NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
11/2024

Levent Ferik

EDITORIAL

Die deutschen Datenschutzbehörden setzen sich bereits seit geraumer Zeit dafür ein, als Marktüberwachungsbehörden für die Umsetzung der KI-Verordnung benannt zu werden. Sie argumentieren, dass Datenschutz und künstliche Intelligenz (KI) eng miteinander verknüpft sind. Neben organisatorischen Aspekten betonen sie, dass ihre Expertise im Bereich Datenschutz eine effektive Überwachung des Einsatzes von KI sicherstellt. Bereits im Mai 2024 hatte die Datenschutzkonferenz (DSK) diese Position unterstützt, im Juli folgte der Europäische Datenschutzausschuss (EDSA).
Bei der Überwachung von KI-Systemen, wie sie gemäß Art. 70 der KI-Verordnung vorgesehen ist, geht es nicht nur um die technische Konformität wie bei Haushaltsgeräten. Ein wesentlicher Unterschied liegt darin, dass KI-Systeme nicht nur technische Standards erfüllen müssen, sondern auch potenzielle Auswirkungen auf Grundrechte und den Datenschutz zu berücksichtigen sind.
Es gibt jedoch auch Stimmen, die statt vieler einzelner Anlaufstellen eine bundesweit zuständige KI-Aufsichtsbehörde als „One-Stop-Shop" für Unternehmen als bessere Alternative zu den Datenschutzaufsichtsbehörden sehen. Eine EU-weit verbindliche und einheitliche Anwendung und Umsetzung schaffe Rechtssicherheit für die Unternehmen und verhindere „Gold Plating". Man erhofft sich dadurch effizient organisierte Prozesse und Strukturen für Vertrauen und Planungssicherheit bei den Unternehmen.
Aktuell wird diskutiert, welche Behörde in Deutschland die Aufsicht über KI-Systeme übernehmen soll. Die Bundesnetzagentur (BNetzA) wird dabei als vielversprechender Kandidat genannt. Aus Sicht der Wirtschaft spricht für die BNetzA, dass sie bereits umfangreiche Erfahrungen in der Aufsicht von Sektoren wie Telekommunikation und Strommarkt gesammelt hat. Zudem könnte sie als zentrale Behörde eine bundesweit einheitliche Auslegung der KI-Verordnung gewährleisten und als verlässliche Anlaufstelle für Unternehmen fungieren.
Der Landesbeauftragte für den Datenschutz Niedersachsen hat eine neue Stabsstelle für künstliche Intelligenz eingerichtet. Diese Stabsstelle soll die datenschutzrechtlichen Aspekte des zunehmenden Einsatzes von KI-Technologien überwachen. Ziel sei es, sicherzustellen, dass der Einsatz von KI mit den Datenschutzgesetzen vereinbar ist und die Grundrechte der Bürgerinnen und Bürger gewahrt bleiben.
Offenbar sind sich die Datenschutzaufsichtsbehörden selbst nicht sicher, wer das „Rennen macht", meint
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Leasing von Fahrrädern: Auftragsverarbeitung oder nicht?

Immer mehr Arbeitgeber bieten ihren Mitarbeitenden die Möglichkeit, Fahrräder zu leasen.

Foto: Kzenon, Adobe Stock

Dafür wird häufig ein Rahmenvertrag mit einem Leasinganbieter geschlossen, und bei Annahme des Angebots durch die Mitarbeitenden erfolgt ein Einzelvertrag. In diesem Zusammenhang werden auch personenbezogene Daten der Mitarbeitenden an den Leasinganbieter übermittelt. Hier kann sich die Frage stellen, ob dies als Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung (DS-GVO) zu bewerten ist.

Nach Art. 4 Nr. 8 DS-GVO ist ein Auftragsverarbeiter, wer personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet. Ein zentraler Punkt der Auftragsverarbeitung ist, dass der Auftragsverarbeiter die Daten ausschließlich auf Weisung des Verantwortlichen verarbeitet (Art. 29 DS-GVO). Zudem muss die Datenverarbeitung die Kerntätigkeit des Auftragsverarbeiters sein.

Beim Fahrrad-Leasing ist die Haupttätigkeit des Leasinganbieters der Abschluss von Leasingverträgen und nicht die Verarbeitung personenbezogener Daten. Diese ist lediglich ein „Nebenbestandteil" der Dienstleistung. Daher handelt es sich nicht um eine Auftragsverarbeitung im Sinne der DS-GVO, sondern um eine Übermittlung personenbezogener Daten, die zur Erfüllung des Leasingvertrags notwendig ist. Dies ist vergleichbar mit der Übermittlung von Beschäftigtendaten bei einer Hotelbuchung für eine Dienstreise – auch hier liegt keine Auftragsverarbeitung vor.

Die Verarbeitung personenbezogener Daten durch den Leasinganbieter ist daher kein Fall der Auftragsverarbeitung, und es ist kein Vertrag gemäß Art. 28 Abs. 3 DS-GVO erforderlich.

Foto: ImageFlow, Adobe Stock

Mitarbeiterexzess: Videoüberwachung durch Kollegen

Manchmal kann ein datenschutzrechtliches Fehlverhalten nicht dem Unternehmen oder Betrieb angelastet werden, nämlich dann, wenn Beschäftigte Daten für eigene private Zwecke verarbeiten und nicht zumindest in der Annahme, im Interesse des Arbeitgebers zu handeln.

Das kann z. B. dann der Fall sein, wenn Bankmitarbeiter:innen, die privat eine Wohnung vermieten, die Möglichkeit einer Bonitätsabfrage nutzen, um die Bonität eines möglichen Mieters abzufragen. Für solche Handlungen ist nicht mehr der Arbeitgeber verantwortlich, sondern die oder der Beschäftigte wird selbst zum Verantwortlichen und kann Adressat:in aufsichtsbehördlicher Maßnahmen werden.

Über eine andere Variante eines Mitarbeiterexzesses berichtet der LfDI Rheinland-Pfalz in seinem aktuellen Tätigkeitsbericht.

In einer Kommune installierte der Kassenverwalter eigenmächtig eine Überwachungskamera, um den Verdacht zu überprüfen, dass eine Kollegin durch Stornobuchungen Geld entwendete. Ohne die Behördenleitung zu informieren, erhärteten die Aufzeichnungen den Verdacht, und die Kollegin wurde fristlos entlassen.

Der LfDI stellte jedoch fest, dass der Kassenverwalter als datenschutzrechtlich Verantwortlicher agierte. Eine heimliche Videoüberwachung am Arbeitsplatz ist nur als letztes Mittel zulässig, wenn keine milderen Maßnahmen zur Aufklärung zur Verfügung stehen. Hier hätte das Fehlverhalten der Kollegin möglicherweise auch durch Protokolldaten nachgewiesen werden können, was die Videoüberwachung fragwürdig macht. Zudem lag keine Einwilligung der Betroffenen vor, und die Einwilligung der übrigen Mitarbeitenden kann aufgrund des Abhängigkeitsverhältnisses nicht als freiwillig angesehen werden.

Die entlassene Mitarbeiterin könnte die Kündigung vor Gericht anfechten und ein Verwertungsverbot der Aufnahmen fordern, da die Überwachung unverhältnismäßig war und von einer unbefugten Person initiiert wurde. Die endgültigen dienstlichen Konsequenzen überließ der LfDI der Behördenleitung.

Foto: Imillian, Adobe Stock

Schutz der Identität von Hinweisgeber*innen

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) Rheinland-Pfalz betont erneut (TB 2023, Ziffer 10.1), dass die Identität von Hinweisgeber*innen und Informant*innen grundsätzlich vertraulich zu behandeln ist.

Ihre Weitergabe darf nur unter bestimmten Voraussetzungen erfolgen, wie etwa

- mit ausdrücklicher Zustimmung oder
- wenn der Hinweis als Beweismittel erforderlich ist und
- sich der Inhalt nicht durch andere Mittel bestätigen lässt.
- Auch bei falschen Anschuldigungen mit schädigender Absicht kann die Identität offengelegt werden.

Weiter auf DataAgenda lesen

Foto: ZinetroN, Adobe Stock

IT-Sicherheitskennzeichen soll mehr Transparenz und Sicherheit schaffen

Mit dem IT-Sicherheitsgesetz 2.0 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen.

Das IT-Sicherheitskennzeichen soll Transparenz für Verbraucherinnen und Verbraucher schaffen, indem es grundlegende Sicherheitseigenschaften von IT-Produkten auf einen Blick erkennbar macht. Denn während immer mehr Alltagsgegenstände mit dem Internet und mit anderen smarten Dingen vernetzt werden, wird es für Verbraucherinnen und Verbraucher immer schwieriger zu beurteilen, welche Geräte und Dienste passende Sicherheitseigenschaften besitzen. Mit dem IT-Sicherheitskennzeichen möchte das BSI gleichzeitig ein Instrument schaffen, das es Herstellern leicht macht, ihre Produkte auf das bevorstehende EU-Gesetz zur Cyberresilienz, den „Cyber Resilience Act", vorzubereiten und bereits jetzt besonders am Markt besonders hervorzuheben. Die Kennzeichnung wird an Produkte und Dienste vergeben, die anerkannte Sicherheitsanforderungen erfüllen.

Das IT-Sicherheitskennzeichen wird vom BSI für Produkte oder Dienstleistungen erteilt, wenn der Hersteller die Konformität des Produkts mit bestimmten IT-Sicherheitsvorgaben vollständig geprüft und deren Erfüllung durch eine Herstellererklärung bestätigt hat. Die Beantragung ist freiwillig und ausschließlich im Rahmen der vom BSI definierten Produktkategorien möglich.

Die Sicherheitseigenschaften müssen während der Laufzeit des Kennzeichens aufrechterhalten werden. Das wird vom BSI stichprobenartig oder anlassbezogen überprüft. Sollten Abweichungen oder Sicherheitslücken auftreten, arbeitet das BSI vertraulich und partnerschaftlich mit den Herstellern zusammen, um den zugesicherten Produktzustand wiederherzustellen.

Verbraucherinnen wiederum können das IT-Sicherheitskennzeichen schnell und einfach nutzen können, um mehr über die IT-Sicherheit digitaler Produkte zu erfahren. Dazu muss der QR-Code im Online-Shop oder direkt auf der Verpackung gescannt werden, um die Produktinformationsseite des BSI aufzurufen.

Interessenkollision und Betriebliches Eingliederungsmanagement

Wenn es im Zusammenhang mit dem Datenschutz um das Thema „Interessenkollision“ geht, steht meist der Datenschutzbeauftragte im Fokus.

Foto: MQ-Illustrations, Adobe Stock

Dabei gibt es mittlerweile eine gefestigte Meinung und auch zahlreiche Entscheidungen, welche anderen Funktionen der Datenschutzbeauftragte (DSB) nicht in Personalunion ausüben sollte. Aber nicht nur hier kann eine Personalunion ein „No-Go“ sein. Eine Interessenkollision kann auch sehr relevant werden, wenn es um das Thema Betriebliches Eingliederungsmanagement (BEM) geht.
Beim betrieblichen Eingliederungsmanagement muss eine klare Trennung zwischen Personalverwaltung und BEM-Verfahren sichergestellt werden, um Datenschutz und Vertrauen zu gewährleisten. Beschäftigte, die innerhalb von zwölf Monaten länger als sechs Wochen krank sind, haben Anspruch auf ein BEM, um die Ursachen der Arbeitsunfähigkeit zu analysieren und zukünftige Fehlzeiten zu vermeiden.
Der Landesbeauftragte für den Datenschutz stellte fest, dass in einer Landesbehörde die Personalleiterin gleichzeitig als BEM-Beauftragte fungierte (TB 2023, Ziffer 6.2). Dies widerspricht der Intention des Gesetzgebers, der eine Trennung beider Rollen vorsieht, um Interessenkonflikte zu vermeiden. Informationen aus BEM-Gesprächen dürfen nicht in die Personalakte einfließen oder für Personalmaßnahmen verwendet werden, da dies das Vertrauen der Beschäftigten in das BEM schwächen und die Offenheit der Betroffenen beeinträchtigen könnte. Der LfDI empfiehlt daher, eine Person außerhalb des Personalbereichs als BEM-Beauftragte einzusetzen, um die Vertraulichkeit und Wirksamkeit des Verfahrens sicherzustellen.

Foto: ArchiVIZ, Adobe Stock

Risiken im Smarthome: IoT-Geräte, Smart Toys und Datenschutz

Fitnesstracker, Smartwatches, Fernseher, Kameras, Smart Toys und Sprachassistenten erleichtern unseren Alltag, bringen aber erhebliche Datenschutz- und Sicherheitsrisiken mit sich.

Diese „smarten" Geräte, die unter dem Begriff Internet der Dinge (Internet of Things, IoT) zusammengefasst werden, senden regelmäßig Daten ins Internet und automatisieren Prozesse wie die Temperatur- oder Lichtsteuerung.

Die zunehmende Vernetzung bringt jedoch Gefahren mit sich: Ungesicherte Geräte können Cyberkriminellen Zugang zum Heimnetzwerk ermöglichen, sensible Daten wie Gesundheitsinformationen abfangen oder die Kontrolle über Geräte und deren Sensoren übernehmen. Untersuchungen zeigen, dass täglich durchschnittlich zehn Angriffe auf jedes internetfähige IoT-Gerät erfolgen.

Laut dem „Cybersicherheitsmonitor 2024" des BSI herrscht bei vielen Nutzer*innen von Smarthome-Geräten eine Sorglosigkeit gegenüber Cyberkriminalität. Häufig sind diese Geräte nicht ausreichend gesichert, was das Risiko der Datenspionage erhöht.

Auch vernetzte Spielzeuge, sogenannte Smart Toys wie interaktive Teddybären oder Smartphone-gesteuerte Autos, bergen Risiken. Sie sammeln persönliche Daten der Kinder und können bei unzureichender Sicherheit von Cyberkriminellen missbraucht werden. Eltern sollten daher Zugriffsrechte überprüfen, sichere Passwörter verwenden, Netzwerkverbindungen bei Bedarf deaktivieren und regelmäßig Updates installieren.

Das EU-geförderte Projekt „#DigitaleVorbilder" des LfDI MV bietet Eltern in seiner Mediathek Videos und Materialien zum Thema Datenschutz und Sicherheit bei smarten Geräten und Spielzeug.

Der Cybersicherheitsmonitor 2024 des BSI untermauert dies:

- Selbst relevante Risiken sind nur einer Minderheit bekannt: 42 Prozent der Befragten haben z. B. schon einmal davon gehört, dass auch Smarthome-Geräte von einer Infektion mit Schadsoftware betroffen sein können.
- Bei der Nutzung von Smarthome-Geräten werden nur wenige Schutzmaßnahmen umgesetzt: Etwa vier von zehn Smart-Speaker-Nutzerinnen und -Nutzer installieren beispielsweise regelmäßig Updates – manuell oder automatisch.

13. GDD-Winter-Workshop

für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

27.–28. Januar 2025 | Garmisch Partenkirchen

Schwerpunkte:

- ✓ Aktuelle Entwicklungen im Datenschutz – im Schwerpunkt: Entwurf Neues Gesetz zu Beschäftigten-Daten
- ✓ Was der Datenschutz von der KI-VO wissen muss
- ✓ Deep Dive KI-VO: Das gilt im Februar 2025
- ✓ Konzepte zur Umsetzung von KI-Kompetenz im Unternehmen zwischen KI-VO und DS-GVO
- ✓ Der EuGH zum Schufascore – Reichweite der Entscheidung für die Datenschutz-Praxis insbesondere bei KI

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Wolfilser, Adobe Stock

Datenschutz bei funkbasierten Verbrauchszählern

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Orientierungshilfe zur datenschutzkonformen Nutzung von funkbasierten Strom-, Wasser- und Heizungszählern veröffentlicht (Datenverarbeitung im Zusammenhang mit funkbasierten Zählern ⬇).

Hintergrund ist die zunehmende Verunsicherung von Verbraucherinnen und Verbrauchern, Hausverwaltungen und Herstellern hinsichtlich des Schutzes und der Verarbeitung von Verbrauchsdaten, die von den neuen Zählern erfasst werden.
Die flächendeckende Einführung dieser Zähler soll Bürger*innen helfen, ihren Energieverbrauch besser zu überwachen und Einsparpotenziale frühzeitig zu erkennen. Gleichzeitig werfen die neue Technik und die damit verbundene Datenübertragung Fragen zum Datenschutz auf, insbesondere zur Rechtmäßigkeit der Erhebung und Nutzung der Daten.
Die Orientierungshilfe klärt diese Fragen und gibt rechtliche Leitlinien für Eigentümer*innen, Hausverwaltungen, Energieversorger und Ableseunternehmen. Erklärtes Ziel ist es, den technischen Fortschritt zu fördern, ohne den Datenschutz zu vernachlässigen.

EuGH: Datenschutzaufsichtsbehörden dürfen nach eigenem Ermessen einschreiten

Der Europäische Gerichtshof (EuGH) hat in der Rechtssache C-768/21 den Handlungsspielraum der Datenschutzaufsichtsbehörden bei der Durchsetzung der Datenschutz-Grundverordnung (DS-GVO) präzisiert.

Foto: Stockwerk-Fotodesign, Adobe Stock

Auslöser des Verfahrens war eine Beschwerde gegen eine Sparkasse beim Hessischen Datenschutzbeauftragten, die vom Verwaltungsgericht Wiesbaden an den EuGH zur Vorabentscheidung weitergeleitet wurde. Im Kern des Verfahrens ging es um die Frage, ob Betroffene einen Anspruch auf bestimmte Maßnahmen durch die Aufsichtsbehörden haben, wenn ein Datenschutzverstoß festgestellt wurde.

Der EuGH entschied, dass Datenschutzbehörden, selbst wenn sie einen Verstoß gegen den Schutz personenbezogener Daten feststellen, nicht zwangsläufig verpflichtet sind, Sanktionen wie Geldbußen zu verhängen. Solche Maßnahmen sind nur dann erforderlich, wenn sie notwendig sind, um die festgestellte Unzulänglichkeit zu beheben und die Einhaltung der DS-GVO sicherzustellen. Dies gilt insbesondere in den Fällen, in denen die verantwortliche Stelle nach Bekanntwerden des Verstoßes von sich aus Maßnahmen ergreift, um den Datenschutzverstoß abzustellen und zukünftige Verstöße zu verhindern.

Das Urteil räumt den Aufsichtsbehörden ein weites Ermessen ein, wie sie bei Verstößen vorgehen wollen. Gleichzeitig wird ihr Handlungsspielraum durch das Ziel der DS-GVO, ein hohes und einheitliches Schutzniveau für personenbezogene Daten zu gewährleisten, begrenzt, sodass im Wege einer Einzelfallprüfung dem konkreten Fall angemessene und verhältnismäßige Maßnahmen ergriffen werden können.

Handlungsempfehlung zum Einsatz von KI in Schulen

Die Kultusministerkonferenz (KMK) hat in Berlin eine Handlungsempfehlung zum Einsatz von künstlicher Intelligenz (KI) in Schulen verabschiedet. Ziel ist es, den konstruktiven und kritischen Umgang mit KI in schulischen Prozessen zu fördern.

Foto: Patrick, Adobe Stock

Die Präsidentin der Kultusministerkonferenz 2024, Christine Streichert-Clivot, unterstreicht die wachsende Bedeutung von KI im Bildungsbereich. „Schule muss KI gezielt einsetzen, um das Lernen zu fördern und gleichzeitig ihre Auswirkungen auf die Gesellschaft zu thematisieren“, so die saarländische Bildungsministerin. KI-basierte Anwendungen in Kinderzimmern erforderten altersgerechte Lernkonzepte, um Schülerinnen und Schüler fit für die digitale Zukunft zu machen. Zudem müsse KI auch in der Lehrkräftefortbildung verankert werden.

Wichtige Punkte der Empfehlung sind:

Einfluss von KI auf das Lernen: KI soll Lehrkräfte unterstützen und personalisierte Lernumgebungen schaffen.

Prüfungskultur: Prüfungen sollen angepasst werden, um die KI-Kompetenzen der Schülerinnen und Schüler fair zu bewerten.

Lehrkräftefortbildung: Lehrkräfte sollen gezielt im Umgang mit KI geschult werden.

Rechtlicher Rahmen: Klare Regelungen zum Datenschutz und zum Einsatz von KI sollen etabliert werden.

Chancengerechtigkeit: Alle Lernenden sollen Zugang zu KI-Kompetenzen erhalten.

Die Empfehlungen stützen sich auf Vorarbeiten der KMK und wissenschaftliche Expertise.

Die vollständige Handlungsempfehlung finden Sie hier.

Data Agenda Podcast Folge 59a: KI-Stimme-Recht. Das geht mit digitalen Stimmen

Mit Hilfe künstlicher Intelligenz kann man menschlich klingende Stimmen künstlich erzeugen und existierende Stimmen synthetisch kopieren. So kann man Geld einsparen ohne menschliche Sprecher zu ersetzen, sagt Professor Dr. Stefan Sporn. Ein Data-Agenda-Podcast über ein neues Geschäftsmodell und technische Möglichkeiten von KI, aber auch über rechtliche und ethische Grenzen der neuen Technik.

Wer sich einen Eindruck davon verschaffen möchte, ob KI Stefan Sporn und Rolf Schwartmann mit ihren persönlichen Stimmen englisch sprechen lassen kann, muss den Podcast zu Ende hören.
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