NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 3/2025

RDV

DATAKONTEXT

Levent Ferik

EDITORIAL

Mehr als 60 deutschsprachige Hochschulen und Forschungseinrichtungen haben beschlossen, ihre Aktivitäten auf der Plattform X (ehemals Twitter) einzustellen. Dieser Schritt erfolgt aufgrund der fehlenden Vereinbarkeit der aktuellen Plattformpolitik mit den Grundwerten der Institutionen, insbesondere in Bezug auf Weltoffenheit, wissenschaftliche Integrität, Transparenz und demokratischen Diskurs. Kritisiert wird unter anderem die algorithmische Verstärkung rechtspopulistischer Inhalte sowie die Einschränkung der organischen Reichweite wissenschaftlicher Beiträge. Diese Entwicklungen gefährden die faktenbasierte Kommunikation und stehen im Widerspruch zu den demokratischen Prinzipien, denen sich die beteiligten Institutionen verpflichtet fühlen. Mit dem Austritt setzen die Hochschulen ein klares Zeichen für eine offene und sachliche Diskussionskultur. Sie betonen die Bedeutung von Vielfalt, Freiheit und Wissenschaft und wollen ihre Kommunikation auf anderen Plattformen fortsetzen. Gleichzeitig beobachten sie die weitere Entwicklung sozialer Netzwerke und deren Algorithmen kritisch, um sicherzustellen, dass ihre Grundwerte gewahrt bleiben.

Zu den beteiligten Institutionen gehören unter anderem die Freie Universität Berlin, die Goethe-Universität Frankfurt, die RWTH Aachen, die Universität Heidelberg sowie die Technische Universität Dresden. Auch Institutionen wie die Universität Ulm, die bereits in der Vergangenheit ihre Aktivitäten auf der Plattform eingestellt haben, unterstützen diesen Schritt und unterstreichen die Relevanz einer faktenbasierten wissenschaftlichen Kommunikation. Aus datenschutzrechtlicher Sicht kann die Nutzung der Plattform X Risiken bergen. Die aktuelle Plattformpolitik steht im Konflikt mit wesentlichen Datenschutzprinzipien, insbesondere hinsichtlich der algorithmischen Profilbildung und der Verarbeitung personenbezogener Daten. Die beteiligten Hochschulen empfehlen daher die Nutzung datenschutzkonformer Kommunikationsplattformen, um die Integrität und Sicherheit wissenschaftlicher Kommunikation zu gewährleisten.

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

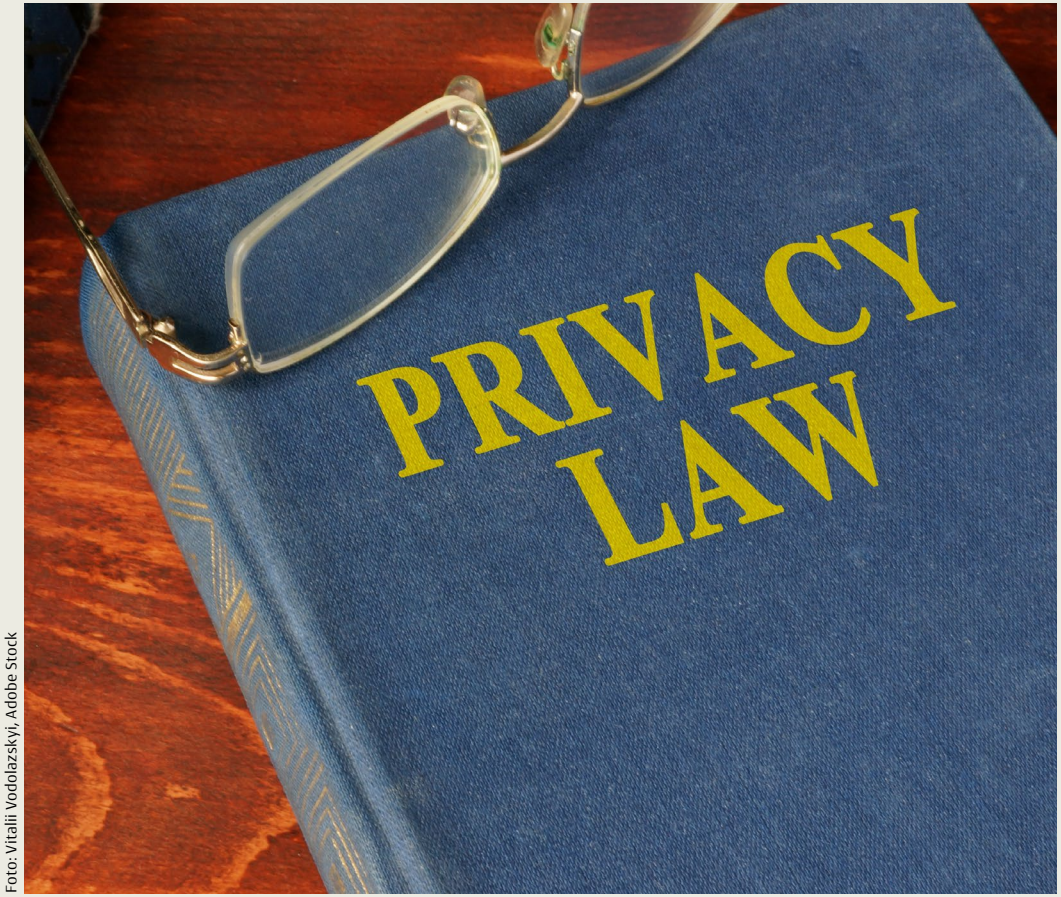

Foto: Vitalii Vodolazskyi, Adobe Stock

Gesammelte Rechtsprechung zum europäischen Datenschutzrecht

Mit dem Ziel der Harmonisierung und der gleichzeitigen Modernisierung des EU-Datenschutzrechts haben das Europäische Parlament und der Rat der Europäischen Union am 27. April 2016 die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) verabschiedet.

Trotz ihres Inkrafttretens seit dem 25. Mai 2018 in allen Mitgliedstaaten sind weiterhin Unterschiede in der nationalen Vollzugspraxis und der Rechtsprechung festzustellen. Um Interessierten und Anwendern im Wege der Rechtsvergleichung weitere Erkenntnisse für die Vollzugspraxis und die Anwendung des Datenschutzrechts zu ermöglichen, stellt die Datenschutzstelle Liechtenstein ihren sog. Judikaturspiegel zum europäischen Datenschutzrecht (2018–2024) als Download zur Verfügung.

Darin werden ausgewählte Gerichtsentscheide aus Mitgliedstaaten des Europäischen Wirtschaftsraums (EWR) (aus dem Zeitraum 2018 bis 2024) in Kurzfassung vorgestellt bzw. wesentliche Passagen der Entscheidungen hervorgehoben. Interessierten ist es damit möglich, auch die Eigenheiten des nationalen Rechtsstands zu ermitteln und abzugrenzen. Download: Judikaturspiegel zum europäischen Datenschutzrecht (2018–2024)

Auch der Europäische Gerichtshof für Menschenrechte (EGMR) bietet eine hilfreiche Publikation (CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS CONCERNING THE PROTECTION OF PERSONAL DATA) an, die als Fallsammlung verstanden werden kann. Diese dürfte jedoch wohl nur für Interessierte handhabbar sein, die sich intensiv mit der Thematik beschäftigen. Die Rechtsprechungsübersicht (Stand Dezember 2022, in englischer Sprache, PDF-Format) ist nachfolgend abrufbar:

Auch die ebenfalls nützlichen Factsheets zum Thema Datenschutz sind aktualisiert (Stand Februar 2024, in englischer Sprache, PDF-Format) und können unter nachfolgender URL abgerufen werden:

Effektive Datenschutzaufsicht für künstliche Intelligenz (KI)

Foto: Jiraphat.N, Adobe Stock

Auf Initiative der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) hat der Europäische Datenschutzausschuss (EDSA) im Rahmen seines Support-Pool-of-Experts-Programms eine Expertise zu KI-Anwendungen in Auftrag gegeben.

Da die Verarbeitung personenbezogener Daten durch KI-Systeme datenschutzrechtliche Vorgaben erfüllen muss, untersucht der Experte Dr. Kris Shrishak in seiner Analyse zentrale Herausforderungen. Dazu gehören die Erkennung und Beseitigung diskriminierender Verzerrungen (Bias) sowie die wirksame Umsetzung der Betroffenenrechte in den verschiedenen Phasen des KI-Lebenszyklus.
Dieses Projekt soll dazu beitragen, die Befangenheit und die Umsetzung der Rechte der betroffenen Personen im KI-Kontext zu verstehen und zu bewerten. Insbesondere kann es den Datenschutzbehörden helfen, indem es Methoden oder Instrumente für die Bewertung der Befangenheit und die Umsetzung der Rechte der betroffenen Personen klärt.
Die Ergebnisse der Untersuchung sind veröffentlicht und auf der Webseite des EDSA frei zugänglich.

Lagunov - stock.adobe.com

12. Hamburger Datenschutztage 2025

Sicherheit im digitalen Zeitalter – Entwicklung und Wachstum mit Verantwortung

Pre-Seminar: 25. Juni 2025
Konferenz: 26.–27. Juni 2025

Schwerpunkte:

- Datenschutz im Wandel
- DS-GVO und neue EU Digital-Rechtsakte
- Data Act: Theorie trifft Praxis
- KI-Praxisbericht: Wie man DS-GVO- und Compliance-Anforderungen bei ChatBots bewältigen kann
- Cybersecurity, Datenschutz und Resilienz: NIS-2 und der Cyber Resilience Act im Fokus
- Datenschutz, Solidarität und Demokratie: Warum Datenethik die Grundlage für eine freie und gerechte Gesellschaft ist
- Vorfallmanagement bei Datenschutzverletzungen

Jetzt anmelden:
www.datakontext.com/ds-tage

IBS data protection

Mit freundlicher Unterstützung
GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

Organisation
DATAKONTEXT

Foto: magele-picture, Adobe Stock

Datenschutzrechtliche Anforderungen an Betriebsvereinbarungen nach dem Europäischen Gerichtshof (EuGH)

Art. 88 der Datenschutz-Grundverordnung (DS-GVO) ermöglicht es den Mitgliedstaaten, durch nationale Vorschriften oder Kollektivvereinbarungen, spezifische Regelungen zur Verarbeitung personenbezogener Daten im Beschäftigungskontext zu treffen. Deutschland hat diese Öffnungsklausel im Bundesdatenschutzgesetz (BDSG) genutzt und in § 26 Abs. 4 BDSG festgelegt, dass Beschäftigtendaten auch auf Grundlage von Kollektivvereinbarungen verarbeitet werden dürfen. Allerdings war bislang unklar, welche Anforderungen solche Regelungen erfüllen müssen.

Mit seinem Urteil vom 19. Dezember 2024 (Rs. C-65/23) hat der EuGH nun Klarheit geschaffen. Er äußerte sich zu den datenschutzrechtlichen Vorgaben für Betriebsvereinbarungen und zur Frage, inwieweit diese gerichtlich überprüfbar sind. Anlass war eine Vorlagefrage des Bundesarbeitsgerichts (BAG).

Muss die nationale Regelung lediglich den Anforderungen aus Art. 88 Abs. 2 DS-GVO entsprechen, besteht ein gewisser Spielraum bei der Erstellung von Kollektivvereinbarungen, der es den Parteien ermöglicht, vom Schutzniveau der DS-GVO nach oben oder unten abzuweichen. Dadurch wären Unternehmen in der Gestaltung ihrer Betriebsvereinbarungen freier und könnten spezifischer auf Besonderheiten ihres Unternehmens eingehen.

Sollte jedoch der Art. 88 DS-GVO keine wesentlichen Abweichungen vom Schutzstandard der DS-GVO erlauben und eine Vollharmonisierung der Kollektivvereinbarungen mit den Grundsätzen der DS-GVO vorsehen, entfällt der Handlungsspielraum der Unternehmen bei Erstellung der Kollektivvereinbarungen, sodass lediglich eine Spezifizierung der DS-GVO-Vorschriften möglich wäre.

Die GDD hat sich mit den möglichen Auswirkungen des Urteils auf die Erstellung von Kollektivvereinbarungen beschäftigt und gibt nützliche Hinweise für die Praxis.

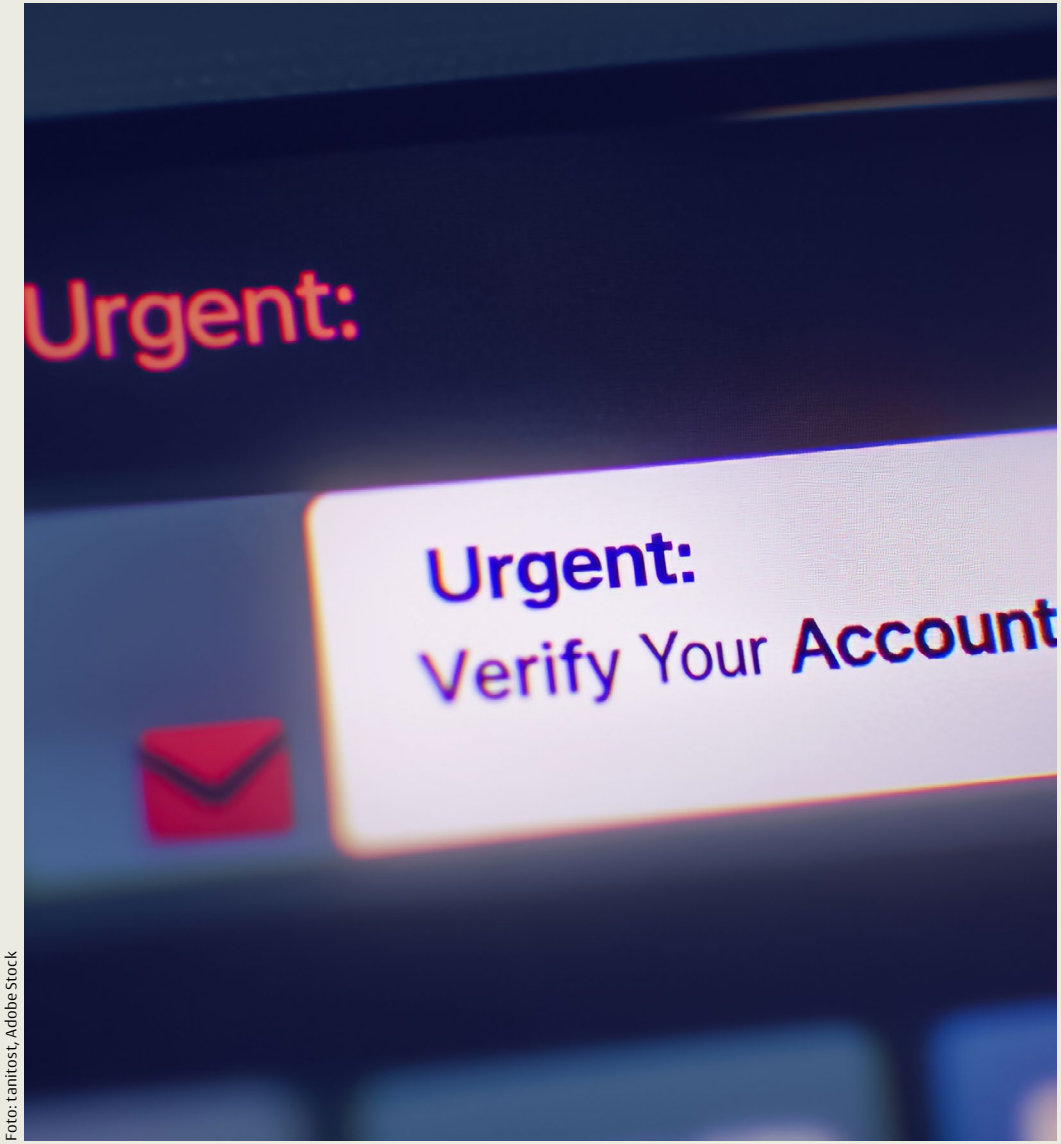

Foto: tanitost, Adobe Stock

Praxishilfe zu Benachrichtigungspflichten gemäß der Art. 33 und 34 DS-GVO

Datenschutzverletzungen stellen Unternehmen und Organisationen vor immense Herausforderungen.

Sie erfordern schnelles Handeln, präzise Analysen und die Einhaltung strikter gesetzlicher Vorgaben. Mit den Regelungen der Art. 33 und 34 DS-GVO gibt die Datenschutz-Grundverordnung Vorgaben für die Meldung von Datenschutzverletzungen, um die Rechte und Freiheiten der Betroffenen zu schützen.
Die GDD-Praxishilfe Checkliste „Meldung von Datenschutzverletzungen nach Art. 33, 34 DS-GVO“ bietet Verantwortlichen eine Unterstützung bei der Umsetzung dieser komplexen Anforderungen. Sie liefert praxisorientierte Erläuterungen zu den Voraussetzungen und Verfahren der Meldepflichten und ergänzt diese durch anschauliche Fallbeispiele aus der Praxis. Ziel ist es, Verantwortlichen die notwendige Orientierung zu geben, um Datenschutzvorfälle korrekt einzuordnen und geeignete Maßnahmen zu ergreifen.
Weitere Praxishilfen der GDD finden Sie hier.

Praxistipp: Datenschutzkonformes Schwärzen

Das datenschutzkonforme Schwärzen von Dokumenten, die personenbezogene Daten enthalten, stellt eine praxisrelevante technisch-organisatorische Maßnahme im Sinne von Art. 32 DS-GVO dar.

Foto: francescosgura, Adobe Stock

Es dient dem Schutz sensibler Informationen vor unbefugtem Zugriff, indem bestimmte personenbezogene Daten irreversibel unkenntlich gemacht werden. Diese Maßnahme ist besonders wichtig, um die Vertraulichkeit und Sicherheit der verarbeiteten Daten zu gewährleisten und das Risiko von Datenpannen zu minimieren.
Wenn Dokumente nicht ausreichend geschwärzt werden – etwa indem die Daten nur optisch verdeckt, aber technisch weiterhin zugänglich sind – entsteht eine erhebliche Gefahr für den Datenschutz. Solche Fehler führen oft zu unbeabsichtigten Offenlegungen personenbezogener Daten und können somit als Datenpannen im Sinne von Art. 33 DS-GVO eingestuft werden. Diese Pannen verpflichten den Verantwortlichen in der Regel zur Meldung an die Aufsichtsbehörden und können zu empfindlichen Sanktionen führen.
Neben der Sächsischen Datenschutz- und Transparenzbeauftragten zeigt nun auch die Datenschutzstelle des Fürstentums Liechtenstein auf, wo den Verantwortlichen beim Schwärzen gelegentlich Fehler unterlaufen. Damit es gar nicht erst zu Verstößen kommt, sollten Beschäftigte, die mit Schwärzungen und der Veröffentlichung von Dokumenten betraut sind, über mögliche Fehlerquellen und Lösungen Bescheid wissen.
Der Beitrag der Behörde kann damit gut und sinnvoll für eine kurze Sensibilisierungsmaßnahme der Beschäftigten genutzt werden.

Foto: NongAsimo, Adobe Stock

Stichtag für KI-getriebene Unternehmen: KI-Kompetenz

Am 2. Februar 2025 trat eine weitere Stufe des AI Act in Kraft, die für verschiedene Unternehmen relevant sein kann. Die entsprechende Norm lautet wie folgt: Artikel 4 KI-Kompetenz:

„Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."

Hier sind die wesentlichen Punkte mit potenziellem Handlungsbedarf für die Verantwortlichen:

Verbot bestimmter KI-Systeme

- Ab diesem Datum sind KI-Systeme mit unannehmbarem Risiko (z. B. Social Scoring) explizit verboten.
- Empfehlung: Überprüfung bestehender oder geplanter KI-Anwendungen auf mögliche Risiken im Sinne der Verordnung.

Kompetenzanforderungen für Mitarbeitende

- Mitarbeitende dürfen KI-Systeme nur nutzen, wenn sie über ausreichende KI-Kompetenz verfügen (technische Kenntnisse, Erfahrung, Schulung, Verständnis des Anwendungskontexts).
- Unklar ist, wie diese Kompetenz konkret nachzuweisen oder zu bewerten ist.
- Empfehlung: Prüfung, ob und welche internen Maßnahmen (Schulungen, Richtlinien) erforderlich sind, um rechtliche Risiken zu minimieren.

Zeitplan für weitere Verpflichtungen und Sanktionen

- Strafen gemäß Art. 99 KI-VO/AI-Act sind erst ab dem 2. August 2025 vorgesehen, sobald nationale Behörden zur Überwachung benannt sind.
- Verpflichtungen für General Purpose AI (GPAI) treten zwölf Monate nach Inkrafttreten der KI-Verordnung in Kraft (ab August 2025).
- Ein Leitfaden für GPAI wird in drei Monaten veröffentlicht, was mögliche weitere Anforderungen präzisieren könnte.
- Empfehlung: Beobachtung der Leitlinien und rechtlichen Entwicklungen, um frühzeitig Compliance-Maßnahmen einleiten zu können.

Jetzt KI-Kompetenz bei allen Beschäftigten aufbauen!

Das unverzichtbare Merkblatt unterstützt Unternehmen bei der Umsetzung von Artikel 4 der KI-Verordnung.

Art. 4 der KI-VO jetzt umsetzen!

- ideal für alle Beschäftigten
- firmenindividuell gestaltbar
- anschaulich illustriert und leicht verständlich geschrieben

Jetzt bestellen:
www.datakontext.com/merkblatt-ki

DATAKONTEXT

Foto: SunPunjiStudio, Adobe Stock

BSI: Chancen und Risiken generativer KI-Modelle

Es gibt bereits zahlreiche Veröffentlichungen, die sich den Chancen aber auch den Risiken widmen, die mit der Nutzung von generativen KI-Modellen einhergehen können. Unter diesen sticht die Ausarbeitung des BSI sicher schon bereits deswegen hervor, weil sie sich naturgemäß auf das Thema IT-Sicherheitsrisiko fokussiert, wenn die Gefahrenseite generativer KI-Modelle betrachtet wird.

Das BSI wendet sich mit einer Aktualisierung der Veröffentlichung „Generative KI-Modelle - Chancen und Risiken für Industrie und Behörden“ (Stand 17.01.2025) an Unternehmen und Behörden, die über den Einsatz generativer KI-Modelle in ihren Arbeitsabläufen nachdenken, um ein grundlegendes Sicherheitsbewusstsein für diese Modelle zu schaffen und ihren sicheren Einsatz zu fördern. Hierzu werden neben Chancen die wichtigsten aktuellen Gefahren, daraus resultierende Risiken während der Planungs- und Entwicklungsphase, dem Betrieb und der Verwendung von generativen KI-Modellen sowie mögliche Gegenmaßnahmen, bezogen auf den gesamten Lebenszyklus, der Modelle aufgezeigt.

Die Ausarbeitung des BSI kann damit als Grundlage für eine systematische Risikoanalyse dienen, die im Zusammenhang mit der Planungs- und Entwicklungsphase, dem Betrieb oder der Verwendung von generativen KI-Modellen durchgeführt werden sollte.

Die Veröffentlichung geht auch auf das Thema „Privacy Attacks“ ein. Dieser Begriff hat sich in der KI-Literatur als Standard für Angriffe etabliert, bei denen sensible Trainingsdaten rekonstruiert werden. Diese müssen jedoch nicht, anders als der Begriff vielleicht suggeriert, einen Personenbezug haben und können beispielsweise auch Firmengeheimnisse oder Ähnliches darstellen. Es ist zu beachten, dass das BSI keine Aussagen zu Datenschutzaspekten im rechtlichen Sinne trifft.

Die aktuelle Fassung wurde um die Chancen Risiken und Gegenmaßnahmen im Kontext von Bild- und Videogeneratoren ergänzt. Die Risiken und Gegenmaßnahmen wurden innerhalb der Kategorien entsprechend der Reihenfolge, in der sie im Lebenszyklus generativer KI-Modelle auftreten, umsortiert. Zudem wurden die Risiken teilweise umstrukturiert oder der Einfachheit wegen zusammengefasst.

Vorhandene Informationen zu großen KI-Sprachmodellen wurden auf den aktuellen Stand gebracht. Die Risiken und Maßnahmen wurden aufgrund der Betrachtung weiterer Ausgabemodalitäten jeweils in einen allgemeingültigen Teil und ggf. weitere modalitätsspezifische Informationen unterteilt.

Foto: blende11.photo, Adobe Stock

BAG stärkt Anforderungen an Geheimhaltungsklauseln in Arbeitsverträgen

Urteil vom 17. Oktober 2024 – Aktenzeichen: 8 AZR 172/23

Hintergrund

Das Bundesarbeitsgericht (BAG) hat in seinem Urteil vom 17. Oktober 2024 (8 AZR 172/23) die Anforderungen an Geheimhaltungsklauseln in Arbeitsverträgen präzisiert. Im vorliegenden Fall klagte ein Unternehmen, das Füllmaschinen für Lebensmittel und Getränke sowie entsprechendes Verpackungsmaterial herstellt, gegen einen ehemaligen Mitarbeiter auf Unterlassung der Weitergabe von Geschäftsgeheimnissen. Der Beklagte war bis zum 31. Dezember 2016 als Central Technology Manager beschäftigt und maßgeblich an der Produktentwicklung beteiligt. Der Arbeitsvertrag enthielt eine Klausel, die ihn verpflichtete, über alle Betriebs- und Geschäftsgeheimnisse sowie sonstige interne Vorgänge auch nach Beendigung des Arbeitsverhältnisses zeitlich unbegrenzt Stillschweigen zu bewahren.

Kernaussagen des Urteils

- **Anwendung des GeschGehG auf frühere Handlungen**: Das am 26. April 2019 in Kraft getretene Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) findet auch auf Unterlassungsansprüche Anwendung, wenn die Wiederholungsgefahr auf eine vor Inkrafttreten des Gesetzes begangene Handlung gestützt wird. Ein Unterlassungsanspruch besteht jedoch nur, wenn das beanstandete Verhalten zum Zeitpunkt seiner Vornahme nach damaligem Recht rechtswidrig war und die Voraussetzungen des GeschGehG zum Zeitpunkt der letztinstanzlichen Entscheidung erfüllt sind.
- **Unwirksamkeit von pauschalen Geheimhaltungsklauseln**: Formularmäßig vereinbarte Vertragsklauseln, die Arbeitnehmer über das Ende des Arbeitsverhältnisses hinaus zeitlich unbegrenzt zum Stillschweigen über alle internen Vorgänge verpflichten (sogenannte Catch-all-Klauseln), benachteiligen die Arbeitnehmer unangemessen und sind daher unwirksam.

Implikationen für die Praxis

Dieses Urteil unterstreicht die Notwendigkeit für Arbeitgeber, Geheimhaltungsklauseln in Arbeitsverträgen präzise und differenziert zu formulieren. Pauschale und zeitlich unbegrenzte Verpflichtungen können als unangemessene Benachteiligung der Arbeitnehmer angesehen werden und somit unwirksam sein. Zudem sind bei der Geltendmachung von Unterlassungsansprüchen die Rechtslage zum Zeitpunkt der Handlung sowie die aktuellen Anforderungen des GeschGehG zu berücksichtigen. Datenschutzbeauftragte und Compliance-Verantwortliche sollten bestehende Verträge und Geheimhaltungsvereinbarungen überprüfen und gegebenenfalls an die aktuellen rechtlichen Vorgaben anpassen, um rechtliche Risiken zu minimieren.

Foto: Andrei, Adobe Stock

Der Europäische Datenschutzausschuss konkretisiert den Begriff der Pseudonymisierung

Der Europäische Datenschutzausschuss (EDSA) hat am 16. Januar 2025 den Begriff der Pseudonymisierung weiter definiert und damit praxisrelevante Klarstellungen getroffen.

Eine öffentliche Konsultation des Europäischen Datenschutzausschusses (EDSA) ist ein Verfahren, bei dem der EDSA Entwürfe zu Datenschutzrichtlinien, Leitlinien oder Empfehlungen veröffentlicht und der Öffentlichkeit die Möglichkeit gibt, dazu Stellung zu nehmen. Die öffentliche Konsultation basiert auf der Datenschutz-Grundverordnung, insbesondere auf Art. 70 DS-GVO, der die Aufgaben des EDSA festlegt. Dazu gehört die Förderung einheitlicher Anwendung der DS-GVO in der EU durch Leitlinien und Empfehlungen. Nach der Konsultationsphase bewertet der EDSA die Rückmeldungen und überarbeitet gegebenenfalls die Vorschläge, bevor sie final verabschiedet werden.

Die Leitlinien enthalten zwei wichtige rechtliche Klarstellungen:

1. Pseudonymisierte Daten, die einer Person durch die Verwendung zusätzlicher Informationen zugeordnet werden könnten, bleiben Informationen, die sich auf eine identifizierbare natürliche Person beziehen, und sind daher immer noch personenbezogene Daten. In der Tat, wenn die Daten von dem für die Verarbeitung Verantwortlichen oder einer anderen Person mit einer Person verknüpft werden können, bleiben sie personenbezogene Daten.
2. Die Pseudonymisierung kann Risiken reduzieren und die Nutzung berechtigter Interessen als Rechtsgrundlage erleichtern (Art. 6 Abs. 1 lit. f DS-GVO), sofern alle anderen Anforderungen der DS-GVO erfüllt sind. Ebenso kann die Pseudonymisierung dazu beitragen, die Vereinbarkeit mit dem ursprünglichen Zweck zu gewährleisten (Art. 6 Abs. 4 DS-GVO).

In den Leitlinien wird erläutert, wie die Pseudonymisierung Organisationen dabei helfen kann, ihren Verpflichtungen in Bezug auf die Umsetzung der Datenschutzgrundsätze (Art. 5 DS-GVO), den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) und der Sicherheit (Art. 32 DS-GVO) nachzukommen. Schließlich werden in den Leitlinien technische Maßnahmen und Garantien bei der Verwendung von Pseudonymisierung analysiert, um die Vertraulichkeit zu gewährleisten und eine unbefugte Identifizierung von Personen zu verhindern.

Die Leitlinien werden bis zum 28. Februar 2025 einer öffentlichen Konsultation unterzogen, um den Interessenträgern Gelegenheit zur Stellungnahme zu geben und die Einbeziehung künftiger Entwicklungen in die Rechtsprechung zu ermöglichen.

DATA AGENDA PODCAST

(Quelle: TH Köln/Schmülgen)

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

Folge #66

Update KI-VO: Leitlinien der Kommission zu verbotenen Praktiken

Kai Zenner

Folge #67

Zukunftsperspektiven für KI-Haftung und ePrivacy

Axel Voss

Data Agenda Podcast Folge 66: Update – KI-VO-Leitlinien der Kommission zu verbotenen Praktiken

Seit dem 2. Februar 2025 gilt Art. 5 KI-VO, der bestimmte KI-Praktiken verbietet. Am 4. Februar 2025 erfolgte die Veröffentlichung der Leitlinien zu verbotenen KI-Praktiken durch die Kommission, die gemäß Art. 96 KI-VO vorgesehen ist. Darin werden einzelne Tatbestandsmerkmale der verbotenen KI-Praktiken, mithilfe von Praxisbeispielen konkretisiert. Diese Leitlinien sind rechtlich nicht bindend, können in der Praxis aber dabei helfen, verbotene KI-Praktiken im eigenen Verantwortungsbereich zu identifizieren. Im Podcast ordnet Kai Zenner, der als Büroleiter von Axel Voss MdEP die Verbote im Gesetzgebungsprozess verhandelt hat, das Papier ein.
Zum Podcast bitte hier klicken.

Data Agenda Podcast Folge 67: Zukunftsperspektiven für KI-Haftung und ePrivacy

Im Februar 2025 hat die EU-Kommission ihr Arbeitsprogramm für 2025 vorgelegt. Der geplante Entwurf der KI-Haftungsrichtline wurde ebenso von der Agenda der EU genommen, wie die ePrivacy-Verordnung. Was hat zum Scheitern geführt und wie geht es weiter? Über die Hintergründe und Konsequenzen spricht Axel Voss, der Berichterstatter des EU-Parlaments für die Richtlinie zur KI-Haftung war. Weitere Themen des Podcasts sind die Aussichten auf eine Änderung der DS-GVO und ein KI-Datengesetz.
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