NEWS BOX DATENSCHUTZ

AUSGABE
8/2022

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Datenschutz ist ein allgegenwärtiges Thema und durchdringt mittlerweile alle Lebensbereiche.

Wie passen beispielsweise Hundekot, Datenschutz und das Thema Vorratsdatenspeicherung zusammen?

Gibt es einen inneren Zusammenhang zwischen Falschparkern und Persönlichkeitsrechten?

Und was genau haben eigentlich Sitzheizungen in Autos mit dem Thema Datensicherheit und Hacking zu tun?

Kennt die Firma Amazon bald auch die Grundrisse der Wohnungen und Häuser der Kunden und was haben Saugroboter damit zu tun?

Bekommt der Kunde (Patient?) auf Wunsch (oder in Prime inkludiert) bald auch in Europa über Amazon ärztliche Konsultation und das Rezept hinterher?

Und hätte das Verwaltungsgericht Göttingen dem Antrag auf Namensänderung bei einem Kind auch dann zustimmen müssen, wenn der Name des Kindes „Siri“ gewesen wäre?

„Verpfeifen“ smarte Klingelanlagen mit Videoüberwachungsfunktionalität sowie Tesla-Fahrzeuge unbemerkt ihre Nutzer/Fahrer?

Viel Spaß beim Lesen der Antworten auf diese Fragen wünscht Ihnen
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: putilov_denis, Adobe Stock

Meldung einer Datenpanne im Rahmen einer Auftragsverarbeitung

Die Pflicht der Meldung nach Art. 33 Abs. 1 DS-GVO trifft nur datenschutzrechtlich „Verantwortliche“ im Sinne des Art. 4 Nr. 7 DS-GVO. Eine Sonderregelung besteht für Auftragsverarbeiter gegenüber dem Verantwortlichen, für den sie tätig sind. Nach Art. 33 Abs. 2 DS-GVO müssen sie Datenschutzverstöße dem Verantwortlichen melden. Grund ist vor allem, dass es sich dabei um Verstöße im Verantwortungsbereich des Verantwortlichen handelt, die dieser wiederum ggf. der Aufsichtsbehörde melden muss. Aus dem aktuellen Tätigkeitsbericht des LfDI (27. Tätigkeitsbericht, Ziffer 11.2) ergibt sich, dass es nicht bei allen Verantwortlichen und Auftragsverarbeitern die für das Zusammenspiel der einzelnen internen und externen Meldepflichten erforderlichen Prozesse gibt.

Weiter auf DataAgenda lesen

LDI NRW: Checkliste zur Datenschutzprüfung

Die Datenschutz-Grundverordnung (DS-GVO) überträgt dem Verantwortlichen bzw. Auftragsverarbeiter die Pflicht, durch organisatorische Maßnahmen die Einhaltung des Datenschutzes sicherzustellen. Wie bei der Umsetzung aller regulatorischen Vorgaben kommt dabei der klaren Definition und Zuordnung von Verantwortlichkeiten und Aufgaben eine entscheidende Bedeutung zu.
Die Herausforderung dabei besteht einerseits darin, dass die Umsetzung der Aufgaben aus der DS-GVO grundsätzlich unabhängig von Größe und Organisationsgrad der betroffenen Einheit, z.B. als kleines oder mittleres Unternehmen (KMU), Konzern oder Behörde, sicherzustellen und somit nicht disponibel ist. Andererseits unterliegt die konkrete interne Zuweisung von Kompetenzen, Rollen und operativen Verantwortlichkeiten der jeweiligen Situation im Unternehmen bzw. in der Behörde, und ist, in Abhängigkeit der Größe und räumlichen Verteilung der Geschäftsstrategie, den allgemeinen Steuerungs- und Führungsmodells und der individuellen Risikosituation anzupassen.

Weiter auf DataAgenda lesen

Foto: Riko Best, Adobe Stock

Datenschutzorganisationen prüfen und bewerten nach der Systematik der Aufsichtsbehörden

Ihr ständiger Begleiter im Datenschutz-Management

Datenschutzorganisationen prüfen und beurteilen mit begrenztem Zeitaufwand

Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit unseren Excel-Tools!

Ihre DS-GVO Umsetzung smart auditiert und visualisiert ab 249 €.

Bestellen Sie direkt unter: **datakontext.com**

DATAKONTEXT

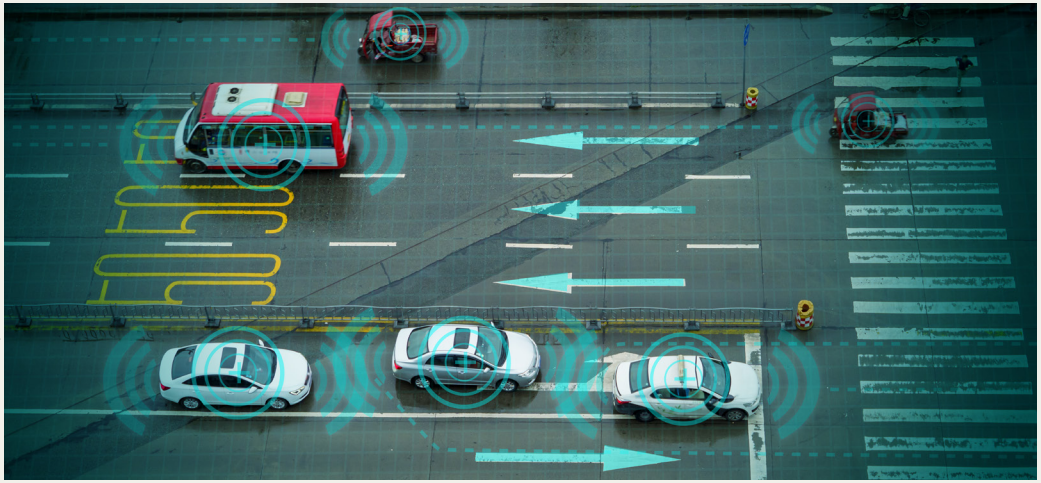

Foto: Have a nice day, Adobe Stock

Millionen-Bußgeld wegen nicht datenschutzkonformer Forschungsfahrten

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen hat gegen die Volkswagen Aktiengesellschaft eine Geldbuße nach Art. 83 Datenschutz-Grundverordnung (DS-GVO) in Höhe von 1,1 Millionen Euro festgesetzt.

Nach Angabe der LfD Niedersachsen sind Ursache des Bußgelds mehrere Verstöße gegen datenschutzrechtliche Bestimmungen in Zusammenhang mit dem Einsatz eines Dienstleisters bei Forschungsfahrten für ein Fahrassistenzsystem zur Vermeidung von Verkehrsunfällen. Das Unternehmen habe umfassend mit der LfD Niedersachsen kooperiert und den Bußgeldbescheid akzeptiert.

Im Fokus der datenschutzrechtlichen Verfehlungen der Volkswagen AG standen folgende Aspekte:

- keine Information betroffener Personen (Art. 13, 14 DS-GVO);
- keine Vereinbarung zur Auftragsverarbeitung (Art. 28 DS-GVO);
- Datenschutz-Folgenabschätzung nicht vorhanden (Art. 35 DS-GVO);
- Verzeichnis der Verarbeitungstätigkeiten unvollständig (Art. 30 DS-GVO).

VW setzte im Jahre 2019 ein Erprobungsfahrzeug ein. Das Fahrzeug wurde eingesetzt, um die Funktionsfähigkeit eines Fahrassistenzsystems zur Vermeidung von Verkehrsunfällen zu testen und zu trainieren. Unter anderem zur Fehleranalyse wurde das Verkehrsgeschehen um das Fahrzeug herum aufgezeichnet. Jedoch fehlten am Fahrzeug Hinweise bzgl. der Kameraaufzeichnungen sowie weitere Informationen für die datenschutzrechtlich Betroffenen, in diesem Fall die anderen Verkehrsteilnehmenden. Erschwerend kam hinzu, dass Volkswagen keinen Auftragsverarbeitungsvertrag mit dem Unternehmen abgeschlossen hatte, das die Fahrten durchführte. Eine erforderlich gehaltene Datenschutz-Folgenabschätzung (DSFA) nach Artikel 35 DS-GVO konnte ebenfalls nicht vorgelegt werden. Die Durchführung eines DSFA wäre aber nach Auffassung der Aufsichtsbehörde notwendig gewesen, um vor Beginn einer solchen Verarbeitung mögliche Risiken und deren Eindämmung bewerten zu können. Schließlich fehlte auch eine Erläuterung der technischen und organisatorischen Schutzmaßnahmen im Verzeichnis der Verarbeitungstätigkeiten, was einen Verstoß gegen die Dokumentationspflichten nach Artikel 30 DS-GVO darstellte.

Quelle: LfD Niedersachsen

Foto: Sergey Kohl, Adobe Stock

„Wächter-Modus" von Tesla-Fahrzeugen in der Kritik

Die Firma Tesla bewirbt ihre Fahrzeuge unter anderem damit, dass diese mehrere erweiterte Schutzfunktionen bieten, die einfach zu aktivieren sind. Über den Touchscreen des Fahrzeugs wird dem Fahrer bspw. Zugriff über „Fahrzeug"> „Sicherheit" auf die einzelnen Funktionen gewährt, um sie einzuschalten.
Eines dieser Funktionen ist der sog. „Wächter-Modus", den Tesla auf seiner Webseite wie folgt beschreibt:
„Der Wächter-Modus ist eine Funktion, mit der Sie verdächtige Aktivitäten rund um Ihren Tesla erfassen können, wenn er an bestimmten Orten geparkt und abgeschlossen ist. Wenn verdächtige Bewegungen erkannt werden, reagiert Ihr Fahrzeug entsprechend der Schwere der Bedrohung. Wird eine erhebliche Bedrohung erkannt, beginnen die Kameras in Ihrem Fahrzeug mit der Aufzeichnung, und die Alarmanlage wird aktiviert. Gleichzeitig erhalten Sie von Ihrer Tesla App eine Benachrichtigung, dass ein Vorfall stattgefunden hat.

[...] *Hinweis: Es liegt in Ihrer alleinigen Verantwortung, alle örtlichen Vorschriften und Eigentumsbeschränkungen hinsichtlich der Verwendung von Kameras zu beachten und einzuhalten.* [...]"

Genau diese Funktion hat den Unmut der Verbraucherzentrale Bundesverband (vzbv) erregt. Der vzbw geht davon aus, dass die Aktivierung des Wächter-Modus im öffentlichen Raum gegen das Datenschutzrecht verstößt und dass Fahrzeughalter:innen bei Nutzung der Funktion des Wächter-Modus zur Einhaltung der Vorschriften der Datenschutzgrundverordnung verpflichtet sind und bei Verstößen ein Bußgeld riskieren. Mit dem Wächter-Modus werde die Umgebung des Fahrzeugs kontinuierlich durch Kameras überwacht.
Der Verbraucherzentrale Bundesverband hat daher beim Landgericht Berlin Klage gegen Tesla erhoben. Der Autokonzern verschweige nämlich genau dieses Risiko bzw. kläre über diesen Umstand nicht auf. Werde der Wächter-Modus bei geparkten Autos aktiviert, würden mehrere am Fahrzeug angebrachte Kameras die Umgebung permanent aufzeichnen. Davon seien dann auch unbeteiligte Passant:innen betroffen. In bestimmten Fällen würden die Aufnahmen im Fahrzeug gespeichert. Damit handele es sich um die Verarbeitung personenbezogener Daten, die der DS-GVO unterliegen, so der vzbv. Zudem sei die anlasslose Aufzeichnung des Geschehens im Fahrzeugumfeld unzulässig. Die rechtskonforme Nutzung der Funktion des Wächter-Modus im öffentlichen Raum ist nach Ansicht des vzbv damit nicht möglich.

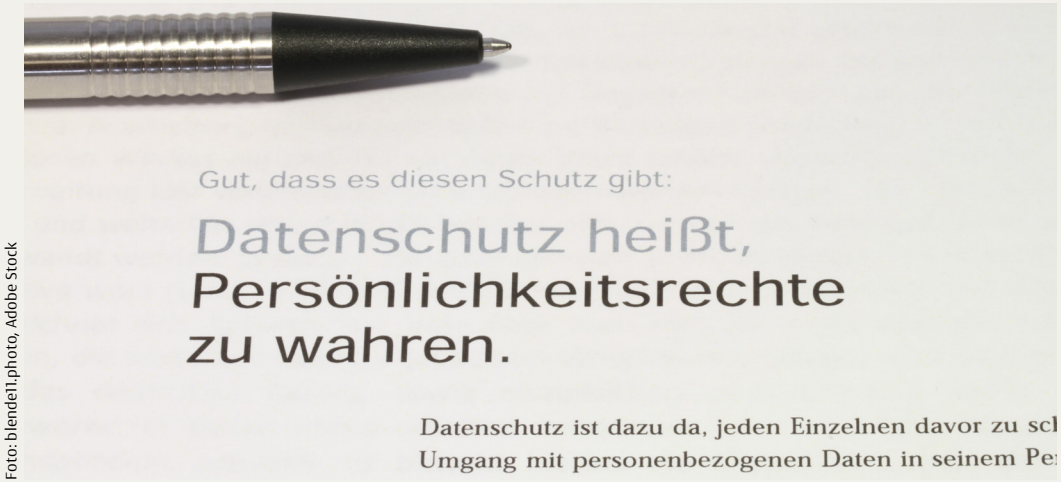

Foto: blende11.photo, Adobe Stock

Handlungsoptionen und Erfolgsaussichten für Betroffene von Datenschutzverstößen

Die Einführung der DS-GVO geht mit einer bewussten Stärkung der Betroffenenrechte einher. „Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen“ heißt es daher ausdrücklich in Erwägungsgrund (ErwGr) Nr. 11.
Hauptpfeiler der neuen Betroffenenrechte sind neben dem strengeren Haftungsregime und den neu eingeführten Einzelansprüchen vor allem die ausgeweiteten Transparenzpflichten bei der Datenverarbeitung. Art. 13 DS-GVO widmet sich den Informationspflichten bei der Direkterhebung, Art. 14 ist das Pendant bei Erhebung von Daten bei Dritten. Die betroffene Person soll die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erhalten (Art. 12 Abs. 1 Satz 1 DS-GVO) und dies stets unentgeltlich (Art. 12 Abs. 5).

Es ist aber nicht garantiert, dass Verantwortliche die Betroffenenrechte beachten oder ihnen die Inanspruchnahme dieser Rechte so einfach wie möglich machen. Es dürfte nicht übertrieben sein, dass sich die meisten der Aufsätze oder Beiträge den Betroffenenrechten aus dem Blickwinkel nähern, wie diese aus der Perspektive des Verantwortlichen in den Grenzen des rechtlich machbaren „sinnvoll begrenzt“ werden könnten. Die wenigsten Beiträge betrachten die Betroffenenrechte aus der Perspektive des Betroffenen.
Die jüngste Publikation des Netzwerks Datenschutzexpertise macht jedoch genau dies. In der Veröffentlichung mit dem Titel „**Betroffen von Datenschutzverstößen – Was kann ich tun? Handlungsoptionen und Erfolgsaussichten“** schildern die Autoren, warum es wichtig ist, dass Betroffene darauf Einfluss nehmen können, dass ihre Datenschutzrechte beachtet werden und stellen Möglichkeiten dar, welche Erfolgschancen damit einhergehen.
Konkret geht es insbesondere um folgende Mechanismen:

- Wahrnehmung der eigenen Rechte direkt gegenüber dem Verantwortlichen und dessen Datenschutzbeauftragten;
- Beschwerde bei den Datenschutzaufsichtsbehörden;
- Einschaltung von Verbraucherzentralen;
- Gang in die Öffentlichkeit.

Die Publikation zeigt, dass für den „Normalbürger“ der Weg zur Verteidigung seines „Rechts auf informationelle Selbstbestimmung“ schwierig bleibt, zumal es sich zumeist um komplexe technische Vorgänge handelt und die Rechtslage unübersichtlich ist. Dann sind Betroffene auf externe, qualifizierte oder gar professionelle Hilfe angewiesen.

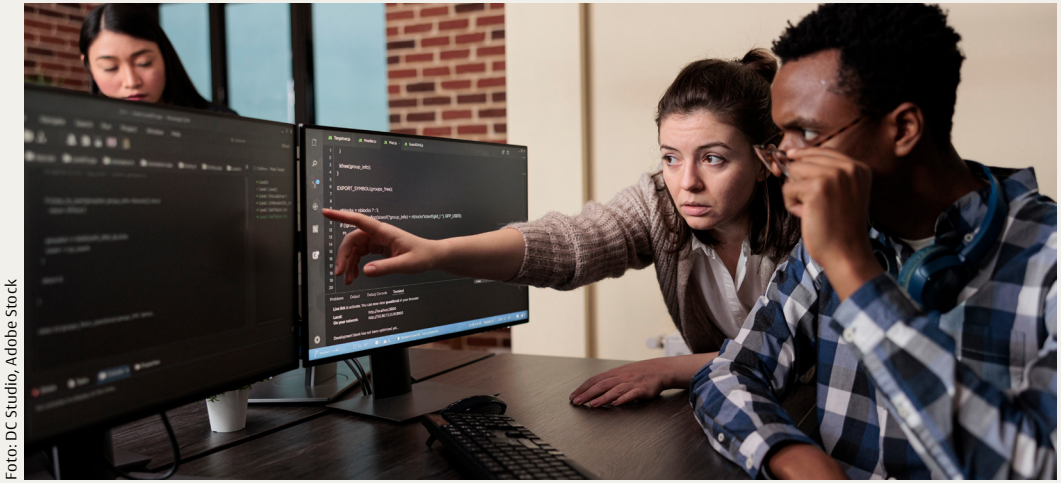

Foto: DC Studio, Adobe Stock

Zu ergreifende Maßnahmen nach Datenpannen

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 er es schwer haben, 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.

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat eine Sammlung der häufigsten Ursachen der bei ihm gemeldeten Datenschutzverletzungen erstellt und dazu eine Empfehlung technischer und organisatorischer Maßnahmen vorgelegt, die bei eingetretener Verletzung des Schutzes personenbezogener Daten der Behebung der Verletzung bzw. der Abmilderung der nachteiligen Auswirkungen dienen können.

Es werden auch Maßnahmen vorgestellt, die der präventiven Vermeidung der entsprechenden Verletzungen dienen können. Die Aufsichtsbehörde betont, dass es sich bei den genannten Maßnahmen nicht um abschließende Empfehlungen handelt, die bei den jeweiligen Datenschutzverletzungen geprüft werden sollten. Es sollte auch stets geprüft werden, ob im Einzelfall weitere Maßnahmen erforderlich sind. Im Falle eines hohen Risikos sind die betroffenen Personen nach Art. 34 DS-GVO zu benachrichtigen. Ein hohes Risiko liege zumindest immer dann vor, wenn besondere Kategorien personenbezogener Daten – z. B. Gesundheitsdaten – Unberechtigten zur Kenntnis gelangen können.

Quelle: Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Foto: Funtap, Adobe Stock

Aufsichtsbehörden prüfen Auftragsverarbeitungsverträge von Webhostern

Auch beim Thema Auftragsverarbeitung gibt es wiederkehrende datenschutzrechtliche Fragen. Darf ein Auftragsverarbeiter bspw. für die Erstellung und Pflege eines Vertrages nach Art. 28 DS-GVO ein Entgelt verlangen und in welchem Umfang wäre das ggf. angemessen? Das BayLDA hatte sich zu dieser Frage bereits vor Geltung der DS-GVO (§ 11 BDSG-alt) geäußert. Die klare Antwort der Aufsichtsbehörde war damals, dass es sich dabei um keine datenschutzrechtliche Frage handelt, sondern um eine Frage, die zivilrechtlich zu lösen ist. In Konsequenz äußerte sich die Aufsichtsbehörde damals nicht zu einer etwaigen Höhe einer Vergütung (7. Tätigkeitsbericht des BayLDA für die Jahre 2015/2017, S. 40).

Weiter auf DataAgenda lesen

Foto: Blue Planet Studio, Adobe Stock

Praxishilfe: Internationaler Datentransfer

Die GDD hat ihre neue Praxishilfe zu „Datenschutzrechtliche Anforderungen an internationale Datentransfers“ veröffentlicht.

Der europäische Gesetzgeber hat, vor dem Hintergrund der Ausweitung des internationalen Handels, die Übermittlung personenbezogener Daten an Datenempfänger in Drittländern unter besondere datenschutzrechtliche Anforderungen gestellt, um Rechte und Freiheiten von Betroffenen zu schützen. Ziel ist es, das durch die Datenschutz-Grundverordnung (DS-GVO) unionsweit gewährleistete Schutzniveau für natürliche Personen nicht zu untergraben, wenn personenbezogene Daten in ein Drittland transferiert werden. Die Art. 44 ff. aus Kapitel V der DS-GVO geben die Bedingungen vor, nach denen Verantwortliche oder Auftragsverarbeiter, die der DS-GVO unterliegen, personenbezogene Daten in Drittländer übermitteln dürfen.

Die vorliegende Praxishilfe der GDD soll Rechtsanwendern einen Überblick über die zur Verfügung stehenden Mechanismen beim sog. „Datenexport“ geben und bei der Einhaltung der datenschutzrechtlichen Anforderungen Unterstützung leisten. Ihr Fokus liegt auf Hinweisen für nichtöffentliche Stellen, daher ist die Übermittlung an sog. „internationale Organisationen“ gem. Art. 4 Nr. 26 DS-GVO im Drittland nicht Gegenstand der Praxishilfe.
Die Praxishilfe erläutert anhand der 2-Stufen Prüfung die Voraussetzungen einer Übermittlung personenbezogener Daten an Empfänger in Drittländer. Im Zuge der ersten Prüfstufe hat der Datenexporteur sicherzustellen, dass die geplante Übermittlung den allgemeinen Anforderungen der DS-GVO bzw. des BDSG oder einer bereichsspezifischen Norm entspricht. Im Rahmen der zweiten Prüfstufe sind die spezifischen Anforderungen aus Kapitel V an die Datenübermittlung an den Verantwortlichen oder Auftragsverarbeiter im Drittland zu prüfen. Dies erfolgt anhand der Maßgabe, dass ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet sein muss, wie z.B. das Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission gemäß Art. 45 Abs. 1 S. 1 DS-GVO oder die Verwendung geeigneter Garantien gemäß Art. 46 DS-GVO.
Die Praxishilfe enthält die nach den Empfehlungen des EDSA (vgl. Empfehlungen 01/2020) anzuwendenden sechs Prüfschritte zur Umsetzung der Vorgaben von Kapitel V der DS-GVO.
Zudem enthält die neue Praxishilfe zwei Muster für Rechtsanwender: Zum einen eine Checkliste für ein Transfer Impact Assessment, zum anderen einen ausgefüllten Anhang I der Standarddatenschutzklauseln, welcher die Umstände des Datentransfers beschreibt.
>> Die neue GDD Praxishilfe „Datenschutzrechtliche Anforderungen an internationale Datentransfers“ können Sie hier abrufen.
Weitere Praxishilfen zu vielen interessanten und aktuellen Themen finden Sie hier.

Foto: vchalup, Adobe Stock

Beschäftige haben weitreichenden Auskunftsanspruch – Unvollständige Auskunft führt zu Schadensersatz

LAG Hamm, Urt. v. 11.05.2021 – 6 Sa 1260/20

Ein Beschäftigter hat das Recht, eine vollständige Auskunft (gemäß Art. 15 DS-GVO) von seinem Arbeitgeber zu erhalten. Kommt der Arbeitgeber dem nur unvollständig oder gar nicht nach, dann hat der Arbeitnehmer ein Recht auf Schadenersatz. So entschied das Landesgericht in Hamm.

Weiter auf DataAgenda lesen

DATAAGENDA UND
LATHAM & WATKINS LLP

DS-GVO-Schadensersatztabelle

RA Tim Wybitul / Dr. Tobias Jacquemain, LL.M.

Stand Juli 2022

LATHAM & WATKINS LLP

DATAKONTEXT

DNS-Kongress auf der Security Essen

Nach dem coronabedingten Aussetzen öffnet die Security Essen wieder vom 20. bis 23. September ihre Tore.

Foto: Sashkin, Adobe Stock

Die Fachmesse ist internationaler Treffpunkt der physischen Sicherheitsbranche und findet im modernisierten Gelände der Messe Essen statt. In den Ausstellungshallen geht es um die Themenbereiche „Dienstleistungen“, „Zutritt, Mechatronik, Mechanik und Systeme“, „Perimeter“, „Video“ sowie „Brand, Einbruch und Systeme“. Darüber hinaus ist Cybersecurity ein Thema: Durch IoT-Devices und die Internet-Anbindung von Produkten und Dienstleistungen, die bisher rein physisch oder autark funktionierten, ergeben sich neue mögliche Angriffsziele für Cyberkriminelle, so die Messe. Smart Homes, digitale Firmengebäude, Videoüberwachung und Zutrittskontrolle in der Cloud seien nur einige Beispiele dafür, dass die Auseinandersetzung mit Datenschutz und Informations-Sicherheit künftig auch für die physische Sicherheitswelt unausweichlich ist.

Deswegen veranstalte man innerhalb des Rahmenprogramms einen passenden Kongress: Auf der ersten Digital Networking Security Konferenz am 20. und 21. September berichten Experten über aktuelle Vorfälle, wichtige Schnittstellen zwischen der Corporate- und IT-Security, rechtliche Vorgaben und geben praktische Umsetzungsbeispiele. So zeigt der Sachbuchautor Thomas R. Köhler in seiner Keynote zum Thema „Zwischen Cybercrime und Cyberwarfare – warum Cybersicherheit Chefsache ist“ anhand von aktuellen Fallbeispielen auf, was die wesentlichen Gefahren für Unternehmen sind, welche Risiken im Internet der Dinge drohen, warum Fabrikautomatisierung und Logistik die neuen Spielfelder der Cybercrime-Szene werden und wie man sich und seine Mitarbeitenden bestmöglich schützen kann. Der Kongress findet in Halle 7 statt und ist für Messebesucher kostenlos. Weitere Informationen gibt es hier.

DataAgenda Podcast Folge 20: DS-GVO im Kreuzverhör – Datenschutz zwischen Wirtschafts- und Bürgerfreiheiten

„In der Anwendung der DS-GVO läuft einiges schief – so war sie nicht gemeint. Wenn die EU im internationalen Wettbewerb der Digitalwirtschaft bestehen will, müssen zügig neue Weichen gestellt werden." Unter dieser Überschrift haben Stefan Brink, Jan Oetjen, Rolf Schwartmann und Axel Voß einen gemeinsamen Text für die F.A.Z. vom 18. Juli 2022 verfasst. Der Beitrag hat Zuspruch und Kritik erfahren. Insbesondere Dr. Stefan Brink als Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg wurde adressiert.

Teil 1:
In Teil 1 der Podcasts erörtert er mit Professor Dr. Rolf Schwartmann den ersten Teil der Thesen aus der F.A.Z. Die Themen in Teil 1 lauten: Inwieweit ist die DS-GVO Verbraucherschutzrecht? Darum sollen Verantwortliche die Auseinandersetzung mit der Aufsicht nicht scheuen. Wo muss die Datenschutzaufsicht umdenken und welche Rolle spielt der EuGH für den Datenschutz? Zum Podcast bitte hier klicken.

Teil 2:
In Teil 2 des Podcasts erörtert Dr. Stefan Brink mit Professor Dr. Rolf Schwartmann den zweiten Teil der Thesen aus der F.A.Z.
Es geht um folgende Fragen: Die neuen Datenakte der DGA, Data Act aber auch die KI-Verordnung setzen auf Datenteilung. Wie stehen sie zur DS-GVO? Welche Anreize braucht die europäische Datenwirtschaft, um die neuen Möglichkeiten zu nutzen? Welche Rolle kann § 26 TTDSG mit seinen anerkannten Diensten der Einwilligungsverwaltung in der Onlinewirtschaft spielen? Wie wichtig ist es für die Praxis, das Instrument der Verhaltensregeln nach Art. 40 und 41 DS-GVO zu nutzen? Wie steht es um die Medienfreiheit in Deutschland unter Geltung des DSA?
Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
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