NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
10/2025

Levent Ferik

EDITORIAL

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat angekündigt, gegen das Urteil des Verwaltungsgerichts (VG) Köln zu den Facebook-Fanpages vorzugehen. Viele Verantwortliche dürften dies als richtigen Schritt sehen, denn nur durch eine höhere Instanz kann weitere Klarheit darüber erlangt werden, wie die gemeinsame Verantwortung von Plattformbetreibern und Fanpage-Betreibern rechtlich zu bewerten ist.
Für viele Verantwortliche bedeutet der aktuelle Zustand vor allem Unsicherheit: Darf man eine Fanpage weiter betreiben? Welche Pflichten bestehen konkret?
Die Entscheidung des VG Köln hat diese Fragen nicht endgültig beantwortet. Ein weiteres Verfahren eröffnet die Chance, dass bald mehr Klarheit und damit eine größere **Rechtssicherheit** entsteht – und genau die brauchen Behörden, Unternehmen und Vereine, die auf digitale Kommunikation angewiesen sind und nicht auf die Reichweite einer Fanpage verzichten möchten. Kleinere Organisationen können womöglich auch gar nicht so schnell auf ein anderes Medium wechseln, ohne die für sie essenzielle Reichweite zu opfern.
Positiv hervorzuheben ist, dass der BfDI die Betreiber in dieser Übergangszeit nicht alleinlässt. Mit der veröffentlichten **Handreichung für Verantwortliche** gibt es eine praktische Orientierung, wie Fanpages bis auf Weiteres (nach ihrer Auffassung) datenschutzkonform genutzt werden können. Auch wenn sie die rechtliche Klärung nicht ersetzt, bietet sie konkrete Anhaltspunkte für die tägliche Praxis.
Der Schritt der BfDI ist zu begrüßen. Rechtssicherheit entsteht nicht von allein – sie muss erstritten werden. Bis dahin sollten Betreiber die Handreichung ernst nehmen und prüfen, ob ihre Fanpages angepasst werden müssen.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

EuGH-Urteil: Pseudonymisierte Daten bleiben personenbezogen

Ein aktuelles Urteil des Europäischen Gerichtshofs (EuGH) vom 4. September 2025 (C-413/23 P) schafft mehr rechtliche Klarheit bezüglich der Einstufung von pseudonymisierten Daten. Das Gericht hat entschieden, dass solche Daten weiterhin als personenbezogen gelten, solange der Datenverantwortliche über die Mittel zur Re-Identifizierung der betroffenen Person verfügt.

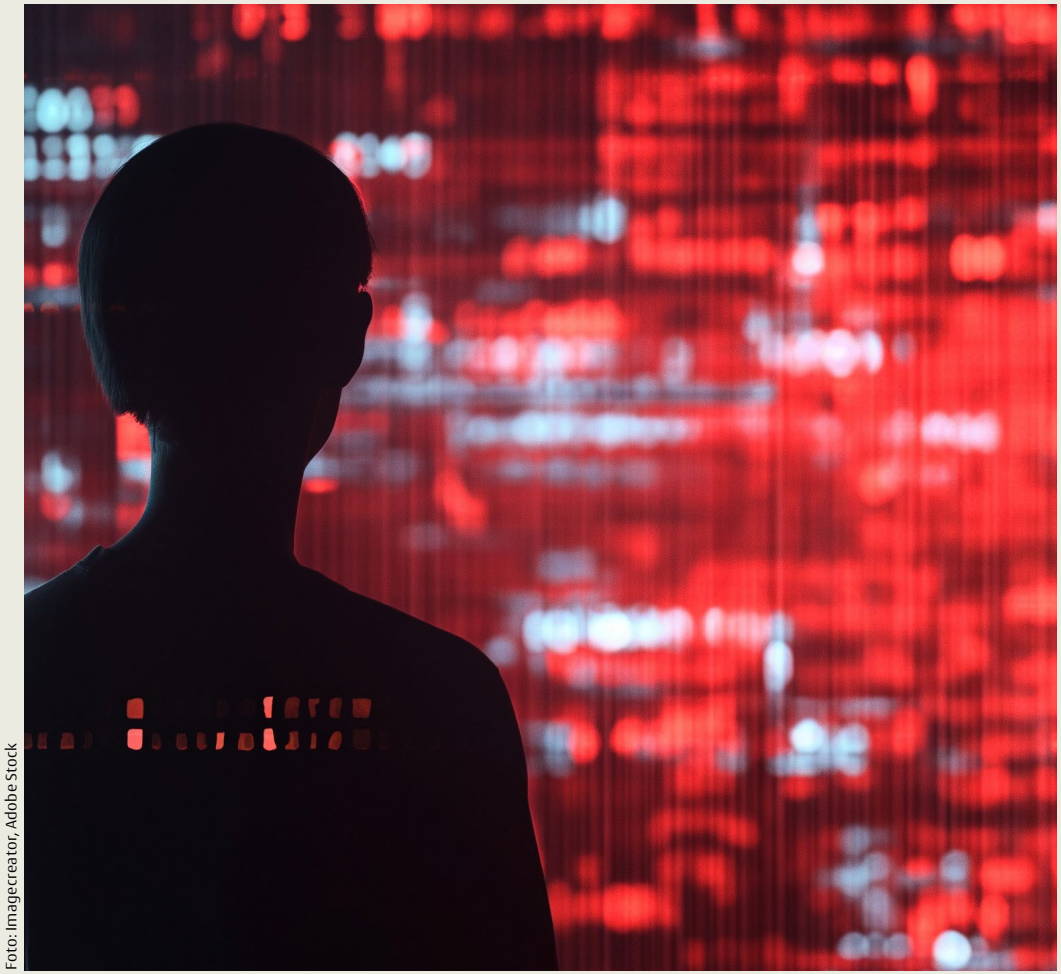

Foto: Imagecreator, Adobe Stock

Perspektive des Verantwortlichen ist entscheidend

Im Mittelpunkt des Urteils steht, dass der Personenbezug von der Perspektive des Datenverantwortlichen aus zu beurteilen ist. Es ist unerheblich, ob der Empfänger der pseudonymisierten Daten die betreffende Person nicht identifizieren kann. Diese Sichtweise bestätigt, dass die Weitergabe von pseudonymisierten Datensätzen an Dritte die datenschutzrechtlichen Verpflichtungen des Verantwortlichen nicht aufhebt.

Konsequenzen für die Praxis

Das Urteil unterstreicht die Notwendigkeit, Pseudonymisierung nicht mit Anonymisierung gleichzusetzen. Für die praktische Anwendung ergeben sich folgende Implikationen:

- **Datenschutzrechtliche Pflichten:** Die Pflichten aus der Datenschutz-Grundverordnung (DS-GVO), insbesondere das Prinzip der Datenminimierung und die Informationspflicht, bleiben für pseudonymisierte Daten in vollem Umfang anwendbar.
- **Transparenz:** Die betroffenen Personen müssen über die Weitergabe ihrer Daten informiert werden, selbst wenn der Empfänger keine Re-Identifizierung vornehmen kann.
- **Vertragsgestaltung:** Die Urteilsbegründung deutet auf die Notwendigkeit hin, vertragliche Regelungen zu treffen, die den Zugriff auf re-identifizierende Informationen ausschließen oder den Empfänger zur Einhaltung des Datenschutzrechts verpflichten.

Foto: Rasel Ai, Adobe Stock

Gericht bestätigt Angemessenheit des EU-US-Datenrahmens

Das Gericht der Europäischen Union hat die Klage auf Nichtigerklärung des neuen transatlantischen Datenschutzrahmens abgewiesen. Die Entscheidung bestätigt den Angemessenheitsbeschluss der Kommission vom 10. Juli 2023, der die Übermittlung personenbezogener Daten zwischen der Europäischen Union und den Vereinigten Staaten ermöglicht. Diese Entscheidung ist von großer Bedeutung für den internationalen Datentransfer und stellt die jüngste Entwicklung nach den Urteilen Schrems I und Schrems II dar, die frühere Rahmenwerke für ungültig erklärten.

Klagegründe und rechtliche Bewertung

Die Klage wurde von einem französischen Staatsbürger eingereicht, der die Rechtmäßigkeit des neuen Rahmens anzweifelte. Zwei zentrale Kritikpunkte wurden vorgebracht:

- die fehlende Unabhängigkeit des Data Protection Review Court (DPRC) und
- die fehlende Regulierung von Sammelerhebungen personenbezogener Daten durch US-Nachrichtendienste.

Unabhängigkeit des DPRC bestätigt

Das Gericht wies den Einwand der mangelnden Unabhängigkeit des DPRC zurück. Es stellte fest, dass die Ernennung und Funktionsweise der Richter/innen durch Garantien gesichert sind. Richter/innen können nur aus triftigen Gründen abberufen werden, und die Exekutive darf ihre Arbeit nicht unrechtmäßig beeinflussen. Außerdem unterliegt der Rechtsrahmen der kontinuierlichen Überwachung durch die Kommission, die bei Bedarf Korrekturmaßnahmen ergreifen kann.

Sammelerhebungen entsprechen EU-Recht

Auch der zweite Klagegrund – die fehlende Regulierung von Sammelerhebungen personenbezogener Daten durch US-Nachrichtendienste – wurde abgewiesen. Das Gericht stellte klar, dass das Urteil Schrems II keine vorherige Genehmigung für Sammelerhebungen verlangt. Wichtiger sei, dass eine nachträgliche gerichtliche Überprüfung möglich ist. Da das US-Recht eine solche nachträgliche Überprüfung der Signalaufklärung durch den DPRC vorsieht, ist der Rechtsschutz als dem Unionsrecht gleichwertig anzusehen. Das Urteil bestätigt somit die Rechtskonformität des immer noch gültigen transatlantischen Datenschutzrahmens.

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: asadykov, Adobe Stock

KI im Justizbetrieb: Leitlinien für verantwortlichen Einsatz

Im Februar 2025 veröffentlichte die „Sedona Conference Journal-Edition Volume 26“ die Leitlinien „Navigating AI in the Judiciary“, verfasst von fünf Richterpersönlichkeiten und einer KI-Expertin. Sie richten sich an gerichtliche Entscheidungsträger/innen und ihr Umfeld in den US-amerikanischen Bundes- und Landesgerichten. Ziel ist es, einen praxisnahen Orientierungsrahmen für den Einsatz von künstlicher Intelligenz (KI) und insbesondere generativer KI (GenAI) im Justizbetrieb zu etablieren.

Grundprinzipien für den Einsatz

Die Leitlinien betonen, dass die gerichtliche Autorität ausschließlich bei Richter/innen liegt – KI darf diese nicht ersetzen. Sie soll die Justiz unterstützen, nicht deren Unabhängigkeit oder Integrität gefährden. Richter/innen bleiben fachliche und ethische Verantwortungsträger/innen, einschließlich der kritischen Überprüfung von KI-generierten Ergebnissen.

Grenzen der KI und Risikobewusstsein

Generative KI erzeugt Inhalte auf Grundlage komplexer Trainingsdaten – allerdings ohne juristische Urteilskraft oder Verlässlichkeit. Der Text weist auf typische Fehlerquellen wie **„Halluzinationen“** (plausibel klingende, aber unzutreffende Aussage), **Automationsbias** (blindes Vertrauen in KI-Ergebnisse) sowie **Bestätigungsfehler** (Fokus auf Informationen, die eigene Vorannahmen bestätigen) hin. Auch die Vertraulichkeit, der Datenschutz und das Potenzial zur Offenlegung sensibler Informationen über Prompts müssen berücksichtigt werden.

Zulässige Einsatzbereiche unter Aufsicht

Trotz der Einschränkungen dürfen KI-Technologien nach Auffassung der Autoren unterstützend genutzt werden – stets unter menschlicher Kontrolle – etwa für:

- Legal Research (mit zuverlässiger Datenbasis);
- Zusammenfassungen von Schriftsätzen, Zeugenaussagen, Akten oder Beweismitteln;
- Entwürfe für Routinebeschlüsse;
- Korrekturlesen und Formatkontrolle;
- Erstellung von Zeitplänen, Dokumentenorganisation oder Barrierefreiheitshilfen.

Dynamischer Orientierungsrahmen

Die Leitlinien sind als lebendes Dokument konzipiert: Sie sollen regelmäßig angepasst werden, um mit technologischen Fortschritten, besserer Zuverlässigkeit von KI-Tools und neuen rechtlichen bzw. ethischen Erkenntnissen Schritt zu halten. Zentral bleibt dabei: Jede KI-Ausgabe muss letztlich vom Menschen verifiziert werden.

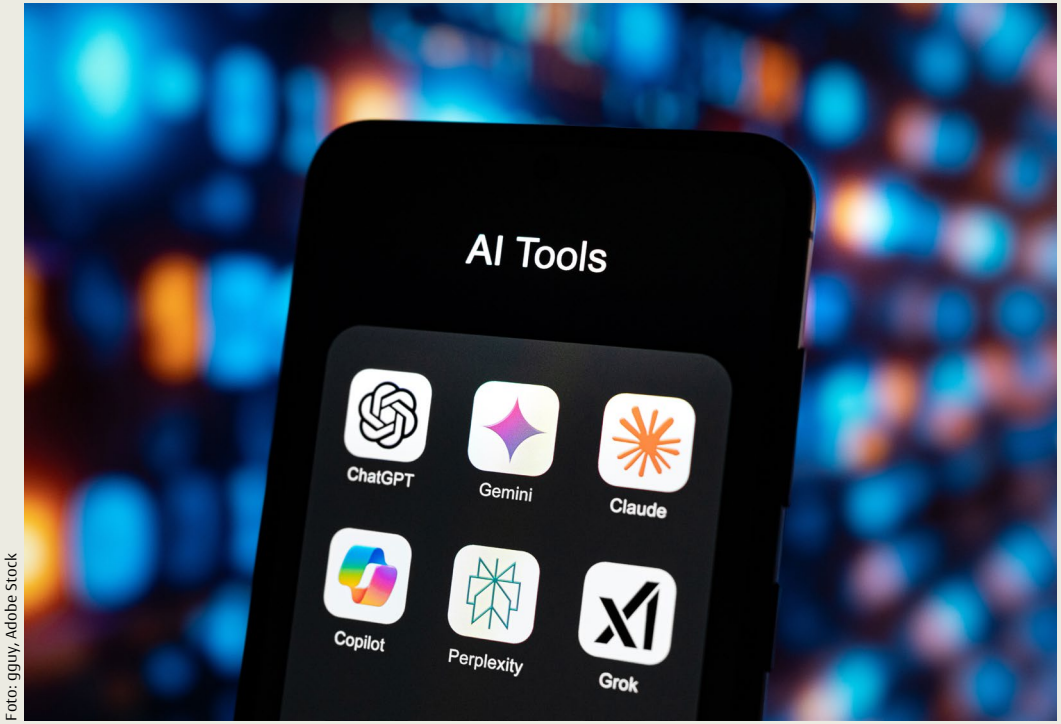

Foto: gguy, Adobe Stock

Arbeitshilfe zur datenschutzrechtlichen Orientierung beim Einsatz von KI

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) hat eine überarbeitete Version des ONKIDA (Orientierungshilfen-Navigator KI & Datenschutz) veröffentlicht. Das Tool dient als kompakte Arbeitshilfe für Behörden und Unternehmen, die KI-Technologien einsetzen oder implementieren möchten, und bringt Struktur in die vielen, teils komplexen datenschutzrechtlichen Vorgaben. Es bietet eine systematische Übersicht zentraler Datenschutzprinzipien und verweist gezielt auf relevante Hilfedokumente – inklusive Fundstellen aus verschiedenen Arbeitspapieren und Stellungnahmen.

Prof. Dr. Tobias Keber, LfDI BW, betont: „Gerade beim Thema künstliche Intelligenz und den vielen neuen Entwicklungen kann man schnell die Übersicht verlieren. ONKIDA ist das hilfreiche Tool, um den Überblick über die verschiedenen datenschutzrechtlichen Implikationen beim Einsatz von künstlicher Intelligenz zu behalten."

Inhaltliche Highlights der Version 2.0:

- Das aktualisierte Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz Künstlicher Intelligenz" des LfDI BW wurde integriert;
- neue Hinweise zur technischen und organisatorischen Sicherheit bei KI-Systemen aus der DSK-Orientierungshilfe;
- Empfehlungen der französischen Datenschutzbehörde CNIL zur KI-Entwicklung;
- die Stellungnahme des EDSA zur Verarbeitung personenbezogener Daten in KI-Modellen (Opinion 28/2024), den KI-Fragenkatalog des BfDI sowie den Bericht des EDSA zu Risiken und Risikominderung bei Large Language Models (LLMs) hat ONKIDA ebenfalls ergänzt.

Technisch präsentiert ONKIDA die Daten in übersichtlichen Tabellen: In der einen Spalte werden zentrale Datenschutzgrundsätze (z. B. Zweckbindung, Datenminimierung, Betroffenenrechte) dargestellt. Die andere Spalte enthält verlinkte Quellen, die diese Aspekte konkret behandeln, inklusive Seiten- oder Randnummern zur direkten Nachverfolgbarkeit. Mit dieser Aktualisierung unterstützt ONKIDA nicht nur den praktischen Umgang mit KI-Projekten, sondern verbessert auch den schnellen Zugriff auf fundierte Orientierungshilfen.

Foto: tonstock, Adobe Stock

KI-Stimmenklon verletzt das Recht an der eigenen Stimme

Das Landgericht Berlin hat in einem richtungsweisenden Urteil festgestellt, dass die Nutzung einer KI-generierten Stimme, die einer bekannten Synchronstimme täuschend ähnlich ist, ohne Einwilligung des Betroffenen einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht darstellt.

Ein prominenter Synchronsprecher, bekannt als deutsche Stimme u. a. von Bruce Willis, wurde ohne seine Zustimmung mittels KI-Stimmenklon in zwei YouTube-Videos eingesetzt. Der Kanalbetreiber – zugleich Betreiber eines Onlineshops – veröffentlichte Videos mit politischem Inhalt und nutzte die Stimme, um Zuschauer/innen anzuziehen und um seine kommerziellen Interessen zu fördern.

Rechtliche Bewertung

Das Gericht stellte klar, dass das allgemeine Persönlichkeitsrecht auch das Recht an der eigenen Stimme umfasst – einschließlich bekannter Synchronstimmen. Entscheidend war die Wiedererkennbarkeit der Stimme. Auch eine synthetische Stimme kann identifizierbar sein und somit eine „Zuordnungsverwirrung" erzeugen, bei der das Publikum fälschlicherweise Auftrag und Zustimmung des Betroffenen annimmt.
Die Argumentation, es handele sich um Satire oder die Stimme sei lediglich „klangvoll gewählt", wies das Gericht zurück. Die Verwendung der Stimme diente kommerziellen Zwecken – namentlich der Reichweitensteigerung und der Bewerbung eines Webshops – und nicht der künstlerischen Auseinandersetzung mit der Stimme oder der Persönlichkeit des Betroffenen.

Rechtsfolgen und Bedeutung

Das Gericht erkannte dem Sprecher einen Unterlassungsanspruch sowie einen Schadensersatz in Form einer fiktiven Lizenzgebühr zu. Diese wurde mit 2.000 Euro pro Video bewertet — insgesamt also 4.000 Euro –, basierend auf üblichen Sprecherhonoraren für Werbeaufträge. Dieses Urteil stärkt die Stellung von Sprecher/innen und Persönlichkeiten im digitalen Zeitalter: Stimmen, auch in digitaler Form, sind schutzwürdig. Der Einsatz synthetischer Stimmen erfordert die klare Einwilligung der betroffenen Person – allein eine Lizenz vom KI-Anbieter genügt nicht.

HBDI veröffentlicht Open-Source-Tool zur Datenerkennung

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) hat den Quellcode eines neu entwickelten Analysewerkzeugs zur Datenerkennung erstmals auf der Plattform OpenCode.de veröffentlicht. Das Tool wurde im Kontext der Untersuchung von Ransomware-Angriffen entwickelt und ermöglicht das automatisierte Auffinden potenziell personenbezogener Daten in umfangreichen Datenmengen.

Foto: Nimra, Adobe Stock

Im Fall eines Ransomware-Angriffs sind Betroffene oft mit mehreren hundert Gigabyte kompromittierter Daten konfrontiert, die Angreifer zur Veröffentlichung im Darknet nutzen, um Lösegeld zu erpressen. Verantwortliche Stellen, insbesondere solche mit historisch gewachsenen und unzureichend dokumentierten IT-Strukturen, stehen vor der Herausforderung, innerhalb kurzer Zeit präzise einschätzen zu können, ob personenbezogene Daten betroffen sind und welche Meldepflichten nach Art. 33 und 34 DS-GVO bestehen.

Das Analysewerkzeug des HBDI durchsucht Datenbestände automatisch nach typischen Indikatoren für personenbezogene Daten – etwa Rentenversicherungsnummern oder Schlüsselbegriffe wie „Abmahnung“, die auf einen Personenbezug hinweisen können.

Der Code wurde auf OpenCode.de veröffentlicht, einer Plattform, die vom Zentrum für Digitale Souveränität der öffentlichen Verwaltung betrieben wird und dem Bundesministerium des Innern zugeordnet ist. Die Bereitstellung erfolgt unter der Open-Source-Lizenz EUPL 1.2, die eine rechtlich unbedenkliche Nutzung und Anpassung, auch durch andere Behörden oder private Akteure, erlaubt.

Mit der Veröffentlichung fördert der HBDI nicht nur die digitale Souveränität der Verwaltung, sondern eröffnet auch die Möglichkeit, dass andere Behörden, Unternehmen, IT-Dienstleister oder Forschungseinrichtungen das Werkzeug weiterentwickeln. Zudem lädt der HBDI ausdrücklich zur Rückmeldung und zur Zusammenarbeit ein, um die Lösung kontinuierlich zu verbessern.

Foto: fotomowo, Adobe Stock

Retourenpakete als ernsthaftes Datenschutzrisiko

Die Landesdatenschutzbeauftragte von Sachsen-Anhalt warnt eindringlich vor dem Weiterverkauf sogenannter „Secret Packs“ oder „Mystery Boxen“. So werden Retouren oder unzustellbare Sendungen bezeichnet, die ohne ausreichende Anonymisierung erneut in den Handel gelangen. Dabei bleibt personenbezogenes Material wie Namen, Adressen, Telefonnummern oder Rechnungsdetails häufig sichtbar. Besonders problematisch sind Fälle, in denen die Verbindung zwischen sensiblen Inhalten (z. B. Kleidung, intime Produkte) und den offenliegenden Daten Rückschlüsse auf private Lebensbereiche erlaubt.

Datenschutzrechtliche Bewertung

Nach Art. 5 Abs. 1 lit. b (Zweckbindung) und Art. 32 DS-GVO (Sicherheit der Verarbeitung) ist eine solche Praxis nicht zulässig: Personenbezogene Daten dürfen nur für ursprünglich festgelegte Zwecke verarbeitet werden. Provisorische Maßnahmen wie Überkleben oder Filzen sind unzureichend, da sie häufig reversibel sind. In Situationen, in denen die Daten auch Aufschluss über intime Lebensbereiche geben, können sogar besonders schützenswerte Informationen nach Art. 9 DS-GVO betroffen sein.

Potenzielle Folgen und Verantwortungsketten

Die Veröffentlichung persönlicher Daten in Kombination mit privaten Inhalten birgt erhebliche Risiken – von Bloßstellung bis hin zu Identitätsmissbrauch. Verantwortlich sind nicht nur die Betreiber solcher Verkaufsautomaten, sondern bereits die Versandzentren, die Retouren ohne datenschutzgerechte Verfahren in den Umlauf bringen.

Erforderliche Maßnahmen

Um diesen Risiken zu begegnen, müssten Verantwortliche ihre Prozesse im Umgang mit Retourenpaketen grundlegend anpassen. Dazu gehöre, dass personenbezogene Daten vor dem Weiterverkauf vollständig entfernt werden. Technische Lösungen wie automatisierte Systeme zur Entfernung von Etiketten und zur Kontrolle auf verbleibende Datenreste seien unverzichtbar, um ein hohes Schutzniveau sicherzustellen. Ergänzend sollten die Pflichten zur Datenlöschung vertraglich klar geregelt und im Rahmen von Auftragsverarbeitungsverträgen nach Art. 28 DS-GVO verbindlich festgelegt werden. Schließlich sei auch eine transparente Kommunikation gegenüber den Betroffenen erforderlich, damit nachvollziehbar wird, wie mit zurückgesandten Waren verfahren wird und welche Maßnahmen zum Schutz der Privatsphäre getroffen werden.

Fanpage-Verfahren: Berufung gegen VG-Urteil eingeleitet

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat vor dem Oberverwaltungsgericht Münster Berufung gegen das Urteil des Verwaltungsgerichts Köln vom 17. Juli 2025 im Fall der Facebook-Fanpages eingelegt. Dieses Verfahren zielt darauf ab, die bislang unklare Rechtslage zur Nutzung sozialer Netzwerke durch öffentliche Stellen zu final klären. Die BfDI respektiert das bisherige Urteil, macht aber zugleich deutlich, dass eine eindeutige, rechtssichere Grundlage entweder durch den Gesetzgeber oder durch ein letztinstanzliches Urteil erforderlich ist.

Foto: Coloures-Pic, Adobe Stock

Bis zu einer rechtlichen Klärung bietet die BfDI der Bundesregierung und anderen Bundesbehörden eine intensive Beratung an. Eine neu veröffentlichte Handreichung erläutert die erforderlichen Schritte für eine datenschutzkonforme Nutzung sozialer Medien. Ziel ist es, Behörden weiterhin die digitale Kommunikation mit Bürgerinnen und Bürgern zu ermöglichen, ohne Risiken im Datenschutz einzugehen. Die private Nutzung ist nicht betroffen.

Die am selben Tag (22. August 2025) veröffentlichte Handreichung „Soziale Netzwerke rechtmäßig nutzen – So geht's" richtet sich gezielt an öffentliche Stellen des Bundes. Sie liefert didaktisch strukturierte und barrierearme Empfehlungen zur datenschutzkonformen Gestaltung von Social-Media-Aktivitäten.

Dabei werden sowohl klassische Verwaltungsbehörden als auch Parlamentsorgane, Gerichte, öffentliche Stiftungen und Sozialversicherungen einbezogen. Die Handreichung enthält einen integrierten „Kontaktfinder", der es Nutzenden ermöglicht, schnell die jeweils zuständige Datenschutzaufsichtsbehörde zu identifizieren.

DATA AGENDA
PODCAST

(Quelle: TH Köln/Schmülgen)

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

Folge #75

Ein Daten-Bypass für die Forschung – Innovation durch KI-Reallabore

Prof. Dr.
Tobias Keber

Prof. Dr.
Felix Sahm

Folge #76

Data Act in der Praxis – „Game Changer“ oder „Rohrkrepierer“?

Dr. Axel Freiherr von dem Bussche

DataAgenda Podcast Folge 75: Ein Daten-Bypass für die Forschung – Innovation durch KI-Reallabore

Künstliche Intelligenz ist ein maßgeblicher Treiber der Innnovation. Zugleich geht es um die Absicherung gegen die mit KI verbundenen Risiken. Der europäische Gesetzgeber hat dazu in der KI-Verordnung eine Vorschrift geschaffen, die die Weiterverarbeitung auch sensibler Daten zur Entwicklung, zum Training und zum Testen von KI-Systemen erlaubt. In sogenannten KI-Reallaboren sollen Entwickler von bestimmten KI-Systemen ansonsten geschützte personenbezogene Daten unter vereinfachten Bedingungen verarbeiten. Es handelt sich also um geschützte Räume für Innovation. Für die KI-Forschung und -Entwicklung in Deutschland könnte das ein Durchbruch sein. Im Podcast diskutieren der stellvertretenden Ärztlichen Direktor des Universitätsklinikums Heidelberg, Prof. Dr. Dr. Felix Sahm und LfDI BW Prof. Dr. Tobias Keber über die Möglichkeiten der Diagnostik und Therapie von Hirntumoren mit Hilfe von KI und über Wege, diese Forschung in KI-Reallaboren datenschutzrechtlich zu ermöglichen. Zum Podcast bitte hier klicken.

Data Agenda Podcast Folge 76: Data Act in der Praxis – „Game Changer“ oder „Rohrkrepierer“?

Am 12.9.2025 ist der Data Act in Kraft getreten. Was bezweckt das neue Gesetz, welchen Nutzen bringt es den Anwendern und welchen Mehrwert hat die Wirtschaft von diesem neuen Rechtsrahmen? Werden Datenschätze gehoben und die Wirtschaft angekurbelt? Welche Möglichkeiten haben Nutzer, um an ihre Daten zu gelangen, und müssen Unternehmen diese herausgeben? Können sich Unternehmen dagegen wehren, und wie unterscheiden sich die Rechte und Pflichten im Verhältnis von Bürgern zur Wirtschaft? Und wie stellt sich die Lage für die Unternehmen selbst dar? Das klingt kompliziert – und das ist es auch. Im Podcast mit Dr. Axel Freiherr von dem Bussche, LL.M. (L.S.E.), CIPP/E, Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Partner bei Taylor Wessing, nähern wir uns dem neuen Rechtsrahmen und geben Antworten auf die Frage: Game Changer oder Rohrkrepierer? 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:
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