NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 9/2021

DATAKONTEXT

Levent Ferik

EDITORIAL

Hätten die Arbeitskreise der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) ein Motto, unter dem sie nicht erst seit Wirksamwerden der DS-GVO ihre sogenannten Praxishilfen veröffentlichen, könnte einer dieser Leitsprüche wie folgt lauten:
„Aus der Praxis – für die Praxis" oder aber auch „Weniger Reden – mehr Machen". Der Verzicht auf die Darstellung von zähen juristischen Theorien und das Abdrucken mächtiger Fußnotenapparate ist hier kein Bug, sondern ein Feature.
Die Praxishilfen der GDD beanspruchen für sich, dem Anwender klare und verständliche Hilfen und Anleitungen an die Hand zu geben, und haben in den meisten Fällen den Datenschutzbeauftragten oder den Verantwortlichen als Rolle und Adressat im Fokus. Daher müssen sich alle Praxishilfen an dem Anspruch messen lassen, inwieweit die Ausführungen diesem Adressatenkreis einen Mehrwert im Hinblick auf das Datenschutzmanagement bieten.
In genau dieser Manier und der gewohnten Qualität nimmt die aktuellste Publikation „Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung" die übrigen Rollen einer Datenschutzorganisation ins Blickfeld. Dabei handelt es sich um eine Überarbeitung der Praxishilfe, in die nunmehr die vielfältigen Erfahrungen aus der Beratungspraxis der GDD-Geschäftsstelle und auch die Erfahrungen, der an der Aktualisierung mitwirkenden Praktiker, einfließen.
Die 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 GDD-Praxishilfe „Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung" versucht auf der Grundlage der gesetzlichen Vorgaben, der Entwicklungen in Unternehmen und Behörden seit Geltung der DS-GVO sowie allgemeiner Organisationsformen ein Modell hierfür aufzuzeigen. Die Herausforderung dabei besteht 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 obliegt die konkrete interne Zuweisung von Kompetenzen, Rollen und operativen Verantwortlichkeiten der jeweiligen konkreten Situation im Unternehmen oder in der Behörde, und ist in Abhängigkeit der Größe und räumlichen Verteilung des Unternehmens, der Geschäftsstrategie, dem allgemeinen Steuerungs- und Führungsmodell und der individuellen Risikosituation anzupassen.
Die Praxishilfe kann hier abgerufen werden oder per Direktdownload (PDF).

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: DOC RABE Media, Adobe Stock

„Zwei-Schrank-Modell" bei Praxisübergabe kann „outgesourct" werden

Das Patientengeheimnis ist Grundlage für die Vertrauensbeziehung zwischen Patientin bzw. Patient und Arzt. Gibt ein Arzt seine Praxis auf oder beendet ein Betriebsarzt seine Tätigkeit für einen Betrieb, so stellt sich die Frage, ob und unter welchen Voraussetzungen die vorhandenen Patientenakten vom Nachfolger übernommen werden dürfen (vgl. Allgemeine Informationen zum Thema Patientenkartei bei Praxisbeendigung und Praxisübergabe).

Weiter auf DataAgenda lesen

Aufsichtsbehörde „warnt" Senatskanzlei wegen Nutzung von Zoom

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat die Senatskanzlei der Freien und Hansestadt Hamburg (FHH) offiziell gewarnt, die Videokonferenzlösung von Zoom Inc. in der sog. on-demand-Variante zu verwenden. Dies verstoße gegen die DS-GVO, da eine solche Nutzung mit der Übermittlung personenbezogener Daten in die USA verbunden sei. In diesem Drittland bestehe kein ausreichender Schutz für solche Daten. Dies sei durch den Europäischen Gerichtshof in der Entscheidung Schrems II bereits vor über einem Jahr (C-311/18) festgestellt worden, und das bis dahin geltende Privacy-Shield als Übermittlungsgrundlage außer Kraft gesetzt. Ein Datentransfer sei daher nur unter sehr engen Voraussetzungen möglich, die bei dem geplanten Einsatz von Zoom durch die Senatskanzlei nicht vorliegen. Die Daten von Behördenbeschäftigten und externen Gesprächsbeteiligten würden auf diese Weise der Gefahr einer anlasslosen staatlichen Massenüberwachung in den USA ausgesetzt, gegen die keine ausreichenden Rechtsschutzmöglichkeiten bestehen. Den kompletten Artikel lesen Sie hier.

Foto: yalcinsonat, Adobe Stock

45. DAFTA

40. RDV-FORUM

Datenschutz im Umbruch: Online-Datenschutz - Internationaler Datentransfer - Schadensersatz für Datenschutzverletzungen

Jetzt anmelden:
datakontext.com/dafta-2021

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Maria Sbytova, Adobe Stock

Homeoffice: LfD Sachsen-Anhalt veröffentlicht umfangreiches Info-Paket

Die Corona-Pandemie hat dafür gesorgt, dass das Thema Homeoffice auch bei Unternehmen, die sich bislang nicht intensiv damit beschäftigt haben, in den Vordergrund gerückt ist. Im „Normalfall" stellt sich die Einrichtung eines Homeoffice-Arbeitsplatzes als eine wohlüberlegte und gut geplante Maßnahme dar. Damit auch im Falle einer pandemiebedingten, schnelleren Umsetzung der Verlagerung, der Datenschutz am heimischen Arbeitsplatz nicht auf der Strecke bleibt, haben auch Datenschutz-Aufsichtsbehörden eine ganze Reihe von Leitfäden veröffentlicht, so beispielsweise das ULD oder auch der BfDI. Neu hinzugekommen ist ein umfangreiches Infopaket des Landesbeauftragten für den Datenschutz (LfD) Sachsen-Anhalt. Auf 16 Seiten informiert der LfD Sachsen-Anhalt mit seinen „Hinweisen zum Homeoffice in Behörden und Betrieben" über das breit gefächerte Thema. In den Hinweisen zum Homeoffice werden Empfehlungen und Notwendigkeiten zur Verarbeitung personenbezogener Daten dargestellt, die bei der Einrichtung von Homeoffice-Arbeitsplätzen bedacht werden müssen.

Die Hinweise gliedern sich in

- Allgemeine Erwägungen und Anforderungen,
- Umgang mit Dokumenten,
- Nutzung dienstlicher Hardware,
- Private Endgeräte,
- Mobiles Arbeiten,
- Nutzung von Cloud-Diensten.

Abgerundet werden die ausführlichen Hinweise durch die „Checkliste Homeoffice". Um die Überprüfung der Berücksichtigung der Hinweise zu erleichtern, werden im Sinne einer Checkliste die wesentlichen Aspekte stichpunktartig aufgelistet. Eine etwas ältere, aber ebenfalls sehr nützliche Checkliste kommt von dem BayLDA in Form eines „Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice". Eine ebenfalls gut sortierte Sammlung zum Thema Datenschutz und Homeoffice bietet die GDD mit weiteren nützlichen Links zum Thema.

Foto: monsitj, Adobe Stock

Cloud Security für KMU

Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden.
Der Kriterienkatalog C5 wurde im Jahr 2016 durch das Bundesamt für Sicherheit in der Informationstechnik erstmalig veröffentlicht. Der C5 bietet Cloud-Kunden eine wichtige Orientierung für die Auswahl eines Anbieters. Er bildet die Grundlage, um ein kundeneigenes Risikomanagement durchführen zu können. Im Jahr 2019 wurde der C5 grundlegend überarbeitet, um auf aktuelle Entwicklungen einzugehen und die Qualität noch weiter zu erhöhen.
Das BSI hat auch einen Mindeststandard zur Mitnutzung externer Cloud-Dienste in der neuen Version 2.0. Der auf der gesetzlichen Grundlage von § 8 Abs. 1 BSIG veröffentlichte Mindeststandard zur Mitnutzung externer Cloud-Dienste sorgt dafür, dass Entscheidungen im Vorfeld einer Mitnutzung externer Cloud-Dienste einen transparenten Ablauf haben und dadurch ein definiertes Mindestsicherheitsniveau erreicht wird. Die Version 2.0 berücksichtigt zugleich den Kriterienkatalog Cloud Computing (C5:2020) sowie das aktuelle IT-Grundschutz-Kompendium (Edition 2021).
Einen besonderen Mehrwert dürfte die aktualisierte Fassung jedoch für Verantwortliche der Bundesverwaltung aufweisen.
Einen anderen Adressatenkreis bedient der Leitfaden „Cloud Security“ des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT).
Der TeleTrusT-Leitfaden „Cloud Security“ richtet sich vorwiegend an kleine und mittlere Unternehmen. Er beginnt mit einer systematischen Betrachtung der Risiken bei der Nutzung von Cloud-Diensten, gegliedert nach allgemeinen IT-Risiken, Cloud-spezifischen Risiken und rechtlichen Anforderungen. Betrachtet werden auch die Sicherheitsvorteile von Cloud Services.
Der Leitfaden zeigt technische, organisatorische und rechtliche Maßnahmen zur Reduktion und Beherrschung ermittelter Risiken auf. Neben Mechanismen und Konfigurationsmöglichkeiten, die integraler Bestandteil der Cloud-Dienste sind, wird fokussiert auf externe Sicherungsmechanismen eingegangen: Identity Provider, Cloud Access Security Broker (CASB), Cloud Encryption Gateways, E-Mail Security Gateways, Cloud VPNs, Cloud Firewalls, Confidential Computing, Backup und Notfallplanung. Im Bereich organisatorischer Maßnahmen wird auf die Aufgabenverteilung zwischen Anbieter und Nutzer sowie auf die Vertragsgestaltung eingegangen.

Foto: Trueffelpix, Adobe Stock

Aufsichtsbehörde verhängt Bußgeld wegen fehlender Datenschutz-Folgen-abschätzung

Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

Weiter auf DataAgenda lesen

Foto: Prostock-studio, Adobe Stock

Veröffentlichung von Kinderfotos: Einverständnis beider Elternteile notwendig

Nach einem Beschluss des OLG Oldenburg aus dem Jahre 2018 (24.05.2018, 13 W 10/18) handelt es sich bei der Veröffentlichung eines Kinderfotos um eine Angelegenheit der elterlichen Sorge. Die Regelung stelle eine Angelegenheit erheblicher Bedeutung für das Kind dar. Das OLG wies in seinem Urteil zunächst darauf hin, dass, gemäß § 22 KunstUrhG, Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Hierzu zähle auch das Einstellen von Fotos auf einer Internetseite. Sei der Abgebildete minderjährig, bedürfe es zusätzlich der Einwilligung seines gesetzlichen Vertreters. Dies sind im Regelfall gemäß § 1629 BGB die sorgeberechtigten Eltern, so das OLG Oldenburg.

Bei gemeinsamem Sorgerecht ist eine einvernehmliche Einwilligung beider Elternteile notwendig

Sofern ein gemeinsames Sorgerecht bestehe, sei es notwendig, dass eine einvernehmliche Einwilligung beider Elternteile vorliege. In dem streitgegenständlichen Fall waren die Eltern des sechsjährigen Kindes geschieden und die Mutter besaß das Aufenthaltsbestimmungsrecht über die Tochter. Darüber hinaus galt das gemeinsame Sorgerecht. Im Zusammenhang mit der Veröffentlichung des Kinderfotos, welches für die Werbung auf der Internetseite des neuen Lebenspartners der Mutter verwendet wurde, sah das Gericht eine hohe Gefährdung des Rechts der Tochter. Bei der Veröffentlichung von Fotos im Internet würden die Fotos einem unbegrenzten Personenkreis zugänglich gemacht.

Aktueller Beschluss des OLG Düsseldorf bestätigt bisherige Wertung

Auch das OLG Düsseldorf befindet, dass die Entscheidung über das rechtliche Vorgehen gegen eine unberechtigte Veröffentlichung von Fotos des Kindes im Internet eine Angelegenheit von erheblicher Bedeutung für das Kind i.S. des § 1628 BGB betrifft (Beschluss vom 20.07.2021 – 1 UF 74/21). Daraus leitet das Gericht in seinen Entscheidungsgründen ab, dass für die Verbreitung von Fotos des Kindes in digitalen sozialen Medien, gemäß § 22 KunstUrhG, die Einwilligung beider sorgeberechtigter Elternteile erforderlich ist. Die Rechtfertigung der Verwendung von Fotos des Kindes in digitalen sozialen Medien, gemäß Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO, erfordere die Einwilligung beider sorgeberechtigter Elternteile.
Es entspreche, gemäß §§ 1628, 1697a BGB, regelmäßig dem Kindeswohl am besten, die Entscheidung über das rechtliche Vorgehen, gegen eine unberechtigte Veröffentlichung eines Fotos des Kindes im Internet, demjenigen Elternteil zu übertragen, der die Gewähr für eine Verhinderung der weiteren Bildverbreitung biete. Dabei sei allein auf die konkrete rechtswidrige Bildverbreitung abzustellen, sodass es nicht darauf ankomme, ob ein Elternteil in einem anderen Fall eine unrechtmäßige Verbreitung von Fotos des Kindes veranlasst oder zugelassen habe.

Foto: Syda Productions, Adobe Stock

Datenschutz-Workshop für Grundschüler

Bedingt durch die aktuelle und langanhaltende Pandemie sind nach Angaben von UNICEF in 188 Ländern die Schulen ganz oder teilweise geschlossen – weltweit sind davon 1.5 Milliarden Kinder und Jugendliche betroffen. Durch die Covid-19-Pandemie verbringen viele von ihnen immer mehr Zeit Online, denn dies ist die einzige Möglichkeit, um weiterzulernen, mit anderen in Kontakt zu bleiben, zu spielen und Freizeitangebote wahrnehmen zu können.
In einigen Weltregionen ist die Internetnutzung seither um 50 Prozent gestiegen. Laut einer Studie der Krankenkasse DAK Gesundheit stieg die durchschnittliche Verweildauer von Zehn- bis 17-Jährigen in Deutschland in den sozialen Medien werktags um 66 Prozent an. Die Nutzungsdauer von Onlinespielen an diesen Tagen stieg um 75 Prozent. Die sog. Zusatzstudie „JIMplus Corona“ kommt zu vergleichbaren Ergebnissen. Während die Nutzung des Internets nicht nur pandemiebedingt immer noch stark wächst, hinkt die Sensibilität für Datenschutzfragen hinterher. Wie in vielen anderen Bereichen der Erziehung ist hier vor allem gefragt, Kinder frühzeitig für mögliche Stolpersteine zu sensibilisieren, sie auf ihrem Weg zu begleiten und ihnen einen reflektierten Umgang beizubringen.
Passend zu diesem Themenbereich und zum neuen Schuljahr veröffentlicht die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, ihr überarbeitetes medienpädagogisches Angebot und bietet Berliner Grundschulen ein neues und kostenloses Workshop-Format an.
Der Workshop „Datenschutz für Kinder“ richtet sich speziell an die Jahrgangsstufen 4 bis 6. Verteilt über fünf Unterrichtsstunden, vermittelt der Workshop digitale Kompetenzen und führt in die Datenschutzwelt ein. Die Schüler*innen entdecken spielerisch, was Daten sind, wie sie erhoben werden und wieso sie schützenswert sind.
Auf www.data-kids.de finden Grundschulkinder, Lehrkräfte und Eltern umfangreiche Materialien, die dabei helfen, sich in der Welt des Datenschutzes besser zurechtzufinden.

Foto: Tanja Esser, Adobe Stock

Unterbliebene Auskunft für Arbeitnehmer führt zu 5.000,– € Schadensersatz nach DS-GVO

Urteil: ArbG Düsseldorf, Urteil v. 5.3.2020 – 9 Ca 6557/18, NZA- RR 2020, 409

Vor dem Arbeitsgericht Düsseldorf klagte ein Arbeitnehmer gegen seinen ehemaligen Arbeitgeber. Gegenstand dieser Rechtsstreitigkeit waren neben zahlreichen anderen arbeitsrechtlichen Streitigkeiten u.a. auch eine unzureichende und nicht rechtzeitige Auskunft nach Art. 15 DS-GVO. Hierfür verlangte der Beschäftigte Schadenersatz nach Art. 82 DS-GVO. Die Auskunft ist gerade deswegen so maßgeblich für den Beschäftigten, damit er Transparenz darüber besitzt, ob seine personenbezogenen Daten von dem beklagten Unternehmen und/oder anderen Personen verarbeitet und weitergegeben wurden.
Mit der Entscheidung vom 05.03.2020 wurde dem Kläger vom Arbeitsgericht Düsseldorf ein Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DS-GVO von 5.000 € zugesprochen. Dieser Ersatz für den erlittenen immateriellen Schaden gründet vor allem darauf, dass der ehemalige Arbeitgeber den Art. 15 DS-GVO verletzt hat und damit das Auskunftsrecht des Klägers beeinträchtigt hat. Der ehemalige Arbeitgeber hat die Auskunft zunächst verwehrt und ist dem Antrag auf Auskunft dann nur verspätet und das auch nur unzureichend nachgekommen. Insoweit ist dem Kläger ein immaterieller Schaden entstanden, der nach Wertung des Verordnungsgebers in Form von Art. 82 DS-GVO unstrittig zu ersetzen ist. Die Verletzung des Rechts auf Auskunft nach Art. 15 DS-GVO stellt gleichzeitig auch eine Missachtung des Europäischen Grundrechts nach Art. 8 Abs. 2 S. 2 der Grundrechte-Charta dar.

DATA AGENDA
PODCAST

Der **10-Minuten-Talk**
mit Prof. Schwartmann

Folge #7

Die Bedeutung der Datenschutz-Grundverordnung für die Rechtsprechung des Bundesgerichtshofs

Dr. Peter Allgayer

Folge #8

Blackout und Zero – die spannende Seite des Datenschutzes

Marc Elsberg

Folge 7: Die Bedeutung der Datenschutz-Grundverordnung für die Rechtsprechung des Bundesgerichtshofs

Der Bundesgerichtshof wird sich bald mit Schadensersatzprozessen nach Art. 82 DS-GVO befassen müssen. Welches Verständnis liegt der DS-GVO zum Strafcharakter von Schadensersatzansprüchen zugrunde, wie beeinflusst das die Rechtsprechung des BGH. Sind Abtretungsmodelle und Legal-Tech rechtlich vertretbar? Inwieweit führt die Geltung der Datenschutzgrundverordnung zu neuen Rechtsfragen oder zu neuen Antworten auf Rechtsfragen? Welche grundlegenden Weichenstellungen stehen vor dem Hintergrund des neuen Rechts an für den BGH im Sandwich zwischen EuGH und Bundesverfassungsgericht an? Dr. Peter Allgayer, Richter am Datenschutzsenat des Bundesgerichtshofs, im DataAgenda Datenschutzpodcast.
Zum Podcast bitte hier klicken.

Folge 8: Blackout und Zero – die spannende Seite des Datenschutzes

Der Bestsellerautor Marc Elsberg hat am 20.11.2020 anlässlich der 44. Datenschutzfachtagung (DAFTA) den Datenschutzpreis der Gesellschaft für Datenschutz und Datensicherheit 2020 erhalten.
„Marc Elsberg hat mit seinen Bestsellern „Black Out“ und „Zero“ die wissenschaftlich wie auch gesellschaftlich sehr relevanten Themen kritische Infrastrukturen und Datenschutz in eindrucksvoller Art und Weise literarisch aufgearbeitet und einer sehr großen Leserschaft vor Augen geführt“, so Prof. Dr. Rolf Schwartmann, Vorsitzender der GDD, in der damaligen Begründung.
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:
Hans-Günter Böse, 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