NEWS BOX DATENSCHUTZ

AUSGABE
12/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Am 19. Oktober 2022 hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI), Herr Dr. Lutz Hasse, seinen 4. Tätigkeitsbericht zum Datenschutz nach der Datenschutz-Grundverordnung (DS-GVO) veröffentlicht.

Der TLfDI berichtet, dass die Corona-Pandemie auch im Berichtsjahr 2021 das beherrschende Thema beim TLfDI gewesen sei. Viele Verantwortliche in Thüringen haben sich vor der Herausforderung gesehen, dass eine große Anzahl der Leistungen nun in der aus Infektionsschutzgründen gebotenen Distanz erbracht werden mussten, sei es die Arbeitsleistung von Beschäftigten aus dem Homeoffice oder der Schulunterricht, so die Behörde. Es habe daher zahlreiche Beratungsanfragen von Verantwortlichen zu digitalen Anwendungen und auch zur datenschutzgerechten Gestaltung der 3G-Nachweise gegeben.

Nachfolgend finden Sie in dieser Ausgabe der Datenschutz Newsbox eine Auswahl praxisrelevanter Fälle aus dem öffentlichen Bereich und auch aus dem nicht-öffentlichen Bereich.

Fälle aus dem öffentlichen Bereich:
1. Unzulässige Videoüberwachung im Kindergarten
2. Datenschutzkonforme Schulnotenverkündung
3. Bußgeld gegen Elternvertreter?

Fälle aus dem nicht-öffentlichen Bereich:
1. Keine Initiativbewerbungen möglich, wegen „Datenschutzbedenken"?
2. Beschäftigtendatenschutz: Steckbrief von Ungeimpften
3. Mitarbeiterexzess: Geldbußen gegen Beschäftigte

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: vegefox.com, Adobe Stock

Kompakte Transparenz: Datenschutz-Icons

Nur etwa jeder vierte Nutzer liest die Texte mit den Nutzungsbedingungen der Internetdienste durch, bevor er sich bei diesen Diensten anmeldet bzw. die Websites nutzt. Einerseits bestimmt Schnelllebigkeit den Alltag vieler Menschen, sodass die Aufmerksamkeit zu einer kostbaren Ressource wird. Andererseits führt die Komplexität von im Hintergrund laufenden Datenverarbeitungen auch bei so „trivialen Dingen" wie dem Besuch einer Webseite dazu, dass der Nutzer über diese Vielzahl von Datenverarbeitungen informiert sein müsste, wenn der Verantwortliche bspw. seinen datenschutzrechtlichen Transparenzanforderungen nachkommen soll.
Um dies bewerkstelligen zu können, hat das Bundesministerium der Justiz bereits vor etlichen Jahren vorgeschlagen, dass neben detaillierteren Hinweisen auch eine weitaus kompaktere Form eines sog. „One-Pagers" angeboten werden könnte.

Eine Möglichkeit der Verdichtung von notwendigen Informationen auf ein noch kompakteres Maß ist sogar in der DS-GVO und seinen Erwägungsgründen enthalten. Die DS-GVO selbst sieht die Verwendung von Bildsymbolen in Art. 12 Abs. 8 und Erwägungsgrund 166 vor.
In diesem Zusammenhang hatte der LfDI Baden-Württemberg 2021 einen Aufruf, verbunden mit einem Wettbewerb, gestartet. Interessierte sollten Icons gestalten, die die Punkte einer Datenschutzinformation gemäß Artikel 13 und 14 der DS-GVO verbildlichen und so die wichtigsten und häufigsten Datenschutzbegriffe und -hinweise auf einen Blick begreifbar machen. Es wurden Symbole für folgende Begriffe gesucht:

- „Verantwortlicher",
- „(personenbezogene) Daten",
- „Zweck",
- „Rechtsgrundlage", mit Icons zu „Einwilligung" und deren „Widerruf", sowie zu „Vertrag",
- „rechtliche Verpflichtung" und „berechtigtes Interesse",
- „Schutz", mit Icons zu den Betroffenenrechten „Auskunft", „Berichtigung", „Einschränkung", „Löschung" sowie „Beschwerde (bei der Aufsichtsbehörde)",
- „Datenschutzbeauftragte*r",
- „Aufsichtsbehörde",
- „Weitergabe" mit Icons zu „Empfänger" und „Übermittlung in Drittstaaten".

Nun präsentiert der LfDI BW das Ergebnis des Wettbewerbs auf seiner Internetseite. Die Datenschutz-Icons stehen für alle Interessierten in Farbe und s/w für Print- und digitale Nutzung kostenlos zum Download zur Verfügung:

Foto: Egor, Adobe Stock

Databreach-Management: EDSA aktualisiert Leitlinien

Angriffe von außen sowie internes Fehlverhalten können trotz ausgiebiger Maßnahmen zur Datensicherheit zu Verletzungen des Schutzes personenbezogener Daten führen. Wenn ein solcher Datenschutzvorfall entsteht und daraus ein Risiko für die Rechte und Freiheiten der betroffenen Personen resultiert, muss diese Datenpanne unverzüglich und möglichst binnen 72 Stunden an die Aufsichtsbehörde gemeldet werden.
Sofern der Verantwortliche nicht bereits im Vorfeld einen solchen Vorfall vorausgedacht sowie die internen und externen Meldewege und Meldeprozesse festgelegt hat und zudem die Verantwortlichkeiten innerhalb des Prozesses festgelegt hat, wird es schwierig, in dieser Zeit eine Meldung nach Maßgabe des Gesetzgebers durchzuführen.

Mit der Meldung einer Datenpanne im Sinne von Art. 33 DS-GVO bzw. mit der Benachrichtigung der Betroffenen nach Art. 34 DS-GVO ist es für den Verantwortlichen aber nicht getan. Auch nach der Meldung hat der Verantwortliche Hausaufgaben zu erledigen.

Zu diesem wichtigen Themenkomplex hat der Europäische Datenschutzausschuss (EDSA) seine Leitlinien (Benachrichtigungen bei Datenschutzverletzungen) veröffentlicht bzw. aktualisiert und führt dazu eine öffentliche Konsultation durch. Der Europäische Datenschutzausschuss hatte die mit der Datenschutz-Grundverordnung zusammenhängenden Leitlinien der Artikel-29-Datenschutzgruppe bei seiner ersten Plenarsitzung im Jahre 2018 bestätigt.

Die Aktualisierung und die öffentliche Konsultation betreffen im wesentlichen Absatz 73 der Leitlinien (im Dokument gelb markiert). Dieser Absatz adressiert die Klarstellung von Meldepflichten von nicht in der EU niedergelassenen Unternehmen. Solche Kommentare sollten bis spätestens 29. November 2022 unter Verwendung des bereitgestellten Formulars eingereicht werden.

Auch wenn die Änderungen in der Leitlinie daher eher redaktioneller Art sein dürften, können Verantwortlichen die Aktualisierung zum Anlass für eine Evaluation der eigenen Prozesse und Policies rund um das Thema nehmen.

11. GDD-Winter-Workshop

für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

30.–31. Januar 2023 | Garmisch Partenkirchen

Praxisthemen:

- ✓ Aktuelle Entwicklungen im Datenschutz
- ✓ Datenschutz und künstliche Intelligenz
- ✓ Datenschutz bei begrenzten Ressourcen rechtssicher und pragmatisch umsetzen
- ✓ Aktuelles zum Beschäftigen-Datenschutz

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: DatenschutzStockfoto, Adobe Stock

BayLfD möchte beim „Bändigen" von Cookies helfen

Betreiber von Webseiten oder Hersteller von Apps für mobile Endgeräte (z.B. Smartphone, Tablet) müssen als Verantwortliche sicherstellen, dass bei der Verarbeitung personenbezogener Daten alle Vorgaben DS-GVO eingehalten werden. Sie sind zugleich Anbieter von Telemediendiensten nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG, hier: § 2 Abs. 2 Nr. 1), welches die Nutzung von Cookies und ähnlichen Technologien zum Ablegen oder Auslesen von Informationen auf den Systemen regelt; solche Technologien werden häufig zur Wiedererkennung von Nutzenden verwendet und sind inzwischen extrem weit verbreitet.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden der Länder und des Bundes (Datenschutzkonferenz, DSK) hat im Dezember 2021 mit der „Orientierungshilfe der Aufsichtsbehörden für die Anbieter:innen von Telemedien (OH Telemedien 2021)" rechtliche und technische Erläuterungen zur Anwendung der DS-GVO und des TTDSG gegeben.

Auch der Bayerische Landesbeauftragte für den Datenschutz (BayLDA) hat zu diesem Thema bereits einiges an Hilfestellung veröffentlicht. Die Kurz-Information 36 „Cookie-Einwilligungen auf Webseiten bayerischer öffentlicher Stellen" bietet Basics, die die aktuelle Kurz-Information 42 „Externe Schriftarten auf Webseiten bayerischer öffentlicher Stellen" sowie Hinweise zu einem häufig eingesetzten Dienst und damit verbundenen Detailproblemen geben. In der umfassenden Orientierungshilfe „Bayerische öffentliche Stellen und Telemedien" sind insbesondere die rechtlichen Rahmenbedingungen für Einwilligungsdialoge eingehend dargestellt.

Bei der aktuellsten Publikation, welche als „Wie bekomme ich die Cookies auf meiner Homepage unter Kontrolle? Tutorial für bayerische öffentliche Stellen und alle anderen Interessierten" betitelt ist, handelt es sich um ein Tutorial. Der Name ist hier Programm, sodass nicht nur öffentliche Stellen, sondern auch Verantwortliche außerhalb der Zuständigkeit des BayLDA wertvolle Tipps erhalten, wie sie die kleinen Hilfsmittel einsetzen können, wenn sie etwas über die Reichweite des eigenen Angebots erfahren möchten oder einen kommerziellen Webseitengestalter beauftragt haben, der nicht ohne Cookies benötigende Webframeworks auszukommen meint, oder gar die Ambition haben, gänzlich cookiefreie Dienste anzubieten.

Foto: Rawpixel.com, Adobe Stock

Keine Initiativbewerbungen möglich, wegen „Datenschutz-bedenken“?

Es kommt nicht selten vor, dass in Unternehmen bestimmte Vorhaben abgeblockt werden und dies lapidar mit dem Hinweis auf „den Datenschutz“ begründet wird. Manchmal sind die Datenschutzbedenken vorgeschoben, aber manchmal sprechen im Kern tatsächlich datenschutzrechtliche Erwägungen dagegen – jedoch sind diese Argumente leider nicht immer nachvollziehbar und verständlich vorgetragen.

Weiter auf DataAgenda lesen

Beschäftigtendatenschutz: Steckbrief von Ungeimpften

Der ebenfalls im 4. Tätigkeitsbericht zum Datenschutz nach der DS-GVO vorgestellte Fall des TLfDI, der sich im Umfeld von Corona-Maßnahmen abspielt (Ziffer 3.1), die in jüngster Vergangenheit vielfach in Unternehmen durchgeführt wurden, führt dem Interessierten vor Augen, was bei der Verarbeitung von Gesundheitsdaten beachten werden sollte, wenn diese über eine Einwilligung der betroffenen Beschäftigten legitimiert werden sollen.

Weiter auf DataAgenda lesen

Foto: narong, Adobe Stock

Unternehmen hadern mit der DS-GVO

Nach einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom unter 503 Unternehmen ab 20 Beschäftigten in Deutschland scheint ein Großteil der Unternehmen mit der Umsetzung der DS-GVO im eigenen Hause unzufrieden – sehen jedoch diese Defizite nicht als etwas, was sie selbst zu verantworten haben.

Foto: photoschmidt, Adobe Stock

Vielmehr seien die Defizite das Ergebnis von Rechtsunsicherheit und einer widersprüchlichen Auslegung der Datenschutzvorgaben innerhalb Europas und zwischen den Bundesländern.

Das Erscheinen neuer Guidelines sehen 88 Prozent der befragten Unternehmen als weiteren Grund für die internen Hemmnisse einer weitreichenderen Umsetzung an. Das Erscheinen neuer Guidelines kann aber auch als Indikator dafür gesehen werden, dass die Aufsichtsbehörden die Rechtsvorschriften mit „Leben füllen" und die Anwendbarkeit dadurch steigern und damit eigentlich die Rechtsunsicherheiten eliminieren, die 78 Prozent als Hemmnis sehen.

77 Prozent geben an, dass durch das Ausrollen neuer Tools immer wieder eine neue Prüfung in Gang gesetzt wird. Auch das dürfte „kein Bug, sondern ein Feature" der DS-GVO sein. Das Versprechen der DS-GVO ist bspw. nicht, dass eine einmal durchgeführte Risikoanalyse oder Datenschutz-Folgenabschätzung auf alle erdenklichen Verarbeitungen oder Tools passt.
40 Prozent der befragten Unternehmen kritisieren, dass ihnen die DS-GVO keinen Wettbewerbsvorteil auf dem internationalen Markt für das eigene Unternehmen gebracht habe – und 30 Prozent sehen sogar Wettbewerbsnachteile.

Die weiteren Ergebnisse finden Sie in der Präsentation: „Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers" des BITKOM.

Foto: tippapatt, Adobe Stock

Mitarbeiterexzess: Geldbußen gegen Beschäftigte

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

In bestimmten Fällen kann aber auch der Arbeitnehmer 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 DSK hat in seiner Entschließung 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.

In seinem Tätigkeitsbericht 2021 schildert der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit verschiedene Fälle des Fehlverhaltens von Beschäftigten, deren Datenschutzverstöße von der Behörde mittels Festsetzung einer Geldbuße geahndet wurden. Damit dürfte das Verhalten der Beschäftigten als Fall des sog. Mitarbeiterexzesses zu bewerten sein, die dazu führen können, dass Geldbußen direkt gegen die Beschäftigten des Verantwortlichen verhängt werden.

Weiter auf DataAgenda lesen

Foto: hkama, Adobe Stock

Lage der IT-Sicherheit in Deutschland: Bedrohung so hoch wie noch nie

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes. Ihre Aufgabe ist es, Deutschland digital sicherzumachen.
Wie jedes Jahr legt das Bundesamt für Sicherheit in der Informationstechnik (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 Cyber-Raum vor.

Nach der Einschätzung des BSI habe sich im Berichtszeitraum die bereits zuvor angespannte Lage weiter zugespitzt. Die Bedrohung im Cyber-Raum sei damit so hoch wie nie. Im Berichtszeitraum sei – wie schon im Vorjahr – eine hohe Bedrohung durch Cybercrime beobachtet worden. Ransomware wird als die Hauptbedrohung (siehe Kapitel Ransomware, S. 13), besonders für Unternehmen eingeschätzt.

Nach Auffassung der Cyber-Sicherheitsbehörde kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine, zum Beispiel durch Hacktivismus, insbesondere mittels Distributed-Denial-of-Service-Angriffen (DDoS-Angriffen), und Kollateralschäden bei Cyber-Sabotage-Angriffen im Rahmen des Krieges hinzu.

Sowohl durch Cybercrime als auch durch Cyber-Aktivitäten im Rahmen des Kriegs in der Ukraine habe es darüber hinaus im Berichtszeitraum Störungen von IT-Lieferketten gegeben. Eine Erhöhung der Resilienz gegenüber Cyber-Angriffen und technischen Störungen ist daher eine Hauptaufgabe für alle beteiligten Akteure in Staat, Wirtschaft und Gesellschaft.

Der Bericht zur Lage der IT-Sicherheit in Deutschland 2022 beschreibt und analysiert die aktuelle IT-Sicherheitslage, auch anhand konkreter Beispiele und Vorfälle. Verantwortliche und Interessierte können aus den Beobachtungen und Lösungsansätzen des BSI Maßnahmen zur Verbesserung der eigenen IT-Sicherheit ableiten.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Foto: amazing studio, Adobe Stock

Unzulässige Videoüberwachung im Kindergarten

Als gutes Beispiel, wie Verantwortliche die Frage der Zulässigkeit einer geplanten Videoüberwachung lösen können, kann der unter Ziffer 2.14 geschilderte Fall „Videoüberwachung im Kindergarten“ im Tätigkeitsbericht für das Jahr 2021 des TLfDI genannt werden.

Bevor eine Videokamera aktiviert wird, ist für jede Verarbeitung eindeutig zu bestimmen und festzulegen, welcher Zweck mit der Videoüberwachung erreicht werden soll. Eine Videoüberwachung kann beispielsweise eingesetzt werden, um vor Einbrüchen, Diebstählen, Vandalismus (Eigentumsschutz) oder Übergriffen (Personenschutz) zu schützen.
Die jeweiligen Zwecke sind für jede einzelne Kamera schriftlich zu dokumentieren und ins Verzeichnis der Verarbeitungstätigkeiten aufzunehmen (vgl. Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen).

Im konkreten Fall hatte ein Kindergarten als eine öffentliche Stelle in Thüringen beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) nachgefragt, ob eine geplante Videoüberwachung im öffentlichen Raum stattfinden dürfe.

Der Verantwortliche für den Kindergarten gab als konkrete Zwecke an:

- **Sicherheit der Kinder**: Im Kindergarten komme es immer wieder vor, dass Fremde diesen betreten würden, die kein Kind bringen oder abholen wollen (Postbote, Vertreter und andere). Kinder hätten das Grundstück des Kindergartens verlassen, ohne dass die Erzieher dies gesehen hätten.
- **Verhindern des Zutritts von „fremden Personen“**: Regelmäßige Belehrungen der Eltern, keine fremden Personen mit auf das Grundstück zu bringen oder Kinder ohne Abmeldung mit hinauszunehmen, hätten bisher nicht dazu geführt, dass diese Vorfälle seltener eintreten.

Der TLfDI prüft die Zulässigkeit des Verfahrens „lehrbuchmäßig“:

1. Zweck und Form der Videoüberwachung

Mit der gewählten „Speicherung der aufgenommenen Bilder“, handele es sich um eine Variante der Videoüberwachung, mit der nachträglich von einer oder einem Beschäftigten der öffentlichen Stelle die erfolgten Geschehnisse nur angesehen werden können, **nachdem** es bereits zu einem Vorfall gekommen ist. Damit könne bereits die Geeignetheit der Maßnahme verneint werden, da damit nicht verhindert werden könne, dass Kinder ohne Kenntnisnahme des Personals das Gelände verlassen.

Weiter auf DataAgenda lesen

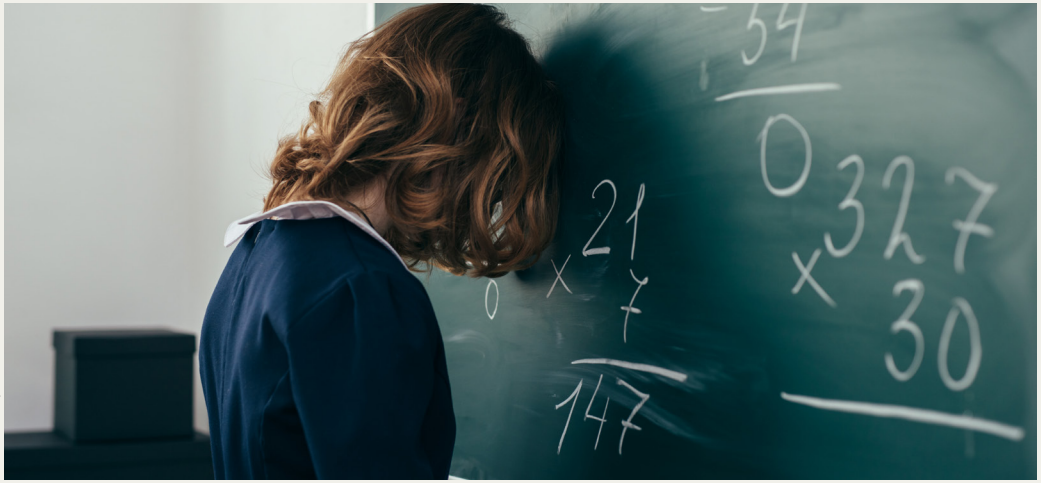

Foto: undrey, Adobe Stock

Datenschutzkonforme Schulnotenverkündung

Unter Ziffer 2.24 schilderte der TLfDI aus seinem aktuellen Tätigkeitsbericht einen Fall, der ggf. etwas polarisieren könnte.
Auf der einen Seite, wie so oft diejenigen, die „nichts dabei finden, wenn Schulnoten öffentlich, d.h. vor der ganzen Klasse vorgelesen (und ggf. auch kommentiert werden)“. Dabei dürften „Argumente“ wie bspw. „das hat uns früher auch nicht geschadet“ fallen.
Die berechtigte Frage ist dann andererseits jedoch, ob alles, was den betroffenen Personen früher nicht (unmittelbar) geschadet hat, auch tatsächlich nach heutiger Betrachtung noch richtig sein kann.

Weiter auf DataAgenda lesen

Bußgeld gegen Elternvertreter wegen WhatsApp-Nutzung?

Unter der Ziffer 2.25 bespricht der TLfDI, abseits der Probleme des „Unternehmens-Datenschutzrechts“ ein Thema, was auch für „Privatleute“, insbesondere für die sog. „Elternvertreter“ interessant sein dürfte.

Die wesentlichen Fragen, die adressiert werden, sind folgende:

1. Dürfen Elternvertreter in ihrer Funktion WhatsApp nutzen?

Ist es zulässig, dass sog. Elternvertreter im schulischen Kontext und bei der Organisation der Aufgaben, die das „gewählte Amt“ notwendig macht, auf den Messenger „WhatsApp“ zurückgreifen können?

Weiter auf DataAgenda lesen

Foto: itchaznong, Adobe Stock

Data Agenda Podcast Folge 24: Neue Aufgaben für den betrieblichen Datenschutz – Unternehmenshaftung für Künstliche Intelligenz

Künstliche Intelligenz ist nicht aufzuhalten und ihr Einsatz im Dienst des Menschen dürfte kaum verzichtbar sein. Aber wie geht man damit um, wenn beim Einsatz einer Maschine Schäden entstehen? Die EU-Kommission hat im September 2022 einen Entwurf zur Behandlung von Haftungsfragen beim Einsatz von Systemen künstlicher Intelligenz vorgelegt. Es muss ein fairer Rechtsrahmen geschaffen werden, der Ansprüche auf Schadensersatz für Mängel von smarten Anwendungen oder Produkten, etwa Roboter oder Anwendungen in Smart-Home-Systemen, regelt.

Wer als Geschädigter einen Schaden geltend macht, muss vor Gericht darlegen, was dessen Ursache ist und dass dem Schädiger ein Verschulden vorzuwerfen ist. Das ist aber mangels Einblick in die Technik grundsätzlich nicht möglich. Opfer wissen nicht, wie das Programm, das ihren Schaden möglicherweise verursacht hat, funktioniert. Mit welchen Daten wurde die KI trainiert und wie wurde sie überwacht und angewendet? Das entstehende Haftungsrecht ergänzt das vorhandene Recht und ist, insbesondere wenn es um datengetriebene Geschäftsmodelle geht, mit der DS-GVO verzahnt. Im DataAgenda-Podcast gibt Dr. Martin Kessen, Richter am Bundesgerichtshof, Auskunft über Grundzüge des Haftungsrechts, das für den betrieblichen Datenschutz Bedeutung erlangen wird.

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