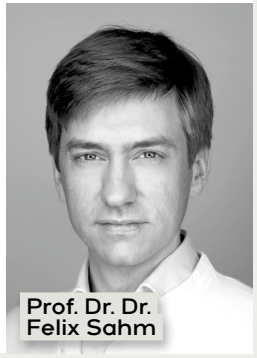
Folge #**99**

Staatsmodernisierung trifft Datenschutz – Darum brauchen wir „KI-Reallabore“ und nicht nur „Reallabore“









Data Agenda Podcast Folge 99 Staatsmodernisierung trifft Datenschutz – Darum brauchen wir „KI-Reallabore“ und nicht nur „Reallabore“

KI-Reallabore dienen nach der KI-Verordnung dazu, KI zu wichtigen, aber zugleich hochriskanten Zwecken zu entwickeln. In jedem Mitgliedstaat der EU muss mindestens ein KI-Reallabor gegründet werden. Es dürfen und sollen aber mehr sein. In Nordrhein-Westfalen soll bald ein Gesetzesentwurf verabschiedet werden. Im Podcast stellt Dr. Dominik Roderburg, Leiter des Referats Staatsmodernisierung in der Staatskanzlei NRW, den Gesetzesentwurf vor. Neuropathologe Felix Sahm erklärt, warum er für seine Forschung auf ein KI-Reallabor angewiesen ist. Bemerkenswert ist, dass Tobias Keber, LfDI Baden-Württemberg, und Denis Lehmkemper, LDI Niedersachsen, das Gesetz in NRW begrüßen. Beim Datenschutz wollen sie allerdings in ihren Bundesländern ein Wörtchen mitreden, um den Fortschritt mitgestalten zu können.
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

