NEWS BOX DATENSCHUTZ

AUSGABE
2/2021

INHALTSVERZEICHNIS

2 Editorial
3 Missbräuchlich anmutende Anfragen zu Betroffenenrechten
4 Mindestanforderungen an sicheres Cloud Computing
5 Geldbuße sowohl gegen Verantwortlichen als auch Auftragsverarbeiter
6 FAQ-Sammlung zum „Schulischen Datenschutz“
8 BSI-Standard zum Notfallmanagement wird aktualisiert
9 Beispiele für Informationspflichten bei Datenpannen
10 GDD äußert sich zur Evaluierung des BDSG 2018
11 Datenschutzkonforme Einstellungen für Zoom
12 10,4 Millionen EUR Bußgeld wegen unzulässiger Videoüberwachung
13 Gesammelte Rechtsprechung zum europäischen Datenschutzrecht
14 Schmerzensgeld/Schadensersatz wegen Verletzung der DS-GVO

DATAKONTEXT

Levent Ferik

EDITORIAL

Würde es sich bei den beiden Personen nicht um die Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie um Professor Dieter Kugelmann, Landesbeauftragter für Datenschutz und die Informationsfreiheit in Rheinland-Pfalz handeln, würde man vielleicht im Netzjargon von einem „Rant" sprechen, bekannt als leidenschaftliche und emotionale (Wut)Rede, in der sich jemand exzessiv über etwas äußert:

„Die Pandemie zeigt, wie der Datenschutz als Sündenbock herhalten muss, wenn Dinge schiefgehen. Es vergeht kein Tag, an dem nicht behauptet wird, dass die Pandemie leicht in den Griff zu bekommen sei, wenn wir nur den Datenschutz zurechtstutzen würden", so die Datenschutzbeauftragten von Berlin und Rheinland-Pfalz.

Schützenhilfe bekommen die beiden Datenschützer von Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D. (2003-2013). Schaar fragt sich anlässlich einiger Aussagen im Rahmen des sogenannten Impfgipfels: „Glaubt die Bundeskanzlerin wirklich, dass die EU auch nur eine Impfdosis mehr bekommen hätte, wenn sie den Herstellern im Gegenzug die Gesundheitsdaten der Geimpften zur Verfügung gestellt hätte?"

Auch der amtierende BfDI, Prof. Ulrich Kelber, ist not amused und macht seinem Ärger auf Twitter Luft „Das ist schon ärgerlich. Der Datenschutz ist nicht schuld an mangelhafter Digitalisierung der Gesundheitsämter, Verspätungen beim Impfen, Überbietungswettbewerb bei „Lockerungen" usw. Unfaires Ablenkungsmanöver zulasten eines Grundrechts."

Der interessierte Bürger dürfte wieder einmal zwiegespalten mitlesen und sich fragen: Wird der Datenschutz (wie so oft) zum Sündenbock gemacht oder liegt die Wahrheit (wie so oft) in der Mitte?

Ihr Levent Ferik

P.S.: Der Datenschutz befindet sich einem ständigem Wandel, auch wir wollen nicht stehen bleiben. Im ersten Schritt erscheint die Datenschutz Newsbox ab sofort in einem neuen Design. Wir wünschen Ihnen besonders viel Spaß beim Lesen dieser Ausgabe und freuen uns auf Ihr Feedback.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: DatenschutzStockfoto, Adobe Stock

Missbräuchlich anmutende Anfragen zu Betroffenenrechten

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) informiert mit einem Hinweisschreiben über eine mutmaßliche „Masche", die sich die Betroffenenrechte der Artikel 15 bis 22 DS-GVO zunutze macht.

Die Geschäftsstelle der GDD weist darauf hin, dass sie sich in letzter Zeit aus dem Kreis ihrer Mitglieder vermehrt mit Meldungen über missbräuchlich anmutende Anfragen zu Betroffenenrechten gem. Art. 15-22 DS-GVO konfrontiert sieht.

Das Vorgehen ziele hierbei darauf ab, unter Aufbau einer Drohkulisse, Verantwortliche zur außergerichtlichen Zahlung eines immateriellen Schadensersatzes in vierstelliger Höhe an den Betroffenen zu bewegen sowie zur Erstattung der angeblich entstandenen Rechtsanwaltskosten.

Die hohe Zahl gleichgelagerter Fälle nimmt die GDD zum Anlass, ihre Mitglieder über die Vorgehensweise zu informieren. Selbstverständlich schadet eine Sensibilisierung aller Verantwortlichen in diesem Zusammenhang nicht.

Weitere sachdienliche Hinweise und Empfehlungen der GDD können Interessierte hier downloaden:

Mindestanforderungen an sicheres Cloud Computing

Foto: Blue Planet Studio, Adobe Stock

Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden.

Der C5 legt fest, welche Kriterien das interne Kontrollsystem der Cloud-Anbieter erfüllen muss bzw. auf welche Anforderungen der Cloud-Anbieter mindestens verpflichtet werden sollte. Der Nachweis, dass ein Cloud-Anbieter die Anforderungen des Katalogs einhält und die Aussagen zur Transparenz korrekt sind, wird durch Bericht nach dem Wirtschaftsprüferstandard ISAE 3402 bzw. IDW PS 951 erbracht. Dieser Bericht basiert auf einer Prüfung nach dem internationalen Wirtschaftsprüferstandard ISAE 3000.

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.

Um das EU-Zertifizierungsschema noch besser an die Bedürfnisse der verschiedenen Stakeholder anzupassen, hat die europäische Cyber-Sicherheitsagentur ENISA am 22. Dezember 2020 die öffentliche Kommentierung des Entwurfs für das Zertifizierungsschema zur Cloud-Sicherheit unter dem Cyber Security Act gestartet. Bis zum 7. Februar 2021 bestand nun die Möglichkeit, den auf der ENISA-Webseite veröffentlichten Entwurf zu kommentieren. www.enisa.europa.eu

Foto: David Hirjak, Adobe Stock

Geldbuße sowohl gegen Verantwortlichen als auch Auftragsverarbeiter

Die Comission Nationale de l'informatique et des libertés, die französische Datenschutzbehörde (‚CNIL'), hat Ende Januar 2021 wegen Verstößen gegen Art. 32 DS-GVO ein Bußgeld sowohl gegen den Verantwortlichen als auch den eingebundenen Auftragsverarbeiter verhängt.

Zwischen Juni 2018 und Januar 2020 erhielt die CNIL mehrere Dutzend Meldungen über Verstöße gegen personenbezogene Daten im Zusammenhang mit einer Website, auf der mehrere Millionen Kunden regelmäßig einkaufen. Die CNIL beschloss, den für die Datenverarbeitung Verantwortlichen und seinen Auftragsverarbeiter zu überprüfen, der mit der Verwaltung dieser Website betraut war.

Im Zuge ihrer Untersuchungen stellte die CNIL fest, dass die betreffende Website zahlreichen Angriffswellen des Typs „Credential Stuffing" ausgesetzt war. Bei dieser Art von Angriff verwenden Angreifer Listen mit „unverschlüsselten" Kennungen und Passwörtern, die im Internet veröffentlicht wurden und damit ebenfalls in der Regel einer Datenverletzung entstammen. Unter der Annahme, dass Benutzer häufig dasselbe Kennwort und denselben Benutzernamen (die E-Mail-Adresse) für verschiedene Dienste verwenden, versucht der Angreifer mithilfe von „Bots", sich bei einer großen Anzahl von Websites anzumelden. Wenn die Authentifizierung erfolgreich ist, ermöglicht dies dem Angreifer, die mit den betreffenden Konten verbundenen Informationen zu sehen.

Die CNIL hat festgestellt, dass die Angreifer auf diese Weise in der Lage waren, folgende Informationen auszulesen: Name, Vorname, E-Mail-Adresse und Geburtsdatum der Kunden, aber auch deren Kundenkartennummer und -guthaben sowie Informationen im Zusammenhang mit ihren Bestellungen. Damit verstießen die beiden Unternehmen nach Auffassung der Behörde gegen Pflicht zur Wahrung der Sicherheit der persönlichen Daten der Kunden gemäß Artikel 32 der DS-GVO. Der Vorwurf der CNIL betraf auch den Umstand, dass die Unternehmen nur langsam Maßnahmen ergriffen, um diese wiederholten Angriffe wirksam zu bekämpfen.

Infolge dieser mangelnden Sorgfalt wurden die Daten von ca. 40.000 Website-Kunden zwischen März 2018 und Februar 2019 unberechtigten Dritten zugänglich gemacht.

Infolgedessen verhängte die CNIL zwei getrennte Geldbußen – 150.000 EUR gegen den für die Verarbeitung Verantwortlichen und 75.000 EUR gegen den Auftragsverarbeiter. Dabei wurde, laut CNIL, berücksichtigt, dass der für die Verarbeitung Verantwortliche über die Durchführung von Maßnahmen entscheiden und seinem Auftragsverarbeiter dokumentierte Anweisungen erteilen muss. Der Auftragsverarbeiter muss jedoch auch nach den geeignetsten technischen und organisatorischen Lösungen suchen, um die Sicherheit der personenbezogenen Daten zu gewährleisten, und diese dem Verantwortlichen vorschlagen.

Quelle: Die Comission Nationale de l'informatique et des libertés ('CNIL')

FAQ-Sammlung zum „Schulischen Datenschutz“

Foto: shintartanya, Adobe Stock

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI Rlp) stellt auf seiner Internetseite eine Sammlung von Fragen und Antworten zum Themengebiet „Schulischer Datenschutz“ zur Verfügung.

Die vorgestellte Sammlung ist Ergebnis einer Kooperation zwischen dem LfDI Rlp, dem Pädagogischen Landesinstitut Rheinland-Pfalz (PL) sowie dem Bildungsministerium. Unter dem Titel „Schulischer Datenschutz in der Praxis – Was Sie schon immer fragen wollten“ veranstalteten die drei beteiligten Stellen Ende 2020 sieben Online-Seminare für Lehrkräfte.

Die Fortbildungen hatten neben einer datenschutzrechtlichen Grundsensibilisierung das Ziel, häufig aufkommende technische und juristische Fragen im schulischen Kontext zu beantworten. Um möglichst konkret auf die Anforderungen der einzelnen Schulformen einzugehen, wurde nach den Zielgruppen Grund- und Förderschulen, weiterführende und berufsbildende Schulen sowie Medienzentren und Multiplikatoren unterschieden.

Im Ergebnis ist eine äußerst praxisrelevante und hilfreiche Sammlung von Fragen und Antworten zu einem Themengebiet entstanden, in welchem ein dringender Bedarf an verlässlichen Informationen rund um Datenschutz zu verzeichnen ist und in absehbarer Zeit auch noch (auch pandemiebedingt) ansteigen wird.

Das Spektrum reicht von Fragen zur Funktion und zu Aufgaben schulischer Datenschutzbeauftragter über den Umgang mit außereuropäischen Online-Diensten nach dem EuGH-Urteil bis hin zur Verarbeitung von Schülerdaten auf privaten Endgeräten. www.datenschutz.rlp.de

Live Online-Schulung

Datenschutz und Betriebsrat unter der DS-GVO

16. März 2021 | online
Referent: David Malzkorn

Schwerpunkte:

- ✓ Welche neuen Aufgaben und Pflichten bekommt der Betriebsrat
- ✓ Wie wirken der Daten-schutz und das BetrVG grundlegend zusammen
- ✓ Verzeichnis der Verarbeitungstätigkeiten im Betriebsrat
- ✓ Auswirkungen der DS-GVO auf Betriebsvereinbarungen

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

BSI-Standard zum Notfallmanagement wird aktualisiert

Foto: Vitalii Vodolazskyi, Adobe Stock

Das BSI entwickelt den IT-Grundschutz weiter fort. In absehbarer Zeit soll auch der Standard 100-4 ersetzt werden. Mit dem BSI-Standard 100-4 hatte das BSI begonnen, einen systematischen Weg aufzuzeigen, wie ein Notfallmanagement in einer Behörde oder einem Unternehmen aufgebaut werden kann, um die Kontinuität des Geschäftsbetriebs sicherzustellen.

Der Standard 100-4 wird durch den neuen Standard 200-4 ersetzt. Dieser soll passgenau und modular die verschiedenen Bedürfnisse unterschiedlich großer Anwender berücksichtigen. Der modernisierte BSI-Standard 200-4 gibt eine praxisnahe Anleitung, um ein Business Continuity Management System (BCMS) in der eigenen Institution aufzubauen und zu etablieren.

Wie aktuell der Draft ist, zeigt sich beispielsweise daran, dass die Weiterentwicklung des etablierten BSI-Standards 100-4 zahlreiche Neuerungen, basierend auf aktuellen Erkenntnissen im Bereich Business Continuity sowie durch die jüngsten Erfahrungen aus der Corona-Pandemie enthält.

Der Community Draft des BSI-Standards 200-4 enthält beispielsweise auch eine detailliertere Ausarbeitung von Teilen der Methodik mit umfangreichen Hilfestellungen, z. B. zur Etablierung der besonderen Aufbauorganisation (Stabsstruktur), dem Soll-Ist-Vergleich in der Geschäftsfortführungsplanung oder Wiederanlaufplanung.

Der Community Draft des BSI-Standards 200-4 kann bis zum 30. Juni 2021 kommentiert werden. www.bsi.bund.de

Beispiele für Informationspflichten bei Datenpannen

Foto: Egor, Adobe Stock

Nach ErwG 85 der DS-GVO kann eine Verletzung des Schutzes personenbezogener Daten – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit der dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Deshalb soll nach dem Willen des Verordnungsgebers der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt.

Betrachtet man die Tätigkeitsberichte der Datenschutz-Aufsichtsbehörden, kann wohl angenommen werden, dass sich die „neue Regelung" des Art. 33 DS-GVO etabliert hat. So berichtet auch der Bayerische Landesbeauftragte für den Datenschutz in seiner Veröffentlichung „Meldepflicht und Benachrichtigungspflicht des Verantwortlichen – Erläuterungen zu Art. 33 und 34 Datenschutz-Grundverordnung", dass die Benachrichtigungspflicht immer wieder Gegenstand von Beratungsanfragen seien.

Beitrag weiterlesen www.dataagenda.de

Foto: MQ-Illustrations, Adobe Stock

GDD äußert sich zur Evaluierung des BDSG 2018

Für das am 25. Mai 2018 wirksam gewordene neue Bundesdatenschutzgesetz ist eine Evaluation spätestens drei Jahre nach Inkrafttreten vorgesehen. Zur Evaluation hat die GDD eine Stellungnahme abgegeben.

Diese Evaluation des BDSG 2018 führt das Bundesministerium des Innern, für Bau und Heimat durch.

Die GDD konzentriert sich in ihrer Stellungnahme auf ausgewählte BDSG-Vorschriften, die auf Grundlage der Öffnungs- bzw. Spezifizierungsklauseln der Datenschutz-Grundverordnung (DS-GVO) ergangen sind.

Hinsichtlich der Rechtsgrundlagen im BDSG hält die GDD die Vorschrift zur Videoüberwachung in § 4 BDSG für eine sachgerechte und praxisrelevante Regelung, die insbesondere für die Videoüberwachung in den von § 4 Abs. 1 Satz 2 BDSG erfassten hoch frequentierten Risikobereichen durch Private Rechtssicherheit schafft.

Bei der Beurteilung des Schwellwertes für die Benennung eines betrieblichen Datenschutzbeauftragten weist die GDD darauf hin, dass hierdurch die effektivste und kostengünstigste Lösung für Wirtschaft und Staat gefunden ist, um die Einhaltung datenschutzrechtlicher Vorgaben bei privaten wie öffentlichen datenverarbeitenden Stellen zu gewährleisten. Die Erfahrung der GDD und auch eine aktuelle Untersuchung der Ruhr-Universität Bochum zeigen, dass im Falle der Nichtbenennung eines Datenschutzbeauftragten oft niemand die Überwachung und Beratung hinsichtlich der Datenschutzpflichten wahrnimmt. Dies ist nicht nur aus Sicht der Personen kritisch, deren personenbezogene Daten verarbeitet werden. Angesichts der immensen Bußgeldrahmen der DS-GVO ist dies auch für die Unternehmen selbst riskant, denn Datenschutzbeauftragte helfen auch bei der Reduzierung von Unternehmensrisiken.

Untersuchung Ruhr-Universität Bochum www.bvdnet.de

Mit Blick auf die Betroffenenrechte weist die GDD darauf hin, dass aus technischen Gründen, beim Einsatz bestimmter am Markt verfügbarer Datenbanksysteme, derzeit faktisch keine Löschung von Datensätzen möglich ist, ohne dass hierdurch u.U. die Konsistenz der gesamten Datenbank gefährdet wird. Bis Verantwortliche teils noch ausstehende Produktnachbesserungen implementieren können, erscheint es aus Sicht der GDD geboten, die in § 35 BDSG bislang auf „nicht automatisierte Datenverarbeitung" begrenzte Befugnis, unter den Voraussetzungen des § 35 Abs. 1 BDSG anstelle der Löschung personenbezogener Daten, eine Einschränkung ihrer Verarbeitung (Art. 18 DS-GVO) vorzunehmen, auch auf Fälle automatisierter Verarbeitung zu erstrecken.

Die detaillierte Stellungnahme der GDD hinsichtlich der einzelnen Vorschriften finden Sie hier zum Download:

Datenschutzkonforme Einstellungen für Zoom

Foto: prima91, Adobe Stock

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat Ende Oktober 2020 eine „Orientierungshilfe Videokonferenzsysteme“ veröffentlicht, in dem sie die datenschutzrechtlichen Anforderungen an die Durchführung von Videokonferenzen durch Unternehmen, Behörden und anderen Organisationen erläutert. Diese Handreichung soll den Verantwortlichen eine Hilfestellung bieten, wie diese Anforderungen erfüllt werden können.

Diese Orientierungshilfe wird durch eine ergänzende Orientierungshilfe (Checkliste Datenschutz in Videokonferenzsystemen) des DSK abgerundet. Die Checkliste soll die wesentlichen Anforderungen an Videokonferenzsysteme der „Orientierungshilfe Videokonferenzsysteme“ der DSK in verkürzter Form darstellen und damit den Verantwortlichen bei der Überprüfung der Frage unterstützen, ob ein Videokonferenzsystem datenschutzkonform ist und die Transparenz- und Dokumentationspflichten erfüllt werden. www.datenschutzkonferenz-online.de

Genau auf diese Checkliste nimmt der Anbieter der Videokonferenzsoftware Zoom Bezug und veröffentlicht eine eigene Anleitung für die zu treffenden Datenschutz-Einstellungen, damit die Empfehlungen der Datenschutzkonferenz DSK umgesetzt werden können. Dafür werden die Kriterien der Checkliste des DSK in der linken Spalte unverändert abgebildet. Auf der rechten Seite findet der Nutzer Hinweise von Zoom zu den Einstellungsmöglichkeiten und weiterführenden Informationen bzw. den rechtlich verbindlichen Dokumenten von Zoom zum Thema Datenschutz.

Nach Angaben des Anbieters soll die Anleitung fortlaufend angepasst werden. Die Anleitung können Sie hier herunterladen:

Foto: jayzynism, Adobe Stock

10,4 Millionen EUR Bußgeld wegen unzulässiger Videoüberwachung

Die Landesbeauftragte für den Datenschutz Niedersachsen hat eine Geldbuße über 10,4 Millionen Euro gegenüber der notebooksbilliger.de AG ausgesprochen. Laut Begründung habe das Unternehmen über mindestens zwei Jahre Beschäftigten per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorlag. Die unzulässigen Kameras erfassten unter anderem Arbeitsplätze, Verkaufsräume, Lager und Aufenthaltsbereiche.

Auch Kundinnen und Kunden von notebooksbilliger.de seien von der unzulässigen Videoüberwachung betroffen, da einige Kameras auf Sitzgelegenheiten im Verkaufsraum gerichtet waren. In Bereichen, in denen sich Menschen typischerweise länger aufhalten, haben die datenschutzrechtlich Betroffenen hohe schutzwürdige Interessen. Das gelte besonders für Sitzbereiche, die offensichtlich zum längeren Verweilen einladen sollen. Deshalb sei die Videoüberwachung durch notebooksbilliger.de in diesen Fällen nicht verhältnismäßig.

Die Notebooksbilliger.de AG hat eine Seite „Fragen und Antworten zum Verfahren der Landesdatenschutzbehörde" geschaltet und stellt den Hergang des bisherigen Verfahrens und ihre Sichtweise dar.

Neben der Höhe des Bußgeldes und der Schwere des vermeintlichen Verstoßes wehrt sich Notebookbilliger.de auch gegen die von der Aufsichtsbehörde geäußerte Darstellung, der Onlinehändler habe systematisch Leistungen und Verhalten seiner Mitarbeiter überwacht.

Beitrag weiterlesen www.dataagenda.de

Quelle: www.lfd.niedersachsen.de

Gesammelte Rechtsprechung zum europäischen Datenschutzrecht

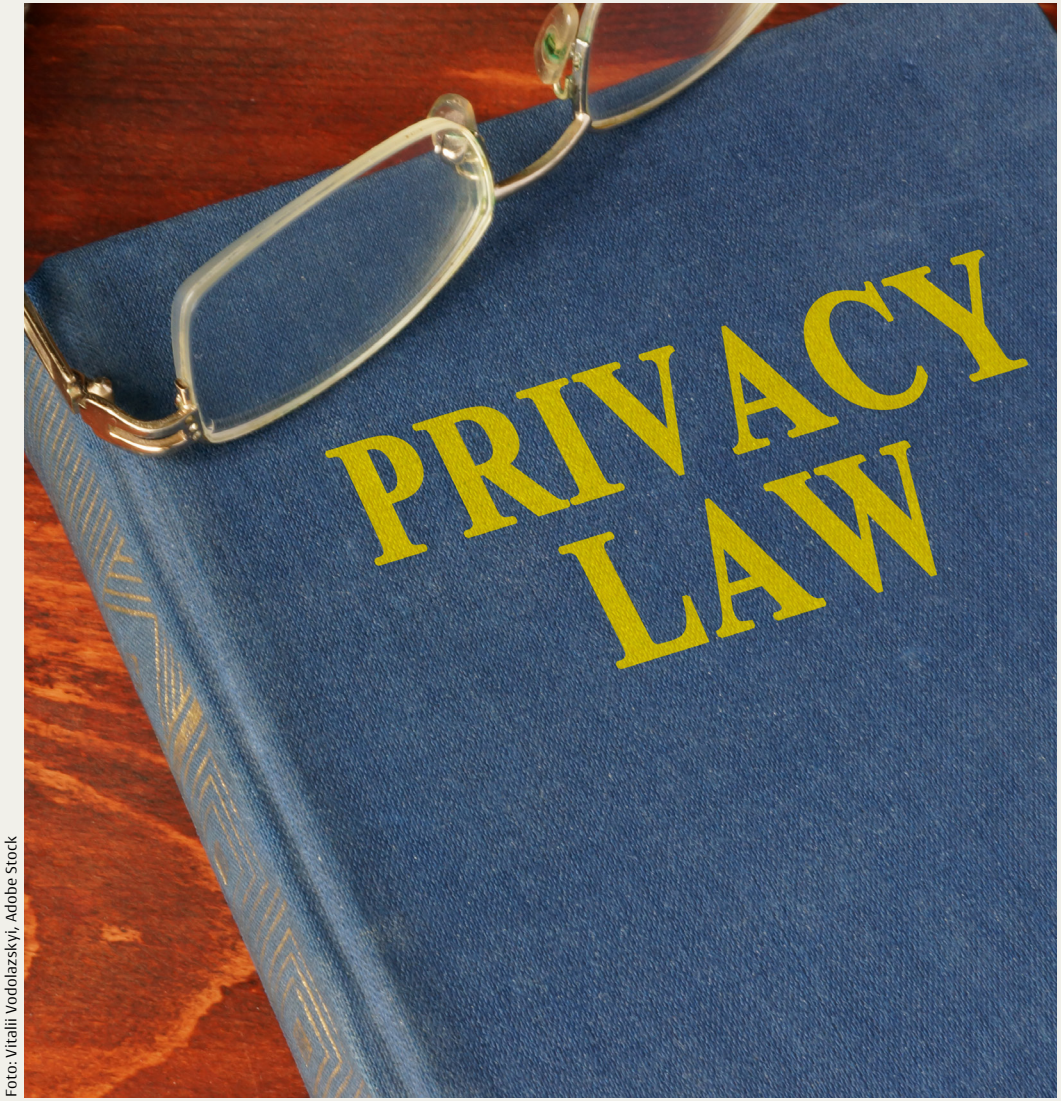

Foto: Vitalii Vodolazskyi, Adobe Stock

Mit dem Ziel der Harmonisierung und der gleichzeitigen Modernisierung des EU-Datenschutzrechts haben das Europäische Parlament und der Rat der Europäischen Union am 27. April 2016 die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) verabschiedet.

Trotz ihres Inkrafttretens seit dem 25. Mai 2018 in allen Mitgliedstaaten sind weiterhin Unterschiede in der nationalen Vollzugspraxis und Rechtsprechung festzustellen. Um Interessierten und Anwendern im Wege der Rechtsvergleichung weitere Erkenntnisse für die Vollzugspraxis und die Anwendung des Datenschutzrechts zu ermöglichen, stellt die Datenschutzstelle Liechtenstein ihren sogenannten Judikaturspiegel zum europäischen Datenschutzrecht (2018 – 2020) hier als Download zur Verfügung:

Darin werden ausgewählte Gerichtsentscheide aus Mitgliedstaaten des EWR (aus dem Zeitraum 2018 bis 2020) in Kurzfassung vorgestellt bzw. wesentliche Passagen der Entscheidungen hervorgehoben. Interessierten ist es damit möglich, auch die Eigenheiten des nationalen Rechtsstandes zu ermitteln und abzugrenzen.

Auch der Europäische Gerichtshof für Menschenrechte (EGMR) bietet eine hilfreiche Publikation (CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS CONCERNING THE PROTECTION OF PERSONAL DATA) an, die als Fallsammlung verstanden werden kann. Diese dürfte jedoch wohl nur für Interessierte handhabbar sein, die sich intensiv mit der Thematik beschäftigen. Die Rechtsprechungsübersicht (Stand Juni 2019) ist hier in englischer Sprache abrufbar:

Auch die ebenfalls nützlichen Factsheets zum Thema Datenschutz sind aktualisiert (Stand Oktober 2020) und können hier abgerufen werden:

Foto: studio v-zwoelf, Adobe Stock

Schmerzensgeld/ Schadensersatz wegen Verletzung der DS-GVO

In jüngster Vergangenheit beschäftigen sich Gerichte auf verschiedensten Instanzen auch mit der Frage, ob und in welcher Höhe Zahlungen von Schmerzensgeld/Schadensersatz in Folge von Verletzungen von Vorschriften der DS-GVO möglich sind.

Insbesondere, wenn es um immaterielle Schäden ging, forderten deutsche Gerichte in der Regel eine gewisse „Spürbarkeit" als Konsequenz der Verletzung, sodass Schmerzensgeld oder Schadensersatz erst zugesprochen wurden, wenn die sogenannte „Bagatellschwelle" überschritten wurde. Es durfte sich also gerade um keine individuell empfundene Unannehmlichkeit ohne ernsthafte Beeinträchtigung für das Selbstbild oder Ansehen einer Person handeln.

Diese Grenze sehen deutsche Gerichte offenbar in immer mehr Fällen als überschritten an. So hat das ArbG Dresden (Urt. v. 26.08.2020 – Az.: 13 Ca 1046/20) einem Kläger einen Schadensersatz nach Art. 82 DS-GVO i. H. v. 1.500, – EUR zugesprochen. Dabei ging es um eine, nach Auffassung des Arbeitsgerichts, unerlaubte Weitergabe von Gesundheitsdaten durch den ehemaligen Arbeitgeber an die Ausländerbehörde sowie die Arbeitsagentur.

Der Kläger war ein ausländischer Beschäftigter des Beklagten, der im Jahre 2019 eine längere Zeit krankgeschrieben war. In einer an die Ausländerbehörde gerichteten E-Mail teilte die Prokuristin des Beklagten mit, dass der betroffene Beschäftigte arbeitsunfähig erkrankt sei. Die Arbeitsagentur erhielt eine Kopie der E-Mail. Mit dem Schreiben an die Arbeitsagentur sollte die Kündigung des Beschäftigten gerechtfertigt werden.

Der von dem Betroffenen eingeschaltete Sächsische Datenschutzbeauftragte stufte die Übermittlung der Gesundheitsdaten an die Behörden als rechtswidrig ein, sodass der Betroffene vor Gericht Schadensersatz unter anderem wegen Verletzung von DS-GVO-Vorschriften begehrte.

Auch in einem Urteil des LG Lüneburg (Urteil vom 14.07.2020, Az. 9 O 145/19) wurden einem Betroffenen Schadensersatz in Höhe von 1.000,– EUR zugesprochen. Die Richter sahen einen Verstoß gegen die DS-GVO, weil die Bank eine Kontoüberziehung ihres Bankkunden in Höhe von 20,– Euro zu Unrecht einer Kredit-Auskunftei, der Schufa Holding AG, gemeldet hatte.

Dabei hielt es einen Anspruch auf Ersatz eines immateriellen Schadens in Gestalt eines Schmerzensgeldes nach Art. 82 Abs. 1 DS-GVO für angemessen.

Den immateriellen Schaden begründete das Gericht mit dem Kontrollverlust des Klägers über seine personenbezogenen Daten. Durch die Übermittlung der Daten an die Schufa habe die Beklagte, so das Gericht, personenbezogene Daten an einen unbeteiligten und unberechtigten Dritten weitergegeben. Dadurch sei der Kläger bloßgestellt worden und es drohe zudem mittelbar eine potenzielle Stigmatisierung, die durch einen Eintrag bei der Schufa entstehen könne.

Quelle: www.juris.de

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

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