

# NEWS BOX

DATENSCHUTZ



## INHALTSVERZEICHNIS

- 2 Editorial
- 3 Europaweite Datenschutzprüfung: Umsetzung des Rechts auf Löschung im Fokus
- 4 EuGH: Erhebung von Anrede-Daten nicht zwingend erforderlich
- 5 GDD veröffentlicht Praxishilfe zum Hinweisgeberschutzgesetz
- 6 Häufige Ursachen von Datenpannen: Ein Überblick
- 7 Datenschutz im Onlinehandel: Gastzugang als Standard, aber Ausnahmen sind möglich
- 8 Fallen mündliche Übermittlungen in den Anwendungsbereich der DS-GVO?
- 9 Aufbewahrungsfrist für Arbeitsunfähigkeitsbescheinigung (AU-Bescheinigung)
- 11 Unrechtmäßige Datenabfrage durch Polizeibeamten führt zu 3.500 Euro Bußgeld
- 12 Strafanzeige als technisch-organisatorische Maßnahme nach Hackerangriff
- 13 DataAgendaDatenschutz Podcast
- 14 Impressum

AUSGABE

4/2025



Levent Ferik

## EDITORIAL

Nach Auffassung der Datenschutzkonferenz (DSK) als Gremium der deutschen Datenschutzaufsichtsbehörden sollen Unternehmen im Rahmen von Art. 83 Datenschutz-Grundverordnung (DS-GVO) für Datenschutzverstöße eines jeden Beschäftigten haften, wenn der Mitarbeiter nicht im Exzess (für eigene Zwecke) gehandelt hat. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten ihrer Beschäftigten

- ohne dass eine Kenntnis oder Anweisung der Geschäftsführung
- oder eine Verletzung der Aufsichtspflicht für die Zurechnung

erforderlich ist.

In bestimmten Fällen kann aber auch der Arbeitnehmer unmittelbar Adressat einer aufsichtsbehördlichen (Sanktions-)Maßnahme sein. Dafür muss der Beschäftigte „Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO zu qualifizieren sein. Die DSK hat in ihrer Entscheidung vom 3. April 2019 („Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!“) betont, dass sogenannte „Exzesse“ der Beschäftigten,

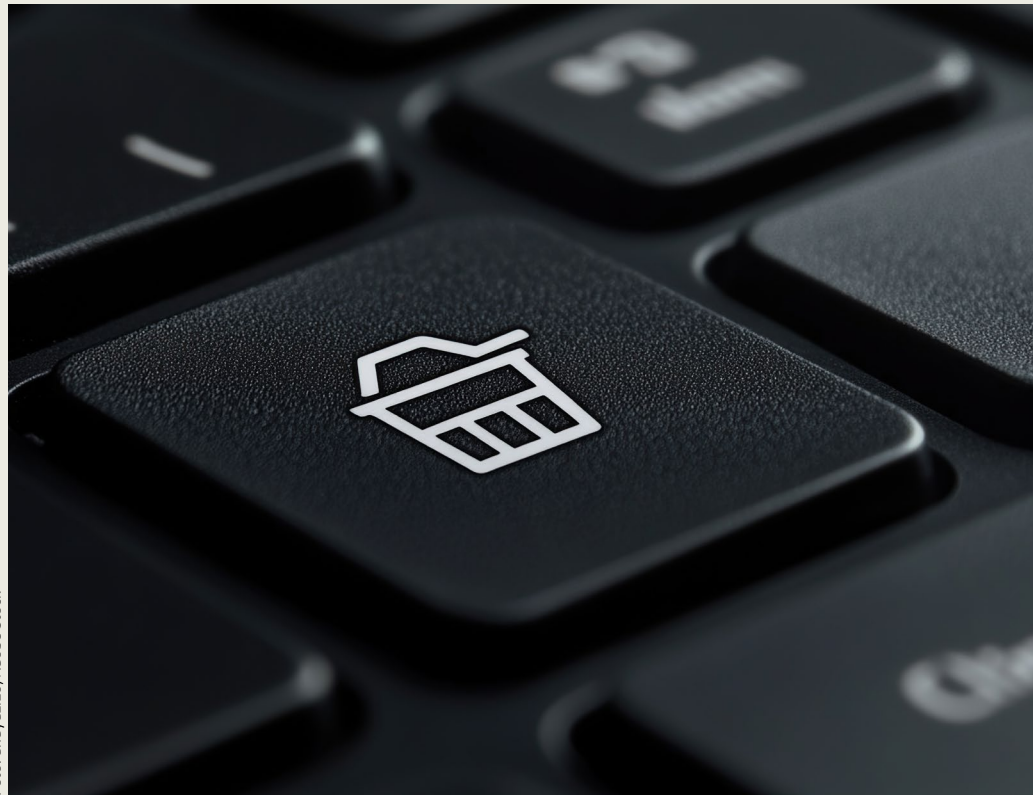
die bei verständiger Würdigung nicht der unternehmerischen Tätigkeit zugeordnet werden können, nicht von der Haftung des Unternehmens erfasst sind.

Schaut man sich die Tätigkeitsberichte der Aufsichtsbehörden an, so verstetigt sich der Eindruck, dass Mitarbeiterexzesse durch unzulässige Datenbankabrufe insbesondere bei der Polizei recht häufig vorkommen. Allein im Berichtsjahr 2023 hat die Berliner Aufsichtsbehörde nach eigenen Angaben 35 Verfahren gegen Polizeibeamt:innen eingeleitet und zum Zeitpunkt der Veröffentlichung des Tätigkeitsberichts bereits insgesamt 32 Bußgelder verhängt. Dass es sich bei dieser Art von Verstoß um einen „Klassiker“ zu handeln scheint, zeigt auch ein entsprechender Fall in dieser Ausgabe der Datenschutz Newsbox.

Ihr  
Levent Ferik



**Sagen Sie uns Ihre Meinung**  
**[kundenservice@datakontext.com](mailto:kundenservice@datakontext.com)**



# Europaweite Datenschutzprüfung: Umsetzung des Rechts auf Löschung im Fokus

Der Europäische Datenschutzausschuss (EDSA) hat seine koordinierte Durchsetzungsmaßnahme für das Jahr 2025 [gestartet](#).

Im Rahmen des „Coordinated Enforcement Framework (CEF)“ wird in diesem Jahr die Umsetzung des Rechts auf Löschung nach Art. 17 DS-GVO untersucht. Deutschland beteiligt sich mit mehreren Landesdatenschutzbehörden an dieser Initiative, die insgesamt 32 europäische Datenschutzaufsichtsbehörden umfasst.

## Ziel und Methodik der Untersuchung

- Schwerpunkt: Analyse der praktischen Umsetzung des Rechts auf Löschung („Recht auf Vergessenwerden“)
- Grundlage: einheitlicher, europaweit abgestimmter Fragebogen
- Zielsetzung: Bewertung der Verfahren zur Löschung personenbezogener Daten, Identifikation bewährter Praktiken und Ermittlung von Optimierungspotenzial

[Weiter auf DataAgenda lesen](#) [↗](#)

## So entwickeln Sie ein rechtskonformes Löschkonzept

- ✓ Leitfaden
- ✓ Checkliste
- ✓ Musterentwurf
- ✓ Vorlagen
- ✓ Ausfüllhinweise



Jetzt bestellen: [datakontext.com](https://datakontext.com)

 DATAKONTEXT

nommen. **“EuGH”** – I. Begriff v  
 ter dem Europäischen Gericht

# EuGH: Erhebung von Anrede-Daten nicht zwingend erforderlich

Der Europäische Gerichtshof (EuGH) [↗](#) hat entschieden, dass die Erhebung von Anrede-Daten („Herr“ oder „Frau“) durch Unternehmen im Rahmen der geschäftlichen Kommunikation nicht zwingend erforderlich ist.

**D**ies gilt auch dann, wenn die Angabe zur Personalisierung der Kundenansprache dient. Die Praxis kann gegen den Grundsatz der Datenminimierung gemäß DS-GVO verstoßen (EuGH, Urteil vom 9. Januar 2025, C-394/23 [↗](#)).

## Hintergrund des Falls

Das französische Eisenbahnunternehmen SNCF Connect fordert beim Online-Ticketkauf die Angabe einer Anrede. Ein Verband kritisierte dies

als Verstoß gegen die DS-GVO, insbesondere gegen den Grundsatz der Datenminimierung, da die Anrede keinen Bezug zur eigentlichen Vertragserfüllung habe. Die französische Datenschutzbehörde CNIL wies die Beschwerde zurück und sah in der Praxis keinen DS-GVO-Verstoß. Der Fall wurde daraufhin dem EuGH vorgelegt.

Der EuGH stellte klar, dass personenbezogene Daten gemäß Art. 5 Abs. 1 lit. c DS-GVO nur in dem Umfang erhoben und verarbeitet werden dürfen, der für den jeweiligen Zweck erforderlich ist. Eine Datenverarbeitung ist insbesondere dann rechtmäßig, wenn:

- 1. Die Verarbeitung für die Vertragserfüllung unerlässlich ist**, oder
- 2. ein berechtigtes Interesse des Verantwortlichen vorliegt**, das die Grundrechte der betroffenen Personen nicht überwiegt.

## 1. Keine Erforderlichkeit für die Vertragserfüllung

Die Anrede ist nach Auffassung des EuGH nicht objektiv unerlässlich für den Abschluss oder die Durchführung eines Schienenverkehrsvertrags. Die geschäftliche Kommunikation könne auch ohne Anrede erfolgen, beispielsweise durch geschlechtsneutrale Höflichkeitsformeln.

## 2. Kein überwiegendes berechtigtes Interesse

Der EuGH betont, dass Unternehmen ihre berechtigten Interessen klar kommunizieren und deren Notwendigkeit begründen müssen. Eine Datenverarbeitung zur geschäftlichen Personalisierung kann nicht als erforderlich gelten, wenn:

- das berechtigte Interesse den Kunden nicht transparent mitgeteilt wurde;
- die Verarbeitung über das absolut Notwendige hinausgeht;
- die Grundrechte und Grundfreiheiten der Betroffenen überwiegen, insbesondere wenn Diskriminierung aufgrund der Geschlechtsidentität möglich ist.

## Fazit

Unternehmen sollten bei der Erhebung von Anrede-Daten kritisch prüfen, ob diese für ihre Geschäftszwecke wirklich erforderlich sind. Der EuGH macht deutlich, dass geschlechtsneutrale Kommunikationsformen eine datensparsamere und rechtlich sicherere Alternative darstellen können.



Whistleblower

Foto: photoopus, Adobe Stock

# GDD veröffentlicht Praxishilfe zum Hinweisgeberschutz- gesetz

Das am 2. Juli 2023 in Kraft getretene Hinweisgeberschutzgesetz (HinSchG) verpflichtet Unternehmen und öffentliche Stellen seit dem 17. Dezember 2023 zur Umsetzung der darin festgelegten Bestimmungen.


Ziel des Gesetzes ist es, hinweisgebende Personen – sogenannte Whistleblower – vor negativen Konsequenzen wie Kündigungen oder anderen beruflichen Benachteiligungen zu schützen, wenn sie Verstöße oder Missstände melden, die eine Gefahr für die Allgemeinheit darstellen.

## Meldekanäle: Interne und externe Meldestellen

Das HinSchG unterscheidet zwischen zwei Arten von Meldestellen:

- **Interne Meldestellen (§§ 12 ff. HinSchG):** Diese müssen von Unternehmen und Behörden mit mindestens 50 Beschäftigten eingerichtet werden. Alternativ können externe Dienstleister als sogenannte „externalisierte interne Meldestelle“ beauftragt werden (§ 14 Abs. 1 S. 1 HinSchG).
- **Externe Meldestellen (§§ 19 ff. HinSchG):** Diese werden von staatlicher Seite eingerichtet. Die zentrale Anlaufstelle auf Bundesebene ist beim **Bundesamt für Justiz** angesiedelt (§ 19 Abs. 1 HinSchG).

Das Gesetz gewährt Hinweisgebern das Recht, frei zu entscheiden, ob sie sich zunächst an eine interne Meldestelle innerhalb des Unternehmens oder der Behörde wenden oder direkt eine externe Meldestelle in Anspruch nehmen.

Die GDD-Praxishilfe bietet eine praxisnahe Orientierungshilfe zur Umsetzung des Hinweisgeberschutzgesetzes  mit besonderem Fokus auf die **datenschutzrechtlichen Anforderungen**. Sie behandelt unter anderem:

- den Umgang mit personenbezogenen Daten von Hinweisgebern und betroffenen Personen,
- die sichere Gestaltung von Meldekanälen,
- den Schutz der Identität der hinweisgebenden Personen,
- Konfliktpotenziale zwischen Datenschutz und Hinweisgeberschutz,
- die Frage der Vereinbarkeit der Rolle eines Datenschutzbeauftragten mit der gleichzeitigen Tätigkeit als interne Meldestelle.



# Häufige Ursachen von Datenpannen: Ein Überblick

**V**erantwortliche Stellen sind verpflichtet, Datenschutzverletzungen, die zu unbefugter Offenlegung oder unbefugtem Zugriff auf personenbezogene Daten führen, den Aufsichtsbehörden zu melden (Art. 33 DS-GVO). Die Berliner Beauftragte für Datenschutz und Informationsfreiheit [hat](#) dabei wiederkehrende Muster identifiziert, die zu solchen Datenpannen führen.

## 1. Schulen und Kindertagesstätten

In pädagogischen Einrichtungen werden vielfältige personenbezogene Daten verarbeitet, darunter Stammdaten, Verhaltensbeurteilungen, Unterlagen zur Kindeswohlgefährdung, Entwicklungsbeurteilungen und Fotos der Kinder. Kinder benötigen einen besonderen Schutz ihrer Daten. Dennoch kommt es regelmäßig zu unbefugtem Zugriff auf diese Informationen.

[Weiter auf DataAgenda lesen](#)



## Schützen Sie Hinweisgeber in Ihrem Unternehmen!

### E-Learning-Kurs: Whistleblowing & Hinweisgeberschutzgesetz

Das Hinweisgeberschutzgesetz stellt Unternehmen vor Herausforderungen. Unser interaktiver E-Learning-Kurs vermittelt praxisnah:

- ✓ Rechtskonforme Umsetzung der Vorschriften
- ✓ Schutz von Hinweisgebern & interne Meldekanäle
- ✓ Flexible Schulung - jederzeit & ortsunabhängig
- ✓ Mit Zertifikat zur Dokumentation der Schulung

**Jetzt informieren & Compliance stärken:**  
[elearning-mit-zertifikat.de](https://elearning-mit-zertifikat.de)

# Datenschutz im Onlinehandel: Gastzugang als Standard, aber Ausnahmen sind möglich

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) prüfte Anfang 2025 mehrere Hamburger Onlineshops und stellte fest, dass ein großes Bekleidungsversandhaus ausschließlich Bestellungen über ein dauerhaftes Kundenkonto ermöglichte. Da dies gegen das Datenschutzprinzip der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DS-GVO verstößt, forderte die Behörde die Einführung einer Gastbestelloption. Das Unternehmen setzte die Vorgabe um.



**D**ie Datenschutzkonferenz (DSK) hatte bereits 2022 beschlossen, dass Onlinehändler ihren Kunden eine Bestellung ohne Registrierung ermöglichen müssen. Ein verpflichtendes Kundenkonto ist datenschutzrechtlich nur zulässig, wenn es für den Bestellprozess zwingend erforderlich ist. Dauerhafte Kundenkonten bergen zudem ein höheres Risiko für Datenschutzverletzungen und Hackerangriffe.

In bestimmten Fällen kann jedoch auf den Gastzugang verzichtet werden, wenn dies durch ein berechtigtes Interesse gerechtfertigt ist. So argumentierte die Plattform Otto.de, dass die Abwicklung von Bestellungen und Retouren sowie der Kundenservice ohne Kundenkonto nicht effizient möglich seien. Der HmbBfDI erkannte dies als legitimen Grund an.

Ein Mitbewerber sah darin einen Wettbewerbsverstoß und klagte. Das Oberlandesgericht Hamburg wies die Klage ab und bestätigte, dass die Ausnahme im Fall von Otto.de gerechtfertigt sei.

Grundsätzlich sind Onlinehändler verpflichtet, eine Gastbestellung anzubieten. Abweichungen sind nur in Ausnahmefällen und bei nachvollziehbaren, berechtigten Interessen zulässig.



# Fallen mündliche Übermittlungen in den Anwendungsbereich der DS-GVO?

## Hintergrund des Verfahrens

Das Berufungsgericht für Ost-Finnland hatte dem Europäischen Gerichtshof (EuGH) eine entscheidende Frage zur Auslegung der Datenschutz-Grundverordnung (DS-GVO) vorgelegt (Az. C-740/22 – Urteil vom 07. März 2024 [↗](#)).

Konkret ging es darum, ob eine mündliche Weitergabe personenbezogener Daten – in diesem Fall Informationen zu möglichen Strafverfahren – als Verarbeitung im Sinne der DS-GVO einzustufen ist.

Eine Prozesspartei forderte mündlich Auskunft aus dem Strafregister eines Gerichts über anhängige oder abgeschlossene Verfahren gegen eine natürliche Person. Strittig war, ob dieser Vorgang als Verarbeitung personenbezogener Daten gemäß Art. 2 Abs. 1 und Art. 4 Nr. 2 DS-GVO zu werten ist, insbesondere wenn die Informationen in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

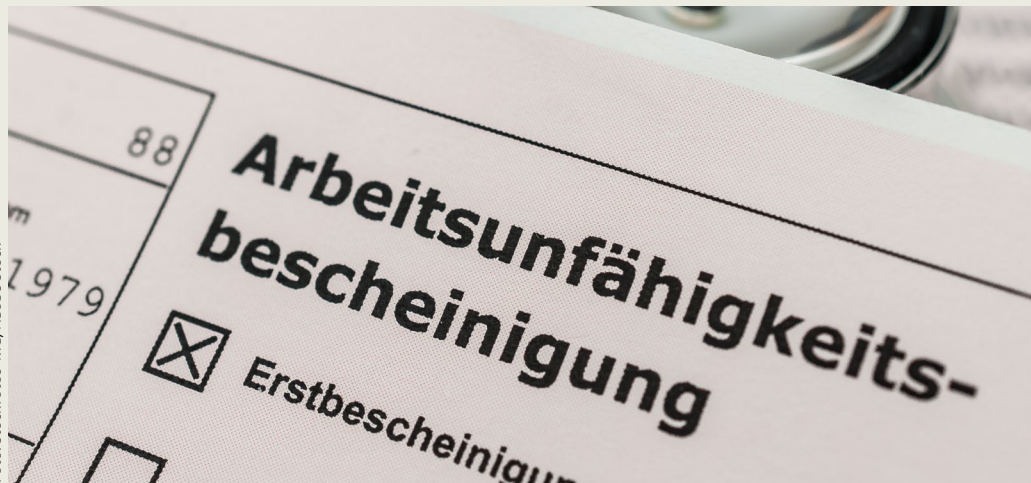
## Kernaussagen des Urteils

- Der EuGH entschied, dass die mündliche Übermittlung personenbezogener Daten als Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO gilt, wenn diese Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.
- Damit fällt auch die mündliche Offenlegung solcher Informationen in den sachlichen Anwendungsbereich der DS-GVO.
- Offen blieb die Frage, ob eine mündliche Übermittlung auch dann unter die DS-GVO fällt, wenn die Daten weder gespeichert noch zur Speicherung vorgesehen sind.

## Auswirkungen auf die Praxis

Diese Entscheidung hat weitreichende Implikationen für den Umgang mit personenbezogenen Daten, auch für betriebliche Szenarien, im Rahmen derer personenbezogene Daten „nur“ mündlich weitergegeben werden. Datenschutzbeauftragte sollten prüfen, ob bestehende Prozesse zur mündlichen Weitergabe von gespeicherten Informationen DS-GVO-konform gestaltet sind.

Vergleichbare Regelungen existieren bereits im deutschen Recht: Das Bundesdatenschutzgesetz (§ 26 Abs. 7 BDSG [↗](#)) und das Kirchliche Datenschutzgesetz (§ 53 Abs. 3 KDG [↗](#)) definieren ausdrücklich, dass auch mündliche Übermittlungen unter den Beschäftigtendatenschutz fallen. Die EuGH-Entscheidung stärkt damit eine strenge Auslegung der DS-GVO und unterstreicht die Bedeutung einer differenzierten Betrachtung mündlicher Datenweitergaben.



# Aufbewahrungsfrist für Arbeitsunfähigkeitsbescheinigung (AU-Bescheinigung)

Gesundheitsdaten gehören gemäß Art. 9 DS-GVO [↗](#) zu den Daten besonderer Kategorien. Ihre Verarbeitung ist nur unter bestimmten Bedingungen zulässig.

Im Rahmen eines Beschäftigungsverhältnisses erfolgt die Erfassung von Arbeitsunfähigkeitsdaten in erster Linie zur Ausübung von Rechten und Pflichten, die sich aus einer Erkrankung oder Schwerbehinderung ergeben – sei es zur Lohnfortzahlung, zur Geltendmachung arbeitsrechtlicher Ansprüche oder im Rahmen des betrieblichen Eingliederungsmanagements (BEM).

Mit der Einführung der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) seit Anfang 2023 ist zudem ein grundlegender Wandel eingetreten: Die bisher üblichen „gelben Scheine“ wurden weitgehend durch die eAU ersetzt, sodass Arbeitgeber künftig elektronische Übermittlungswege nutzen. Dies erfordert nicht nur den Umstieg auf digitale Archivierungslösungen, sondern auch den Einsatz technischer und organisatorischer Maßnahmen zur Sicherstellung des Datenschutzes und der Integrität der Gesundheitsdaten.

Die Erfassung und Verarbeitung der AU-Daten obliegt ausschließlich der Personalverwaltung. Nur diese darf die sensiblen Gesundheitsdaten speichern und auswerten – und dies ausschließlich zu den gesetzlich vorgesehenen Zwecken, etwa zur Berechnung der Lohnfortzahlung oder zur Initiierung eines BEM.

In der Praxis besteht häufig Unklarheit darüber, wie lange Arbeitsunfähigkeitsbescheinigungen aufbewahrt werden dürfen. Dabei sind speziell folgende Punkte zu beachten:

## 1. Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO):

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die jeweiligen Verarbeitungszwecke erforderlich ist. Sobald der Zweck entfällt, muss auch die Speicherung beendet werden – sofern keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

## 2. Gesetzliche Ausnahmen:

Gesetzliche Vorschriften und gerichtliche Entscheidungen können längere Aufbewahrungsfristen vorsehen. So hat das Bundesarbeitsgericht in seinem Urteil vom 25. April 2018 (Az. 2 AZR 6/18) [↗](#) entschieden, dass bei einer Kündigung wegen häufiger Kurzerkrankungen ein Referenzzeitraum von drei Jahren maßgeblich ist – insbesondere, wenn es um die Erstellung einer Gesundheitsprognose geht. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI [↗](#)) hält in seinem Tätigkeitsbericht (2020, Ziffer 4.25) ebenfalls eine Speicherdauer von drei Jahren als angemessen.

# Beschäftigtendatenschutz rechtssicher umsetzen

Der unverzichtbare Kommentar  
für Ihren Arbeitsalltag.

- Neuer Co-Autor Prof. Dr. Gregor Thüsing, Direktor des Instituts für Arbeitsrecht an der Universität Bonn, Mitglied des Deutschen Ethikrats, führender Experte für Arbeits- und Sozialrecht
- Unterstützung für Unternehmen bei der Einhaltung gesetzlicher Vorgaben und Minimierung von Datenschutzrisiken
- Perfekt für Datenschutz- und Personalverantwortliche in Unternehmen, Rechtsanwälte sowie Berater

Handbuch Beschäftigtendatenschutz  
Aktuelle Rechtsfragen und Umsetzungshilfen  
Prof. Peter Gola, Prof. Dr. Gregor Thüsing  
9. komplett neu bearbeitete Auflage 2025  
ISBN 978-3-89577-888-9  
848 Seiten; 17 x 24 cm Hardcover  
169,99 € inkl. MwSt. mit E-Book zum Download (PDF)

9. komplett  
neu  
bearbeitete  
Auflage!



Jetzt bestellen: [www.datakontext.com/handbuch](http://www.datakontext.com/handbuch)



# Unrechtmäßige Datenabfrage durch Polizeibeamten führt zu 3.500 Euro Bußgeld

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg verhängte ein Bußgeld von 3.500 Euro [↗](#) gegen einen Polizeibeamten, der ohne dienstlichen Anlass eine Abfrage im Melderegister durchführte.

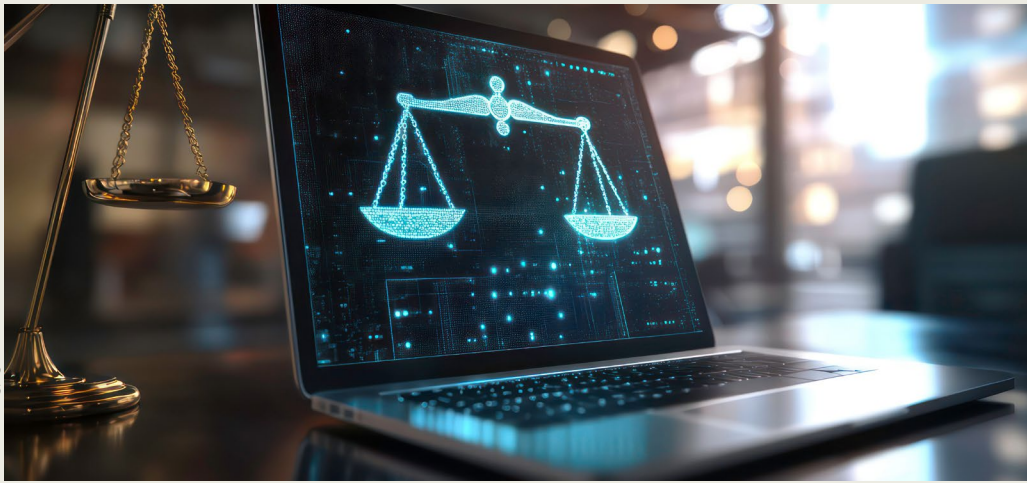
**D**er Beamte hatte zuvor eine Frau bei einer Verkehrskontrolle angetroffen und nutzte anschließend das Melderegister, um ihr dort hinterlegtes Lichtbild einzusehen. Dies geschah im Rahmen einer persönlichen Bewertungsskala, bei der er Frauen anhand subjektiver Kriterien einstuft und ab einem bestimmten Wert deren Fotos abrief.

Diese Handlung verstößt gegen Art. 6 Abs. 1 sowie Art. 5 Abs. 1 DS-GVO und ist gemäß Art. 83 Abs. 5 lit. a DS-GVO bußgeldbewehrt. Bei der Bemessung der Bußgeldhöhe wurden alle tatbezogenen Umstände berücksichtigt. Erschwerend wirkten sich die herabwürdigende Objektivierung der Betroffenen und das systematische Vorgehen des Beamten aus.

Polizeibeamte haben Zugang zu sensiblen Daten der Bürgerinnen und Bürger und genießen ein hohes Vertrauen in der Bevölkerung. Daher ist ein verantwortungsvoller Umgang mit diesen Daten essenziell. Bei missbräuchlicher Nutzung dienstlicher Datenbanken zu privaten Zwecken schreitet der Landesbeauftragte konsequent ein. Im vorliegenden Fall zeigte sich die Polizei kooperativ und hatte ein eigenes Interesse an der Aufklärung des Sachverhalts.

Im Jahr 2024 wurden dem Landesbeauftragten zwölf Fälle von rechtswidriger Nutzung dienstlicher Datenbanken durch Polizeibeschäftigte gemeldet. Insgesamt wurden Bußgelder in Höhe von 14.550 Euro verhängt. Diese Sanktionen sollen als wirksame und abschreckende Maßnahmen gemäß Art. 3 Abs. 1 DS-GVO dienen.

Der vorliegende Fall wurde dem Landesbeauftragten 2024 bekannt. Im Januar 2025 erließ er das Bußgeld, wodurch das Verfahren rechtskräftig abgeschlossen wurde. Solche Vorfälle werden entweder durch Anzeigen betroffener Personen oder durch interne Mitteilungen der Polizei, beispielsweise im Rahmen von Stichprobenkontrollen oder Disziplinarverfahren, bekannt.



# Strafanzeige als technisch-organisatorische Maßnahme nach Hackerangriff

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfd) hat in seiner Aktuellen Kurz-Information 57 (AKI 57) [☞](#) darauf hingewiesen, dass Verantwortliche bei Datenpannen, insbesondere nach Hackerangriffen, nicht nur die Meldepflichten gemäß der DS-GVO, sondern auch weitere Mitteilungspflichten außerhalb der DS-GVO berücksichtigen sollten.

**E**ine Strafanzeige kann dabei als sinnvolle technisch-organisatorische Maßnahme angesehen werden. Öffentliche Stellen sind nach Art. 33 DS-GVO verpflichtet, Datensicherheitsverletzungen, die ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellen, unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls der zuständigen Datenschutzaufsichtsbehörde zu melden. Diese Meldepflicht dient der Transparenz und der Sicherstellung geeigneter Schutzmaßnahmen für die betroffenen Personen. Neben der DS-GVO können weitere gesetzliche Mitteilungspflichten relevant sein:

- **Sozialleistungsträger:** Diese müssen nach § 83a Zehntes Buch Sozialgesetzbuch (SGB X) Verletzungen des Schutzes von Sozialdaten auch der zuständigen Rechts- oder Fachaufsichtsbehörde melden.
- **Betreiber kritischer Infrastrukturen:** Gemäß § 8b Abs. 4 BSI-Gesetz (BSIG) und § 11 Abs. 1c Energiewirtschaftsgesetz (EnWG) besteht eine Meldepflicht an das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei bestimmten Störungen.

Obwohl keine allgemeine gesetzliche Verpflichtung besteht, nach Art. 33 DS-GVO meldepflichtige Vorfälle auch den Strafverfolgungsbehörden mitzuteilen, kann eine Strafanzeige im Fall eines Hackerangriffs als sinnvolle technisch-organisatorische Maßnahme des Verantwortlichen betrachtet werden. Dies kann dazu beitragen, weitere Schäden zu verhindern und die Sicherheit der Datenverarbeitung zu gewährleisten.

## Fazit

Verantwortliche sollten bei einer Datenpanne nicht nur die Meldepflichten gemäß DS-GVO beachten, sondern auch weitere gesetzliche Mitteilungspflichten berücksichtigen. Eine Strafanzeige kann dabei als sinnvolle Maßnahme dienen, um die Sicherheit der Datenverarbeitung zu erhöhen und weiteren Schaden abzuwenden.



# DATA AGENDA PODCAST



(Foto: TH Köln/Schmülgen)

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

Folge #**68**

Begleitmusik des Datenrechts -  
Die Entwürfe zur Durchführung  
von Data Act und KI-VO

Kristin Benedikt



## Data Agenda Podcast Folge 68: Begleitmusik des Datenrechts - die Entwürfe zur Durchführung von Data Act und KI-VO

Die Entbürokratisierung des Datenschutzes steht kurz vor der Bundestagswahl 2025 oben auf der politischen Agenda. Anfang 2025 wurden zwei Referentenentwürfe zum Datenrecht vorgelegt. Erfüllen der „Entwurf des Gesetzes zur Umsetzung der KI-Verordnung“ und der Entwurf des „Data Act-Durchführungsgesetzes“ dieses Ziel oder schaffen sie gar zusätzliche Bürokratie? Soll sich die neue Bundesregierung mit einem nationalen „Datengesetz“ befassen? Was kann ein Digitalministerium zur Entbürokratisierung beitragen? Mit diesen Fragen befasst sich Kristin Benedikt, Richterin am Verwaltungsgericht Regensburg, im DataAgenda Podcast Nr. 68.

Zum Podcast bitte [hier](#) klicken.

Weitere Folgen unter [DataAgenda.de/podcast](https://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](http://www.datakontext.com/newsletter)



## KI-Datenschutz im Konzern – Use Cases, Prozesse und Umsetzungshilfen

6. Mai 2025 | Online | 10:00 Uhr – 13:15 Uhr  
Referent: Prof. Dr. Thorsten Behling

### Schwerpunktt Themen:

- ✓ Unterscheidung zwischen KI-Modell und KI-System
- ✓ Einführung in typische Use Cases für die Bereiche HR, Marketing und Konzern- und Unternehmenssteuerung
- ✓ Datenschutzrechtliche Umsetzungsbegleitung im Konzern
- ✓ Vorstellung von Prozess- und Umsetzungsbeispielen

Jetzt anmelden: [www.datakontext.com](http://www.datakontext.com)