NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
1/2025

Levent Ferik

Klassiker: Mitarbeiterexzess durch unzulässige Datenbankabfragen

In bestimmten Fällen können auch Beschäftigte unmittelbar Adressat einer aufsichtsbehördlichen (Sanktions-)Maßnahme sein. Dafür muss der Beschäftigte als „Verantwortlicher" im Sinne des Art. 4 Nr. 7 DS-GVO zu qualifizieren sein.
Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 03.04.2019 („Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!") betont, dass sogenannte „Exzesse" von Beschäftigten, die bei verständiger Würdigung nicht der unternehmerischen Tätigkeit zugeordnet werden können, nicht von der Haftung des Unternehmens erfasst werden.

Unzulässige Datenbankabfragen durch die Polizei:

Schaut man sich die Tätigkeitsberichte der Aufsichtsbehörde an, so verfestigt sich der Eindruck, dass Mitarbeiterexzesse durch unzulässige Datenbankabfragen 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, u. a. in den folgenden Fällen:

- Eine Polizeibeamtin fragte aus privatem Interesse Daten über ihren Ex-Mann ab.
- Ein Polizeibeamter schrieb über sein privates Mobiltelefon, dessen Nummer er im Rahmen eines Polizeieinsatzes dienstlich erhalten hatte, eine Bürgerin an, um mit ihr zu flirten.
- Ein Polizeibeamter fragte als Geschädigter eines mutmaßlichen Wohnungseinbruchs aus privatem Interesse den dazugehörigen Ermittlungsvorgang ab.
- Ein Polizeibeamter fragte Daten eines seiner Dienstgruppe neu zugewiesenen Kollegens ab, um auszuschließen, dass er mit diesem nicht bereits polizeilich zu tun hatte.
- Ein Polizeibeamter schrieb eine Bürgerin, die er zuvor auf dem Parkplatz eines Lebensmittelhändlers gesehen hatte, über ihre private Handynummer an, die er mithilfe ihres Kfz-Kennzeichens der Datenbank entnahm.

Alle diese Datenverarbeitungen waren rechtswidrig, da die Abfragen in der POLIKS-Datenbank nicht zur Erfüllung der gesetzlichen Aufgaben der Strafverfolgung und Gefahrenabwehr erfolgten. Es ist dabei unerheblich, welche Beweggründe den nicht dienstlichen Datenabfragen und Datennutzungen zugrunde lagen.
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: InwAI, Adobe Stock

Aktualisierung: Mindeststandard für die Protokollierung und Detektion von Cyberangriffen

Immer häufiger werden Cyberangriffe auf Unternehmen und Regierungen bekannt, die für die Betroffenen schwerwiegende Folgen haben.

Die meisten IT-Systeme in Organisationen verfügen über die Möglichkeit, ein Audit-Logging zu aktivieren. Bereits mit den Standardeinstellungen werden dabei in der Regel alle wichtigen Ereignisse aufgezeichnet. Damit dabei aber keine gigantischen Datenmengen entstehen, die nur mit hohem Aufwand verarbeitet und gespeichert werden können, werden normalerweise nicht alle Ereignisse in maximaler Detailtiefe protokolliert. Daher ist es nicht ausgeschlossen, dass nach einem Cyberangriff Protokolldateien, die zur Analyse des Angriffs benötigt werden, nicht oder nicht mehr verfügbar sind.
Auch vor diesem Hintergrund hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun den Mindeststandard zur Protokollierung und Detektion von Cyberangriffen (Version 2.1) aktualisiert. Der Standard, der zuletzt im Juni 2023 grundlegend überarbeitet wurde, definiert gemäß § 8 Abs. 1 BSI-Gesetz (BSIG) die Mindestanforderungen an die Informationssicherheit des Bundes. Ziel ist es, ein einheitliches und effektives Vorgehen zur Erkennung und Abwehr von Cyberangriffen auf die IT-Infrastruktur des Bundes sicherzustellen.

Wesentliche Neuerungen

Die aktualisierte Version enthält präzisierte Vorgaben zur Speicherdauer von Protokoll- und Protokollierungsdaten sowie differenzierte Anforderungen an deren Löschung. Außerdem wurden die Referenztabelle und die Verweise überarbeitet, um eine bessere Orientierung und Anwendbarkeit zu gewährleisten.

Bedeutung des Standards

Die Protokollierung von Ereignissen und die frühzeitige Detektion von sicherheitsrelevanten Ereignissen (Security Related Events, SRE) sind essenziell, um Cyberangriffe frühzeitig zu erkennen und deren Folgen abzumildern. Mit diesem Mindeststandard wird eine einheitliche Grundlage für den Schutz der Kommunikationstechnik des Bundes geschaffen.

Weitere Informationen

Die vollständige Dokumentation und eine Übersicht der Änderungen sind auf der Webseite des BSI verfügbar. Die neue Version unterstützt Bundesbehörden und Institutionen dabei, ihre Informationssicherheit nachhaltig zu verbessern und Cyberrisiken gezielt zu begegnen.

Foto: Bussarin, Adobe Stock

Löschpflicht nicht beachtet: 900.000 Euro Bußgeld

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat gegen ein Hamburger Unternehmen aus der Forderungsmanagement-Branche ein Bußgeld in Höhe von 900.000 Euro verhängt.
Das Unternehmen hatte personenbezogene Daten trotz abgelaufener Löschfristen bis zu fünf Jahre lang ohne Rechtsgrundlage gespeichert und damit gegen die Datenschutz-Grundverordnung (DS-GVO) verstoßen. Der Bußgeldbescheid ist rechtskräftig, das Unternehmen hat den Verstoß eingeräumt und das Bußgeld akzeptiert.

Weiter auf DataAgenda lesen

Foto: ImageFlow, Adobe Stock

Risiko- und Folgenabschätzung von KI-Systemen

2021 wurde der Ausschuss für künstliche Intelligenz (Committee on Artificial Intelligence, CAI) damit beauftragt, einen rechtsverbindlichen Vertrag zu KI auf Basis der Europarats-Standards zu entwickeln.

Nach Verhandlungen mit 46 Mitgliedstaaten, der EU und 11 Nichtmitgliedstaaten verabschiedete der Europarat am 17. Mai 2024 das Rahmenübereinkommen über KI, Menschenrechte, Demokratie und Rechtsstaatlichkeit.

Dieses technologieneutrale Abkommen regelt den gesamten Lebenszyklus von KI-Systemen, fördert Innovationen und adressiert Risiken für Grundwerte. Ergänzend wurde HUDERIA (Human Rights, Democracy, and the Rule of Law Impact Assessment for AI Systems), ein Instrument zur Durchführung von Folgenabschätzungen bei der Anwendung von Systemen der künstlichen Intelligenz, welches technische und soziotechnische Aspekte berücksichtigt.

Der Europarat hat ein aktuelles Papier (Stand 28.11.2024) zu dieser Methode veröffentlicht.

In diesem Dokument wird die HUDERIA-Methode beschrieben, eine vom Europarat entwickelte, nicht rechtsverbindliche Anleitung zur Risiko- und Folgenabschätzung von KI-Systemen zum Schutz und zur Förderung von Menschenrechten, Demokratie und Rechtsstaatlichkeit. Sie bietet einen strukturierten Ansatz mit vier Elementen: Kontextbezogene Risikoanalyse (Context-Based Risk Analysis, COBRA), Prozess der Stakeholder-Einbindung (Stakeholder Engagement Process, SEP), Risiko- und Folgenabschätzung (Risk and Impact Assessment, RIA) und Maßnahmenplan (Mitigation Plan, MP).

Die Methode verfolgt einen soziotechnischen Ansatz und betont Iterationen zur kontinuierlichen Überprüfung und Anpassung der Maßnahmen im gesamten Lebenszyklus des KI-Systems. Ziel ist die Förderung verantwortungsvoller KI-Entwicklung und -Anwendung, die die genannten Werte schützt. Die Anleitung beinhaltet detaillierte Fragen und Hinweise zur Umsetzung der einzelnen Schritte.

Foto: tomfallen, Adobe Stock

Mitwirkungspflichten Betroffener bei der Feststellung ihrer Identität

An die Ausübung von Betroffenenrechten kann eine Mitwirkungspflicht geknüpft sein, wenn begründete Zweifel an der Identität der antragstellenden Person bestehen. In diesen Fällen kann die Anforderung eines Identitätsnachweises gerechtfertigt sein.

Die Verantwortlichen müssen die Zweifel darlegen. Auch müssen die Grundsätze des Art. 5 Datenschutz-Grundverordnung (DS-GVO) beachtet und eine nicht notwendige Neuerhebung von Daten vermieden werden.
Eine allgemeine Identifizierungspflicht bei der Ausübung von Betroffenenrechten besteht nicht. Vielmehr ist in jedem Einzelfall zu prüfen, ob die Identität ohne weiteren Nachweis feststellbar ist, um den Anforderungen des Art. 12 Abs. 2 DS-GVO zu genügen und die Ausübung der Rechte so einfach wie möglich zu machen, so das Verwaltungsgericht Berlin (Beschluss vom 24. April 2023, 1 K 227/22).

Weiter auf DataAgenda lesen

Foto: Thares2020, Adobe Stock

Datenschutz-Fallstricke beim Asset Deal

Ein Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. September 2024 befasst sich mit der Übermittlung personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset Deals.

Bei der Veräußerung eines Unternehmens stehen zwei Methoden zur Verfügung, die unterschiedliche Auswirkungen auf den Umgang mit personenbezogenen Daten haben: der **Share Deal** und der **Asset Deal**. Während der Share Deal aus datenschutzrechtlicher Sicht meist unkompliziert ist, erfordert der Asset Deal eine differenzierte Betrachtung.

Weiter auf DataAgenda lesen

BSI: Cyberkriminelle Schattenwirtschaft professionalisiert sich weiter

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes. Seine Aufgabe ist es, Deutschland digital sicher zu machen.

Wie jedes Jahr legt das BSI mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland einen umfassenden und fundierten Überblick über die Bedrohungen Deutschlands, seiner Bürger:innen und seiner Wirtschaft im Cyberraum vor.

Die IT-Sicherheitslage in Deutschland bleibt weiter angespannt und geprägt von zunehmend ausgefeilten und vielfältigen Bedrohungen im Cyberraum. Der aktuelle Bericht beleuchtet zentrale Entwicklungen und Herausforderungen:

Weiter auf DataAgenda lesen

Foto: Who is Danny, Adobe Stock

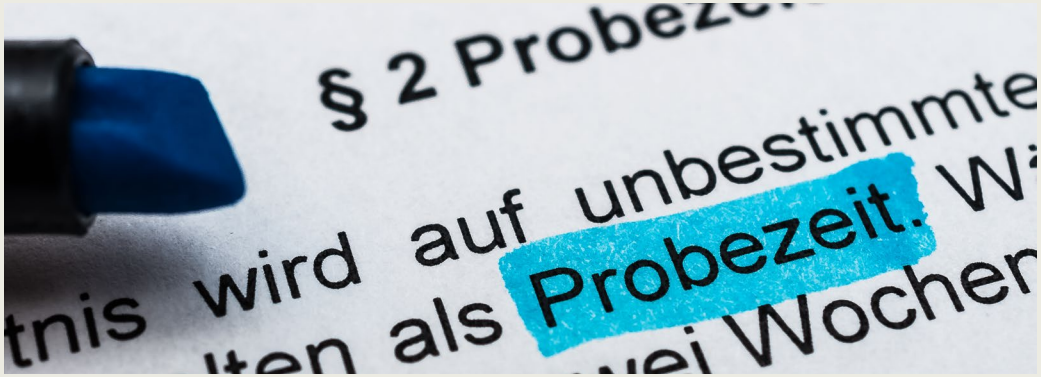


Foto: Stockfotos-MG, Adobe Stock

Beschäftigtendaten: Bußgeld wegen unzulässiger Datensammlung in der Probezeit

Hintergrund

Ein Unternehmen wurde von der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) mit einem Bußgeld von 215.000 Euro belegt, weil es sensible personenbezogene Daten seiner Beschäftigten während der Probezeit unrechtmäßig verarbeitet hatte. Die Daten wurden ohne Kenntnis der Betroffenen erfasst und für Kündigungsentscheidungen genutzt (S. 25, Jahresbericht 2023).

Details des Falls

Eine Vorgesetzte erstellte auf Anweisung der Geschäftsführung eine Liste mit Stammdaten, Leistungsbeurteilungen und Empfehlungen für mögliche Kündigungen. In einer weiteren Spalte der Liste befanden sich jedoch hochsensible Informationen, darunter persönliche Ansichten der Mitarbeitenden, Angaben zu psychischen Behandlungen und Interessen an einer Betriebsratsgründung. Diese Daten, die größtenteils im Zusammenhang mit der Dienstplanung übermittelt worden waren, wurden an die Geschäftsführung weitergegeben.

Weiter auf DataAgenda lesen

ICO untersucht KI-gestütztes Recruiting

Die britische Datenschutzbehörde ICO hat am 6. November 2024 Empfehlungen für Entwickler und Anbieter von KI-gestützten Recruiting-Tools veröffentlicht, um die Persönlichkeitsrechte von Bewerbern besser zu schützen.

KI wird zunehmend zur Effizienzsteigerung im Bewerbungsprozess eingesetzt, birgt aber Risiken wie Diskriminierung und Datenschutzverletzungen, wenn sie nicht rechtmäßig eingesetzt wird.
Nach erfolgten Audits von Entwicklern und Anbietern stellte die ICO fast 300 Empfehlungen aus, darunter die faire Verarbeitung personenbezogener Daten, die Minimierung der Datenmenge und die transparente Information der Bewerber.

Weiter auf DataAgenda lesen


Foto: Antto-AI, Adobe Stock

Foto: Introvertia, Adobe Stock

BAG: Mitbestimmungspflicht bei der Einführung eines Headset-Systems

Das Bundesarbeitsgericht (BAG) hat mit Beschluss vom 16.07.2024 (Az. 1 ABR 16/23) klargestellt, dass die Einführung eines Headset-Systems, das die Überwachung von Arbeitnehmern ermöglicht, der Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) unterliegt.

Die Entscheidung betont die weitreichenden Mitbestimmungsrechte des Gesamtbetriebsrats, insbesondere bei zentral verwalteten technischen Einrichtungen.

Sachverhalt

Ein Bekleidungseinzelhändler führte in einer Filiale mit über 200 Beschäftigten ein Headset-System zur internen Kommunikation ein. Das System ermöglichte die drahtlose Live-Kommunikation, ohne Gespräche oder Daten aufzuzeichnen. Dennoch konnten Vorgesetzte Gespräche mithören und Beschäftigte anhand ihrer Stimme oder ihrer Dienstpläne identifizieren. Die zentrale IT-Abteilung der Konzernmutter verwaltete das System über das „V-Portal“ in Dublin. Der lokale Betriebsrat der Filiale sah hierin eine mitbestimmungspflichtige technische Einrichtung, während die Arbeitgeberin sich auf eine Gesamtbetriebsvereinbarung berief und eine Überwachungsfunktion verneinte.

Weiter auf DataAgenda lesen

Foto: xyz+, Adobe Stock

Kontrollpflicht und Haftung bei Auftragsverarbeitern

Das Oberlandesgericht Dresden hat am 15. Oktober 2024 (4 U 422/24 / Oberlandesgericht Dresden / 15.10.2024) entschieden, dass Verantwortliche nach Beendigung eines Verarbeitungsvertrags eine Kontrollpflicht zur Löschung personenbezogener Daten haben.

Ein Verantwortlicher kann sich bei Nichteinhaltung dieser Pflicht nicht auf einen „Exzess" des Auftragsverarbeiters berufen.

Kernpunkte des Urteils

- **Kontrollpflicht nach Vertragsende**: Verantwortliche müssen sicherstellen, dass der Auftragsverarbeiter personenbezogene Daten nach Beendigung des Vertrags löscht und dies bestätigen lässt.
- **Haftungsumfang**: Verantwortliche bleiben haftbar, wenn sie die Einhaltung von Löschfristen und Sicherheitsmaßnahmen beim Auftragsverarbeiter nicht ausreichend überwachen.
- **Immaterieller Schaden durch Spam**: Der Empfang von Spam-Nachrichten allein begründet keinen immateriellen Schadenersatzanspruch nach Art. 82 DS-GVO.

Hintergrund des Falls

Ein Datenleck beim Auftragsverarbeiter eines Musikstreaming-Dienstes führte zur Offenlegung von Kundendaten. Der Kläger machte Schadensersatz geltend, da die Sicherheits- und Kontrollpflichten durch den Verantwortlichen angeblich verletzt wurden.

Praxisrelevanz

Datenschutzbeauftragte und Verantwortliche sollten sicherstellen, dass:

- Löschungsnachweise nach Beendigung von Verarbeitungsverträgen eingefordert und dokumentiert werden,
- regelmäßige Überprüfungen und klare Sicherheitsanforderungen im Vertragsverhältnis festgelegt sind,
- Ansprüche auf Schadensersatz bei Datenschutzverletzungen sorgfältig dokumentiert und begründet werden.

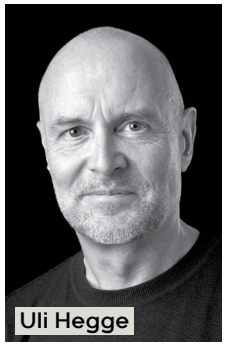
DATA AGENDA PODCAST

(Quelle: TH Köln/Schmülgen)

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

Folge #**63**

Datenschutz in der Onlinewirtschaft – Datennutzungsrecht und Einwilligungsverwaltung



Folge #**64**

Datenrecht 2025: Koordinierter Zukunftsoptimismus

Data Agenda Podcast Folge 63: Datenschutz in der Onlinewirtschaft – Datennutzungsrecht und Einwilligungsverwaltung

Dirk Freytag (BVDW und Content Pass) und Uli Hegge (netID) sind gestandene Digitalunternehmer. Sie setzen sich für die Umsetzung eines fairen, effizienten und in der Praxis lebbaren Datenschutz in der Onlinewirtschaft ein. Im Podcast geht es um die Idee eines Datennutzungsrechts und das Verständnis des Datenschutzbeauftragten im Sinne eines Datennutzungsbeauftragten, um Einwilligungsverwaltungsdienste und Single-Sign-on-Angebote sowie um die Notwendigkeit eines Digitalministeriums.
Zum Podcast bitte hier klicken.

Data Agenda Podcast Folge 64: Datenrecht 2025: Koordinierter Zukunftsoptimismus

In dieser Folge werfen wir einen Blick auf das Datenrecht 2025. Außerdem gibt es einen Jahresrück- und Ausblick über die Themen Datenwirtschaft, Datenschutz, Künstliche Intelligenz, Demokratie und Datensicherheit mit Professor Dr. Tobias Keber (LfDI BW) und Axel Voss (MdEP).
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