NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

2 Editorial
3 Datenzugang für Forschende im Rahmen des Digital Services Act (DSA)
4 EU-UK-Angemessenheitsbeschluss bleibt bis Dezember 2031 gültig
5 Checkliste: Datensicherheit durch Datenschutz
6 Elektronische Patientenakte: Datenschutzrisiken und Drittstaatenzugriffe
7 Mitbestimmungsrechte des Betriebsrats bei der Einhaltung des Datenschutzes
8 BVwG (Österreich) konkretisiert Haushaltsausnahme nach DS-GVO
9 BEM: Weitergabe betriebsärztlicher Gutachten an die Schwerbehindertenvertretung
10 Einsichtsrechte bei internen Untersuchungen
11 15.000 Euro Entschädigung für unzulässige Videoüberwachung
13 Impressum

AUSGABE
12/2025

Levent Ferik

EDITORIAL

Das parlamentarische Auskunftsrecht ist ein fundamentales Kontrollinstrument – ebenso wie das Auskunftsrecht nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) für Betroffene ein Instrument darstellt, welche die Ausübung weiterer Betroffenenrechte überhaupt sinnvoll ermöglicht. Doch beide Rechte bergen ein Spannungsfeld: Was passiert, wenn sie systematisch genutzt werden, um möglichst detaillierte Informationen über kritische Strukturen zu sammeln oder die Stoßrichtung ihrer Ausübung missbräuchlich ist?

Aktuell sorgt die Praxis der AfD für Debatten. Innenexperten in Thüringen warnen, dass die Fraktion mit einer hohen Zahl kleiner Anfragen gezielt Daten zu sicherheitsrelevanter Infrastruktur erhebt – von Energie- und Wasserleitungen bis hin zu digitalen Netzen. Kritikpunkte betreffen insbesondere den Umfang, die Detailtiefe und die Sensibilität der abgefragten Informationen. Politikerinnen und Experten diskutieren, ob diese Vorgehensweise noch dem parlamentarischen Zweck dient oder die Grenze zur Ausforschung überschreitet.

Formal korrekt – und dennoch heikel, weil die Abfrage sensibler Details die Grenze zwischen legitimer Kontrolle und potenzieller Ausforschung verwischt. Ähnlich verhält es sich im Datenschutz: Das Auskunftsrecht nach Art. 15 DSGVO schützt die Betroffenen, kann aber im Missbrauchsfall dazu verwendet werden, Daten systematisch zusammenzutragen, die entweder zweckwidrig genutzt werden sollen oder gar wiederum die Persönlichkeitsrechte von anderen betroffenen Personen verletzen. Auch die Verletzung von Geschäftsgeheimnissen oder Risiken für Whistleblower, denen Anonymität zugesichert wurde, sind denkbar.

Die Parallele ist eindeutig: Jedes Recht auf Auskunft kann – abhängig vom Einsatz – sowohl Schutzmechanismus als auch Risikoquelle sein. Die Lektion bleibt: Rechte und Transparenzinstrumente sind unverzichtbar. Sie benötigen aber Kontextbewusstsein, Sensibilität und kritische Abwägung. Nur so bleiben sie Mittel zur Kontrolle und nicht zur unbeabsichtigten Offenlegung sensibler Informationen.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Ruth, Adobe Stock

Datenzugang für Forschende im Rahmen des Digital Services Act (DSA)

Seit dem 29. Oktober 2025 haben Forschende die Möglichkeit, bei sehr großen Online-Plattformen und -Suchmaschinen den Zugang zu internen, nicht-öffentlichen Plattformdaten zu beantragen.

Die Bearbeitung von Daten der Nutzenden, die Rückschlüsse auf Einzelpersonen zulassen können, etwa über Interaktionen, Profile oder veröffentlichte Inhalte, verlangt die sorgfältige Beachtung der Datenschutz-Grundverordnung. Die zuständige Aufsichtsbehörde prüft im Zulassungsverfahren u. a. die Verhältnismäßigkeit der Datenverarbeitung und die Beschreibung technischer sowie organisatorischer Maßnahmen durch Forschende. Eine entsprechende Hilfestellung bietet eine Checkliste des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI).

Checkliste für Datenschutz- und Datensicherheitsstandards

Die vom HmbBfDI veröffentlichte Checkliste legt klar dar, welche Informationen Antragstellende angeben müssen:

- Erläuterung, ob anonymisierte bzw. pseudonymisierte Daten verarbeitet werden können.
- Angaben zu den konkreten Zwecken der Datenverarbeitung mit Bezug auf Art. 40 Abs. 4 DSA.
- Beschreibung der technischen und organisatorischen Maßnahmen (TOM) – z. B. Verschlüsselung, Rechte- und Rollenkonzepte, Löschkonzepte.
- Hinweise zur etwaigen Notwendigkeit einer Datenschutz-Folgenabschätzung (DSFA).

Praxisrelevanz

Für interne Datenschutzbeauftragte, IT-Sicherheitsbeauftragte und Forschungsverantwortliche ergibt sich damit Folgendes:

- Der Datenzugang nach dem DSA erfordert eine fundierte datenschutzrechtliche Prüfung bereits im Antrags- und Genehmigungsprozess.
- Die von HmbBfDI bereitgestellte Checkliste kann als strukturierte Vorlage dienen, um Anforderungen der DS-GVO sowie der DSA-Zulassung nachzuweisen.
- Dokumentation und Nachweis technischer sowie organisatorischer Maßnahmen gewinnen weiter an Bedeutung – nicht nur im eigenen Risikomanagement, sondern auch im Kontext externer Forschungszugriffe.
- Die frühe Einbindung von Datenschutz- und Sicherheitsverantwortlichen in Forschungsprojekte mit Plattformdaten ist essenziell, um Compliance-gerecht zu arbeiten.

Foto: AkborHussain, Adobe Stock

EU-UK-Angemessenheits-beschluss bleibt bis Dezember 2031 gültig

Der European Data Protection Board (EDPB) hat im Oktober 2025 zwei Stellungnahmen („Opinion 26/2025“ und „Opinion 27/2025“) zu den Entwürfen der Europäischen Kommission für die Verlängerung der Angemessenheitsbeschlüsse des Vereinigten Königreichs (United Kingdom, UK) aufgelegt – einmal im Bereich der DS-GVO und einmal in Bezug auf die Richtlinie über den Datenschutz im Bereich der Strafverfolgung (LED).
Die Beschlüsse sollen es weiterhin ermöglichen, personenbezogene Daten aus der EU bzw. dem Europäischen Wirtschaftsraum (EWR) in das Vereinigte Königreich ohne zusätzliche Garantien zu übermitteln.

Weiter auf DataAgenda lesen

Foto: Kaniz Fatema, Adobe Stock

Checkliste: Datensicherheit durch Datenschutz

Das Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) berichtet von einer steigenden Zahl von Cybervorfällen bei bayerischen Unternehmen – von kompromittierten E-Mail-Accounts über gezielte Spear-Phishing-Angriffe bis hin zu gravierenden Verschlüsselungs- und Erpressungsszenarien. Die wirtschaftlichen Schäden sind erheblich und die datenschutzrechtlichen Folgen für betroffene Personen häufig kaum mehr überschaubar. In Reaktion darauf verfolgt die BayLDA das Ziel, das bestehende Präventionsprogramm konsequent auszubauen und auf zentrale Schutzmaßnahmen hinzuweisen – mit dem Leitbild der „uneinnehmbaren Festung".

Kerndokument: „Checkliste Cyberfestung – 10 Punkte für mehr Datensicherheit"

Die Checkliste (nach Art. 32 DS-GVO) dient als Good-Practice-Instrument zur Soll-Ist-Analyse technischer und organisatorischer Schutzmaßnahmen.

Die zehn Schwerpunktbereiche sind:

1. Netzwerkperimeter und Angriffsmöglichkeiten ermitteln – dazu gehören Inventarisierung interner und externer Komponenten, Cloud-Dienste sowie regelmäßige Port-/Netzwerkscans.
2. Mehr-Faktor-Authentifizierung (MFA) einsetzen – insbesondere für Administratoren, Cloud-Dienste, VPN-Zugänge; plus Protokollierung und Schulung.
3. Umgang mit lokalen Administratorkonten regeln – Minimierung von Konten, differenzierte Passwörter, Protokollierung, ggf. Just-in-Time-Zugänge.
4. PowerShell-Skripte einschränken – restriktiver Einsatz, Whitelisting, Signaturpflicht, Protokollierung.
5. Netzwerksegmentierung nutzen – Aufteilung des Netzwerks in Zonen, interne Firewalls, Dokumentation, Zero-Trust-Prinzipien.
6. Zentralen Internetübergangspunkt überwachen – Einsatz von Next Generation Firewall (NGFW), DNS-Filterung, E-Mail-Gateways, SIEM/IDS/IPS, Egress-Filtering, TLS/SSL-Inspection.
7. Ransomware-sichere Backups verwenden – Umsetzung der 3-2-1-Regel, Offline- und WORM-Lösungen, Testwiederherstellungen, Verschlüsselung.
8. Awareness und Social Engineering thematisieren – regelmäßige Schulungen, Phishing-Simulationen, Meldeprozesse, Sensibilisierung für KI-gestützte Angriffe.
9. Software-Updates durchführen – Patch-Management mit Inventarisierung, Priorisierung nach Risiko, Testumgebung, automatisierte Verteilung.
10. Domain Controller absichern – (Im Dokument vertieft, z. B. Härtung von Domänencontrollern, Bewegungsüberwachung; nicht im Überblicksabschnitt gelistet)

Die BayLDA betont, dass diese Checkliste nicht als abschließend zu verstehen ist, sondern als Orientierung für eine individuelle Risikobetrachtung innerhalb der eigenen Organisation.

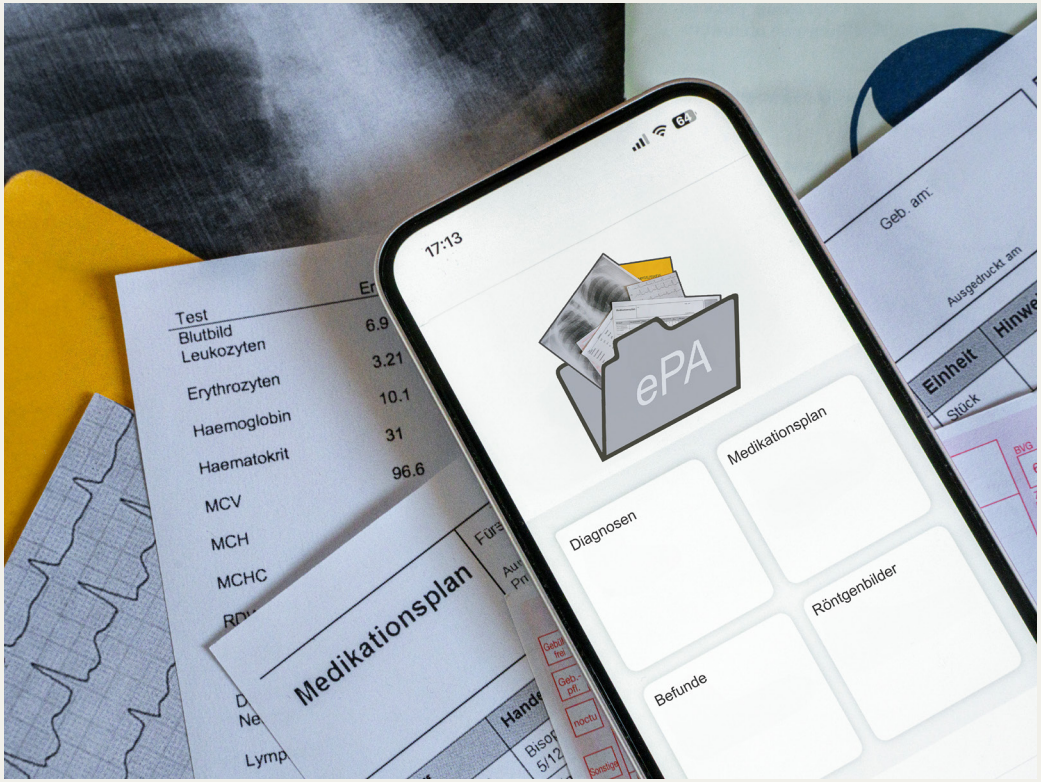


Foto: Andrea Gaitanides, Adobe Stock

Elektronische Patientenakte: Datenschutzrisiken und Drittstaatenzugriffe

Die Einführung der elektronischen Patientenakte (ePA) in Deutschland wirft weiterhin grundlegende datenschutzrechtliche Fragen auf. Eine „Kleine Anfrage" der Fraktion Die Linke (Drucksache 21/1912) fokussiert unter anderem auf die Möglichkeit, dass Dienstleister wie IBM Deutschland GmbH oder RISE GmbH Daten der ePA aufgrund außereuropäischer Gesetze an Behörden außerhalb der EU übermitteln könnten.

Technische und organisatorische Schutzmaßnahmen

Die Bundesregierung führt aus, dass ePADaten verschlüsselt in deutschen Rechenzentren verarbeitet werden; zugleich ist jedoch unklar, wie Vertragsklauseln mit externen Dienstleistern gestaltet sind, die Drittstaatenzugriffe erlauben könnten. netzpolitik.org moniert, dass trotz technischer Architektur mit EndtoEndVerschlüsselung und Zugriffskontrollen die rechtliche Absicherung gegenüber extraterritorialen Zugriffen unzureichend dargelegt wird.

Zugriffsrechte und Transparenz

In der Anfrage wird betont, dass Versicherte ihre Daten selektiv freigeben oder verbergen können sollen und Einblick in Protokolle über Zugriffe auf ihre ePA erhalten sollen. Die Praxis zeigt jedoch, dass die Nachvollziehbarkeit und Transparenz solcher Zugriffe eine zentrale Rolle spielen, um den datenschutzrechtlichen Anforderungen gerecht zu werden.

Barrierefreiheit und Zugang

Auch der barrierefreie und gleichberechtigte Zugang zur ePA wird diskutiert. Menschen ohne eigenes Endgerät oder Internetzugang sowie Nutzerinnen und Nutzer mit Seh-, Hör- oder motorischen Einschränkungen sollen nach den Vorgaben der Barrierefreie-Informationstechnik-Verordnung (BITV 2.0) Zugang erhalten. Die Umsetzung entsprechender Lösungen ist bislang noch nicht vollständig realisiert.

Internationale Rechtsfragen

Neben technischen Aspekten wird die rechtliche Dimension relevant: US-amerikanische Regelungen wie der CLOUD Act könnten theoretisch Zugriff auf Daten erzwingen, wodurch die internationale Datenweitergabe der ePA kritisch bewertet wird. Die Kombination aus technischen Sicherheitsmaßnahmen, Vertragsgestaltung und internationalen Rechtsnormen bleibt somit ein zentrales Thema für die Beurteilung des Datenschutzes der ePA.

Foto: Nico, Adobe Stock

Mitbestimmungsrechte des Betriebsrats bei der Einhaltung des Datenschutzes

Das Verfahren (LArbG Frankfurt 5. Kammer, Beschluss vom 5. Dezember 2024 , Az: 5 TaBV 4/24) betraf die Einführung eines IT-Systems („HCM“) in einem international agierenden Unternehmen, das u. a. Stammdaten von Beschäftigten verwaltete und auf Servern eines US-amerikanischen Konzerns betrieben wurde. Der Betriebsrat war in das Einigungsstellenverfahren eingebunden; die Betriebsvereinbarung (BV HCM) regelte u. a. die Nutzung, die Datenverarbeitung und den Datentransfer. Der Betriebsrat beanstandete insbesondere, dass ein Datentransfer in die USA rechtswidrig sei und diskussionswürdig im Bereich Mitbestimmung nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) sowie § 87 Abs. 1 Nr. 1 BetrVG.

Weiter auf DataAgenda lesen

Foto: Wool World, Adobe Stock

BVwG (Österreich) konkretisiert Haushaltsausnahme nach DS-GVO

In dem zugrunde liegenden Verfahren (W258 2242162-1/24E) beschwerte sich eine Nachbarin über heimliche angefertigte Bildaufnahmen, die ein Anrainer in ihrer privaten Garagenbox gemacht und anschließend an ihren früheren Lebensgefährten weitergegeben haben soll. Die Datenschutzbehörde (DSB) stellte 2021 eine Verletzung des Rechts auf Geheimhaltung gemäß § 1 Abs. 1 Datenschutzgesetz (DSG) fest. Gegen diesen Bescheid erhob der Beschwerdegegner Rechtsmittel. Das Bundesverwaltungsgericht (BVwG) wies die Beschwerde nun ab und bestätigte den Bescheid mit Präzisierungen.

Sachverhalt

Zwischen Ende Juni und Anfang Juli 2020 betrat der Beschwerdegegner ohne Zustimmung der Betroffenen die zugeordnete Garagenbox, installierte dort verdeckt eine Kamera und fertigte mehrere Lichtbilder an; mindestens zwei zeigten die Betroffene selbst. Anschließend übermittelte er die Aufnahmen per WhatsApp an ihren ehemaligen Lebensgefährten. Ziel war laut Feststellungen des Gerichts, Konflikte zwischen beiden zu schüren. Die Behauptung des Beschwerdegegners, das Bildmaterial sei anonym übermittelt worden, wertete das BVwG als widersprüchlich und konstruiert.

Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DS-GVO

Das Gericht setzt sich ausführlich mit der Frage auseinander, ob die Haushaltsausnahme eingreift. Dies wurde zweifach verneint:

1. Erstellung der Aufnahmen

Die Kamera wurde im privaten Bereich einer dritten Person installiert. Die Verarbeitung richtete sich damit bewusst auf einen Bereich außerhalb der eigenen Privatsphäre des Verantwortlichen. Eine ausschließlich persönliche oder familiäre Tätigkeit lag daher nicht vor. Damit scheidet die Ausnahme bereits im ersten Schritt aus.

2. Weitergabe der Bilder

Die Übermittlung an den ehemaligen Lebensgefährten der Betroffenen lässt den Vorgang ebenfalls aus der persönlichen Sphäre des Beschwerdegegners heraustreten. Es bestand kein familiärer oder häuslicher Bezug. Auch insoweit ist Art. 2 Abs. 2 lit. c DS-GVO nicht anwendbar. Das BVwG betont, gestützt auf einschlägige EuGH-Rechtsprechung, dass die Haushaltsausnahme eng auszulegen ist und bei Überwachungshandlungen, die in die Sphäre Dritter reichen, regelmäßig entfällt.

Rechtliche Würdigung

Mangels Haushaltsausnahme gilt die DS-GVO vollständig. Die verdeckte Aufnahme und Weitergabe verstößt gegen zentrale Verarbeitungsgrundsätze – insbesondere Transparenz und Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO). Beide Handlungen erfolgten ohne Rechtsgrundlage und ohne Möglichkeit der Betroffenen, mit der Verarbeitung zu rechnen.

Foto: Garun Studios, Adobe Stock

BEM: Weitergabe betriebsärztlicher Gutachten an die Schwerbehindertenvertretung

In einem vom Betrieblichen Eingliederungsmanagement (BEM) zu unterscheidenden Präventionsverfahren nach § 167 Abs. 1 SGB IX schaltet der Arbeitgeber frühzeitig unter anderem die Schwerbehindertenvertretung ein, wenn personen-, verhaltens- oder betriebsbedingte Schwierigkeiten eintreten, die das Beschäftigungsverhältnis mit einem schwerbehinderten oder ihm gleichgestellten Menschen gefährden könnten.

Ziel dieses Verfahrens ist es, eine vorzeitige Beendigung des Beschäftigungsverhältnisses (insbesondere durch Kündigung) aufgrund dieser Schwierigkeiten möglichst zu vermeiden. Im Präventionsverfahren soll umfassend erörtert werden, wie die bestehenden Schwierigkeiten im Beschäftigungsverhältnis beseitigt werden können. Es dient damit vorrangig der Konfliktprävention. Das Präventionsverfahren bedarf im Vergleich zum BEM keiner Zustimmung der oder des betroffenen Beschäftigten.

Die Frage, ob betriebsärztliche Gutachten im Rahmen des BEM oder eines Präventionsverfahrens an die Schwerbehindertenvertretung weitergegeben werden dürfen, ist datenschutzrechtlich sensibel. Nach § 178 Abs. 2 Sozialgesetzbuch (SGB) IX ist die Schwerbehindertenvertretung in Angelegenheiten, die einzelne schwerbehinderte Beschäftigte betreffen, zu informieren und anzuhören. Ein eigenständiges, einwilligungsunabhängiges Einsichtsrecht in Personalakten besteht jedoch nicht (§ 178 Abs. 3 Satz 1 SGB IX).

Im BEM nach § 167 Abs. 2 SGB IX muss der Arbeitgeber allen Beschäftigten, die länger als sechs Wochen arbeitsunfähig waren, ein BEM anbieten. Die Teilnahme der Schwerbehindertenvertretung setzt die Zustimmung der betroffenen Person voraus. Betriebsärztliche Gutachten enthalten dabei sensible Gesundheitsdaten (Art. 9 DS-GVO) und dürfen daher ohne ausdrückliche, freiwillige Einwilligung der Beschäftigten nicht weitergegeben werden, so der BayLfD in seinem 34. Tätigkeitsbericht 2024.

Im Präventionsverfahren nach § 167 Abs. 1 SGB IX ist eine Beteiligung der Schwerbehindertenvertretung vorgesehen, um Konflikte im Beschäftigungsverhältnis frühzeitig zu beheben. Dennoch ist die Weitergabe von betriebsärztlichen Gutachten auch hier grundsätzlich nur mit ausdrücklicher Einwilligung der Betroffenen zulässig, da diese Informationen regelmäßig personenbezogen sind und Teil der Personalakte werden.

Fazit:

Sowohl im BEM als auch im Präventionsverfahren entscheidet in der Regel die betroffene Person über die Weitergabe betriebsärztlicher Gutachten an die Schwerbehindertenvertretung. Arbeitgeber sind verpflichtet, das Vorliegen wirksamer Einwilligungen zu dokumentieren und nachzuweisen, um den datenschutzrechtlichen Anforderungen nach Art. 5 Abs. 2 und Art. 7 Abs. 1 DS-GVO zu genügen.

Foto: oksa_studio, Adobe Stock

Einsichtsrechte bei internen Untersuchungen

Das Landesarbeitsgericht München (Az. 2 SLa 70/25, 12. Juni 2025) hat klargestellt, unter welchen Bedingungen Mitarbeitende Einsicht in interne Untersuchungsberichte erhalten. Gegenstand war ein Compliance-Abschlussbericht über Beschwerden gegen eine leitende Angestellte, der Zeugenaussagen, interne Bewertungen und Empfehlungen enthielt.

Datenschutzrechtlicher Kern

Mitarbeitende haben kein generelles Recht auf Herausgabe des vollständigen Berichts, sondern nur auf Einsicht in ihre personenbezogenen Daten gemäß Art. 15 DSGVO. Bewertungen, Empfehlungen oder Aussagen Dritter müssen nicht offengelegt werden. Das Urteil betont die Bedeutung einer klaren Strukturierung und Dokumentation: Personenbezogene Daten der Betroffenen, interne Bewertungen und Schutzinformationen für Hinweisgeber oder Zeugen sollten getrennt behandelt werden. Schwärzungen gelten als geeignetes Mittel, um Auskunftsansprüche zu erfüllen und zugleich den Schutz Dritter zu wahren.

Arbeitsrechtliche Perspektive

Werden Berichte in die Personalakte übernommen, entsteht ein Einsichtsrecht nach § 26 Abs. 2 SprAuG bzw. § 83 BetrVG. Ein pauschales Verweigerungsrecht zugunsten des Unternehmens besteht nicht; jede Entscheidung erfordert eine individuelle Abwägung zwischen Transparenz und Schutzinteressen.

Praxisleitlinien für Compliance und HR

Für Compliance- und HR-Abteilungen empfiehlt es sich, interne Untersuchungsberichte modular zu strukturieren. Eine Trennung ermöglicht es, Mitarbeitenden gezielt Zugang zu den für sie relevanten Informationen zu gewähren, ohne interne Bewertungen oder sensible Drittdaten offenzulegen.
Gleichzeitig erleichtert die modulare Struktur die Versionskontrolle, das Zugriffsmanagement und die Dokumentation datenschutzkonformer Entscheidungen. Unternehmen sollten frühzeitig klären, wer datenschutzrechtlich für die Verarbeitung verantwortlich ist, und in internen Richtlinien das Spannungsfeld zwischen Auskunftsrechten und Schutzinteressen festlegen. So wird sichergestellt, dass Betroffene angemessene Einsicht erhalten, während Hinweisgeber, Zeugen und Geschäftsgeheimnisse geschützt bleiben.

Foto: Snap Vivid, Adobe Stock

15.000 Euro Entschädigung für unzulässige Videoüberwachung

Das Landesarbeitsgericht Hamm (Az. 18 SLa 959/24, 28. Mai 2025) hat sich mit der datenschutzrechtlichen Zulässigkeit einer umfangreichen Videoüberwachung am Arbeitsplatz befasst. Der Arbeitgeber hatte über einen längeren Zeitraum zahlreiche Kameras im Innenbereich des Betriebs eingesetzt, die Beschäftigte dauerhaft und in hoher Auflösung erfassten. Die Betriebshalle der Beklagten besteht aus einer Produktionshalle, in welcher Stahl verarbeitet wird, einem Pausenraum, Umkleideräumen, WCs, zwei Büros und einem angrenzenden Lagerraum.
Etwa zehn Meter hinter dem Arbeitsplatz des Klägers war in einer Höhe von ca. fünf bis sechs Metern eine Videokamera installiert, die im Wesentlichen den sicherheitsrelevanten Auf- und Abladebereich der Maschine aufzeichnet Die Aufnahmen wurden gespeichert und konnten live ausgewertet werden.
Ein Arbeitnehmer sah sich dadurch in seinen Rechten verletzt und machte datenschutzrechtliche Ansprüche geltend – unter anderem auf Schadensersatz.

Entscheidung und Konsequenzen

Das Gericht sah einen erheblichen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers, da durch die Videoaufnahmen seine informationelle Selbstbestimmung beeinträchtigt wurde. Entscheidend war, dass die Datenverarbeitung weder durch eine wirksame Einwilligung (Art. 7 DS-GVO) noch durch eine einschlägige Rechtsgrundlage (z. B. § 26 Bundesdatenschutzgesetz (BDSG)) gedeckt war. Zudem erfüllte die Maßnahme nicht die Anforderungen der Verhältnismäßigkeit nach Art. 6 Abs. 1 lit. f DS-GVO bzw. § 26 Abs. 1 BDSG (z. B. fehlende konkrete Gefährdungssituation, großflächiger Innenbereich überwacht).
Das Gericht verneinte zwar einen Anspruch auf Unterlassung (da das Arbeitsverhältnis beendet war und keine Wiederholungsgefahr bestand). Es bejahte jedoch einen Anspruch auf Zahlung einer Geldentschädigung gemäß § 253 Abs. 2 BGB i. V. m. §§ 280 Abs. 1, 823 Abs. 1 Bürgerliches Gesetzbuch (BGB) – wegen der rechtswidrigen, schuldhaften und erheblichen Verletzung des Persönlichkeitsrechts. Die Höhe der Entschädigung betrug 15.000 Euro – begründet mit der langen Überwachungsdauer, der HD-Live-Überwachung und der Weigerung des Arbeitgebers, die Überwachung trotz Widerspruchs einzustellen.

Relevanz für Datenschutzpraxis

Für Verantwortliche und Datenschutzbeauftragte in Betrieben gilt:

- Bei Verstößen drohen nicht nur Bußgelder, sondern auch erhebliche Entschädigungsforderungen von Arbeitnehmerseite.
- Jede Videoüberwachung von Beschäftigten fällt unter die DS-GVO bzw. das BDSG und bedarf einer konkreten Rechtsgrundlage und Verhältnismäßigkeit.
- Eine vertragliche „Einwilligung“ im Arbeitsvertrag ersetzt keine freiwillige, informierte Einwilligung nach Art. 7 DS-GVO.
- Zweckbindung ist zentral: Allgemeine Sicherheitszwecke oder große Flächenüberwachung reichen nicht ohne konkret belegbare Gefährdung.
- Dokumentation und Beratung im Vorfeld sind essenziell. Das Gericht kritisierte fehlende datenschutzrechtliche Beratung im Vorfeld.

DATA AGENDA PODCAST

(Quelle: TH Köln/Schmülgen)

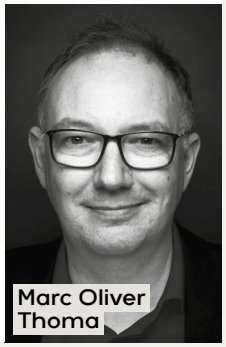
Der **Experten-Talk** mit Prof. Dr. Schwartmann

Folge #78

Mehr als Datenschutzaufsicht – Die Rolle der Bundesnetzagentur im KI- und Datenrecht

Folge #79

Datenschutz-management-software im Praxischeck



Data Agenda Podcast Folge 78: Mehr als Datenschutzaufsicht – Die Rolle der Bundesnetzagentur im KI- und Datenrecht

Die Bundesnetzagentur spielt für die Aufsicht im Daten- und KI-Recht nach dem Data Act und der KI-Verordnung eine zentrale Rolle. Der Gesetzgebungsprozess in Deutschland ist am 4. November angelaufen. Im Podcast berichtet Axel Voss (MdEP) über die Konzeption der Aufsicht nach der KI-VO und Andrea Sanders-Winter, Leiterin der Abteilung Digitales bei der BNetzA stellt die Pläne der Behörde und den Stand der Implementierung dar.
Die Fragen lauten unter anderem: Was hat der EU-Gesetzgeber sich bei der Konzeption der KI-Aufsicht gedacht? Wie ist die KI-Aufsicht ausgestaltet? Welche Lehren hat man aus der DS-GVO gezogen? Was ist die Aufgabe der Bundesnetzagentur in der Daten- und KI-Aufsicht? Was bedeutet Marktaufsicht? Wie wird das Zusammenspiel mit den anderen Aufsichtsbehörden bei DA und KI-VO im Datenschutz in Bund und Ländern ausgestaltet sein? Was ändert sich für die Unternehmen unter Aufsicht der BNetzA?
Zum Podcast bitte hier klicken.

Data Agenda Podcast Folge 79: Datenschutzmanagementsoftware im Praxischeck

Die rechtlichen Anforderungen an die Umsetzung der technisch-organisatorischen Maßnahmen an die Datenverarbeitung nach der DS-GVO werden immer komplexer. Vor diesem Hintergrund stellt sich Frage nach tauglicher Software immer drängender. Der Rechtsanwalt Michael Rohrlich und Datenschutzberater Marc Oliver Thoma testen regelmäßig derartige Tools. Im Podcast geben die Experten GDD-Geschäftsführer Andreas Jaspers und mir unter anderem Auskunft über die Arten solcher Werkzeuge, mögliche Einsatzfelder und die Frage, ob man die sie besser cloudbasiert oder on premise nutzen soll.
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