NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE 5/2021

DATAKONTEXT

Levent Ferik

EDITORIAL

Für die Bausteine, bei denen Lösungen von Microsofts Office 365 zum Einsatz kommen sollen, hat das Ministerium für Kultus, Jugend und Sport Baden-Württemberg vor geraumer Zeit mit externen Partnern eine Datenschutz-Folgenabschätzung (DSFA) erarbeitet. Die DSFA wurde in Absprache und enger Kooperation mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDi) Dr. Stefan Brink beraten und weiterentwickelt. Im Pilotprojekt hat der LfDI BW letztes Jahr geprüft, ob die in der Datenschutz-Folgenabschätzung beschriebenen Datenflüsse auch den tatsächlich messbaren Übermittlungen entsprechen und ob ein hinreichendes Datenschutzniveau auch in der Praxis besteht.
Im Wesentlichen hat der LfDI BW nach eigenen Angaben geprüft, ob die in der DSFA vorgeschlagenen Abhilfemaßnahmen zur Minimierung der Risiken der Microsoft-Software tatsächlich umgesetzt wurden und sich als ausreichend erwiesen. Daneben stand im Fokus der Prüfungen, welche Datenflüsse beim Pilotbetrieb tatsächlich messbar stattfanden, insbesondere ob unerwünschte beziehungsweise nicht angeforderte Datenverarbeitungen, beispielsweise von Telemetrie-, Diagnose- (oder anders bezeichneten) Daten, erkennbar waren und inwieweit die Verarbeitung personenbezogener Daten von Lehrern und Schülern zu eigenen Zwecken Microsofts festgestellt werden konnten.
Viele hatten wohl auf einen Ritterschlag als Ergebnis der DSFA gehofft, damit der womöglich geplante Einsatz auch tatsächlich im Unternehmen empfohlen werden kann.
Das Ergebnis des LfDI BW fiel jedoch mehr als ernüchternd aus:
Die Risiken beim Einsatz der nun erprobten Microsoft-Dienste im Schulbereich bewertete der LfDI BW als inakzeptabel hoch und rät davon ab, diese dort zu nutzen. Die Schulen seien weder in der Lage ihren Rechenschaftspflichten aus Art. 5 Abs. 2 DS-GVO gerecht zu werden, noch sei eine hinreichende Rechtsgrundlage für stattfindende Datenübermittlungen in Regionen außerhalb der EU erkennbar.

Die erhoffte Lösung im Bereich Office 365 scheint also noch nicht gefunden worden zu sein, fürchtet, Ihr Levent Ferik.

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: blende11.photo, Adobe Stock

Neue Praxishilfe zur Einwilligung

Unter der Mitarbeit des GDD-Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ (AK GSW) wurde eine Praxishilfe mit dem Titel „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers“ erarbeitet und veröffentlicht.
Bei der Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten ist stets zu beachten, dass eine Einwilligung in die Verarbeitung dieser Daten nur möglich ist, wenn der betreffende Mitgliedstaat kein Verbot dieser Verarbeitung erlassen hat. So ist z.B. die Verarbeitung von Gesundheits- und Sozialdaten in Deutschland abschließend in den Sozialgesetzbüchern (SGB) geregelt und eine von den dort legitimierten Verarbeitungsmöglichkeiten abweichende Nutzung von Sozialdaten dürfte auch mit einer Einwilligung nicht legitimiert werden können. Weiterhin können, entsprechend Art. 9 Abs. 4 DS-GVO, die Mitgliedstaaten durch nationale Regelungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten „zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten“. Dies geschah in Deutschland sowohl im Bundesrecht als auch in den verschiedenen, durch die Bundesländer erlassenen Gesetzen.

Mit der vorliegenden Praxishilfe liegt eine umfassende und ganz aktuelle rechtliche Interpretation der Einwilligung – nicht nur für den Forschungsbereich – vor. Sie beinhaltet sowohl Bezüge zur jüngsten Rechtsprechung als auch auf die EDSA-Leitlinien. Die Thematik „Broad Consent“ wurde als eigenes Kapitel aufgegriffen, genauso wie die Einwilligung im Beschäftigtenverhältnis. Ein eigenes Kapitel widmet sich „Häufig gestellten Fragen (FAQ)“ zum Thema Einwilligungen; allein dieser FAQ-Teil umfasst etwas mehr als dreißig Seiten. Neben klassischen Themen wie „Datenweitergabe an den Hausarzt“ werden auch aktuelle Fragestellungen wie z.B. „Bezahlen mit Daten“ oder die „Delegation des Einwilligungsrechts an Dritte“ in diesem FAQ-Teil besprochen.

Die Praxishilfe wurde neben dem Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ der GDD von den folgenden Verbänden unter einer Creative-Commons-Lizenz (4.0 Deutschland Lizenzvertrag) veröffentlicht:

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (gmds)
- Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Die Praxishilfe können Sie hier downloaden:
Weitere Infos finden Sie hier:

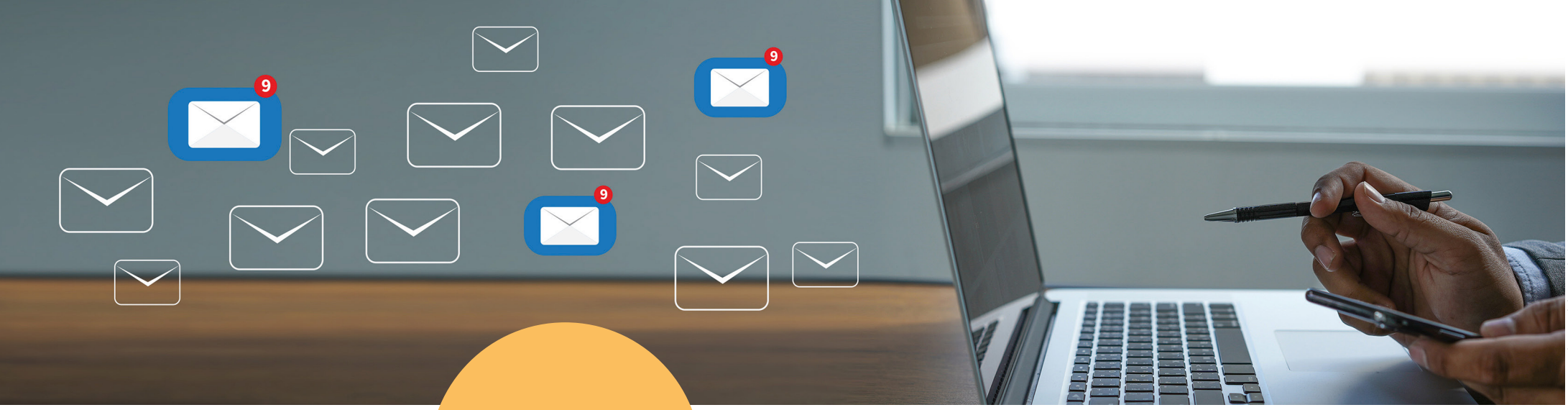

Foto: onephoto, Adobe Stock

Online-Kompaktkurs

Update E-Mail-Marketing

Aktuelle Rechtsfragen zwischen Datenschutz- und Wettbewerbsrecht

14. Juni 2021, 10 bis 11:30 Uhr | online
Referent: Sebastian Schulz

Schwerpunkte:

- ✓ Welche Rechtsgrundlagen sind im E-Mail-Marketing von Bedeutung?
- ✓ Wechselwirkung zwischen Datenschutz- und Wettbewerbsrecht
- ✓ Unter welchen Voraussetzungen kann vom Grundsatz der Einwilligung abgewichen werden?
- ✓ Darstellung der maßgeblichen Rechtsprechung und aktueller behördlicher Verfahren
- ✓ Wie sollte auf Abmahnungen reagiert werden? Wie sollte eine sinnvolle Unterlassungserklärung gestaltet sein?

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: Ilona, Adobe Stock

BSI: Umfrage zur IT-Sicherheit im Home-Office

„In der Pandemie sind allein in Deutschland zwölf Millionen Berufstätige ins Home-Office gewechselt“, so eines der Ergebnisse einer repräsentativen Umfrage des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dazu hat das BSI 1.000 Unternehmen und Betriebe befragt. Eine weitere eher besorgniserregende Feststellung im Rahmen dieser Umfrage ist jedoch, dass die IT-Sicherheit mit dem immer häufiger anzutreffenden Home-Office nicht Schritt zu halten scheint.
Befragt wurden explizit nur diejenigen Unternehmen, welche mindestens drei Mitarbeitende beschäftigen und aktuell Mitarbeitende im Home-Office haben. Diese Unternehmen wurden auf der Grundlage eines repräsentativen Screenings aus allen Unternehmen ab drei Beschäftigten identifiziert. Das BSI gibt, als weiteres Ergebnis der Umfrage, zu bedenken, dass IT-Sicherheit noch zu wenig in Budgets, Abläufen und Köpfen der Unternehmen angekommen sei. Der Digitalisierungsturbo Corona treibe IT-Projekte in den Unternehmen voran, jedoch müsse Digitalisierung und IT-Sicherheit als eine Einheit gedacht und umgesetzt werden. Wer jetzt die Weichen für eine solide Informationssicherheit seiner Infrastruktur legt, der sichert seine Zukunft – in schweren Pandemiezeiten und darüber hinaus, so das BSI. Für mobiles Arbeiten bedürfe es einer richtigen Balance zwischen dem benutzerfreundlichen Zugriff auf Unternehmensdaten und dem Schutz der IT. Ein robustes und risikobasiertes IT-Sicherheitsmanagement, Mitarbeiterschulungen und gut durchdachte Notfallkonzepte seien hierfür notwendig.

Weitere wichtige Erkenntnisse aus der Umfrage:
Über 50 Prozent der Unternehmen investieren weniger als 10 Prozent der IT-Ausgaben in Cyber-Sicherheit. Das BSI empfiehlt, bis 20 Prozent des IT-Budgets in Sicherheit zu investieren.
Je kleiner die Firma, desto schwerwiegender die Folgen. Für Kleinst- und Kleinunternehmen mit weniger als 50 Mitarbeitenden hat eine von vier Cyberattacken existenzbedrohende Folgen.
Obwohl kostengünstig, werden einfache Sicherheitsmaßnahmen wie Mobil Device Management, Notfallübungen oder der Grundsatz „IT-Sicherheit ist Chefsache“ nicht genügend umgesetzt.
Den Ergebniskurzbericht der repräsentativen Umfrage des BSI können Sie hier runterladen:

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Meldepflichten in der Datenschutzpraxis – Praxisreport zum Thema Datenschutzverletzung

Foto: artinspiring, Adobe Stock

Im Rahmen der Konsultation des Europäischen Datenschutzausschusses zu Beispielfällen einer Datenschutzverletzung hat die GDD eine Umfrage für die Öffentlichkeit initiiert, deren Ergebnisse die Bedeutung dieser Thematik für die Datenschutzpraxis einordnet und Datenschutzpraktikern einen tieferen Einblick anhand von fünf Beispielfällen aus der Praxis im Umgang mit „Datenpannen" gibt.

Den Schwerpunkt der GDD-Umfrage bildete die Frage nach der konkreten Beschreibung einer Datenschutzverletzung, um den Umgang von Verantwortlichen mit den gesetzlichen Pflichten aus Art. 33 u. 34 DS-GVO insgesamt in Erfahrung zu bringen und wichtige Beurteilungskriterien für den Leser aufzuzeigen.

Auf Basis der Ergebnisse sind Verantwortliche für den Datenschutz oder Datenschutzbeauftragte dazu angehalten, sich mit Meldepflichten auseinanderzusetzen, da Verletzungen des Schutzes personenbezogener Daten in den unterschiedlichsten Ausprägungen auftreten können. Hinsichtlich ihres Erkennens und einer sich daran anschließenden Risikobewertung bedarf es daher Kenntnisse der rechtlichen Anforderungen. Außerdem bestehen starke Anhaltspunkte dafür, dass ausreichend geschulte Mitarbeiter, welche als interne Meldestelle für Datenschutzverletzungen fungieren können, einen wichtigen Beitrag im Umgang mit Meldepflichten und der Vermeidung von Datenpannen leisten dürften.

Mithilfe des **GDD-Praxisreport 2021 – Datenschutzverletzungen** möchte die GDD einen wichtigen Beitrag für die Rechtsanwendung leisten. Die GDD wird ihren Mitgliedern zu diesem Zweck außerdem den Ratgeber zu Datenpannen in der aktualisierten 3. Auflage im Mai 2021 zur Verfügung stellen.

Den Praxisreport können Sie hier downloaden:

Mitarbeiterinformation Datenschutz

Mitarbeiter einfach und
rechtssicher sensibilisieren

- ideal für alle Mitarbeiter
- leicht verständlich
- anschaulich illustriert
- firmenindividuell gestaltbar
- in 5 Sprachen verfügbar

Bestseller
millionenfach verkauft

jetzt bestellen:
datakontext.com/mitarbeiterinformation

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: DatenschutzStockfoto, Adobe Stock

Auskunftsanspruch: Erteilung einer Kopie nach Art. 15 Abs. 3 DS-GVO

Das Bundesarbeitsgericht (BAG, Urteil vom 27. April 2021 – 2 AZR 342/20) musste sich mit der Frage befassen, in welchem Umfang eine Arbeitgeberin ihren Beschäftigten im Rahmen eines Auskunftsverlangens nach Art. 15 Abs. 3 DS-GVO Kopien von deren personenbezogenen Daten zur Verfügung stellen muss.
Die Parteien stritten im konkreten Fall darüber, ob der Kläger von der Beklagten die Erteilung einer Kopie seines E-Mail-Verkehrs mit ihr sowie der E-Mails, die ihn persönlich erwähnen, verlangen kann.

Der Kläger war bei der Beklagten als Wirtschaftsjurist beschäftigt. Nachdem die Beklagte das Arbeitsverhältnis gekündigt hatte, erteilte sie dem Kläger auf dessen Verlangen im März 2019 Auskunft über seine von ihr verarbeiteten personenbezogenen Daten bzw. deren Kategorien. Außerdem stellte sie dem Kläger die gespeicherten personenbezogenen Daten als sog. ZIP-Dateien zur Verfügung. Mit seiner Klage hat der Kläger u.a. geltend gemacht, die Beklagte schulde ihm gemäß Art.15 Abs. 3 DS-GVO weiterhin eine Kopie seiner von ihr verarbeiteten personenbezogenen Daten. Zu diesen gehörten auch der zwischen ihm und der Beklagten geführte E-Mail-Verkehr sowie diejenigen E-Mails, in denen er genannt werde. Das Arbeitsgericht hat die Klage, soweit sie auf die Erteilung einer Kopie seiner personenbezogenen Daten gerichtet ist, abgewiesen. Das Landesarbeitsgericht hat ihr teilweise entsprochen und sie im Übrigen abgewiesen. Es hat angenommen, der Kläger habe zwar einen Anspruch auf Erteilung einer Kopie seiner personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Ein weitergehender Anspruch, insbesondere auf Kopien des vollständigen E-Mail-Verkehrs, bestehe dagegen nicht. Mit seiner Revision verfolgte der Kläger sein Begehren, soweit er damit unterlegen ist, weiter.

Das BAG hat nun entschieden, dass ein Klageantrag auf Überlassung einer Kopie von E-Mails nicht hinreichend bestimmt sei (iSv. § 253 Abs. 2 Nr. 2 ZPO), wenn die E-Mails, von denen eine Kopie zur Verfügung gestellt werden soll, nicht so genau bezeichnet sind, dass im Vollstreckungsverfahren unzweifelhaft ist, auf welche E-Mails sich die Verurteilung bezieht. Weiter auf DataAgenda lesen

Quelle: Bundesarbeitsgericht, Urteil vom 27. April 2021 – 2 AZR 342/20 –

Foto: bluedesign, Adobe Stock

Abberufung eines DSB: BAG legt Frage dem EuGH vor

Zur Klärung der Frage, ob die Anforderungen des Bundesdatenschutzgesetzes (BDSG) an die Abberufung eines betrieblichen Datenschutzbeauftragten im Einklang mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) stehen, hat der Neunte Senat des Bundesarbeitsgerichts ein Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union gerichtet. Die Parteien streiten über die Wirksamkeit der Bestellung sowie der Abberufung des Klägers zum Datenschutzbeauftragten.

Der Kläger ist Arbeitnehmer der Beklagten und freigestellter Betriebsratsvorsitzender des bei ihr gebildeten Betriebsrats. Daneben ist er stellvertretender Gesamtbetriebsratsvorsitzender in mehreren in Deutschland ansässigen Unternehmen, die zum internationalen X-Konzern gehören, dem auch die Beklagte angehört. Mit Wirkung zum 1. Juni 2015 wurde der Kläger von der Beklagten zum betrieblichen Datenschutzbeauftragten und von den weiteren in Deutschland ansässigen konzernzugehörigen Gesellschaften zum externen Datenschutzbeauftragten bestellt. Ziel seiner Bestellungen war die Erreichung eines konzerneinheitlichen Datenschutzstandards. Im September 2017 meldete der Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit gegenüber der Muttergesellschaft der Beklagten wegen der hauptberuflichen Tätigkeit des Klägers als Betriebsratsvorsitzender und dadurch zu befürchtender Interessenkollisionen Zweifel an der Zuverlässigkeit des Klägers als Datenschutzbeauftragter an. In der Folge traf der Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit unter Bezugnahme auf § 4f BDSG aF die Feststellung, dass der Kläger nicht über die für die Bestellung eines betrieblichen Datenschutzbeauftragten notwendige Zuverlässigkeit verfüge und er nicht wirksam zum betrieblichen Datenschutzbeauftragten bestellt worden sei. Den vollständigen Beitrag finden Sie auf DataAgenda

Studiengang „Digital Administration and Cyber Security“ geht in die zweite Runde

Foto: HS Bund

Im letzten Wintersemester startete an der Hochschule des Bundes für öffentliche Verwaltung (HS Bund) in Brühl der Studiengang „Digital Administration and Cyber Security" – kurz DACS (DataAgenda berichtete). Mit Beginn des Sommersemesters sind weitere 60 Studierende in das Beamtenverhältnis auf Probe übernommen worden. Wir möchten uns nach den Eindrücken des ersten Semesters erkundigen und sprachen hierzu mit Prof. Dr. Marie Bergmann, Regierungsdirektor Fabian Weber und Prof. Dr. Lorenz Franck.

? DataAgenda: Frau Bergmann, Sie sind Professorin für Mathematik und Informatik, beides Fächer, die bereits zum Studienstart eine wesentliche Rolle spielen. Womit geht es los im DACS?

Bergmann: Die theoretische Informatik beginnt mit der Einführung in Datenstrukturen und Algorithmik am Beispiel der Programmiersprache Python. Hier lernen die Studierenden, was und wie ein Computer Daten speichern und mit diesen arbeiten kann. Aber die Leistung von Computern bzw. die Berechenbarkeit hat auch ihre Grenzen. So lernten die Studierenden, dass es gar nicht so schlimm ist, dass man Primfaktoren nicht effizient berechnen kann, denn sonst wären die meisten Verschlüsselungsalgorithmen nicht sicher.

? DataAgenda: Herr Weber, Sie sind hauptamtlich Lehrender im Bereich der technischen Informatik. Worum geht es dort?

Weber: In der technischen Informatik befassen sich die Studierenden mit dem Aufbau und der Funktionsweise von heutigen Rechnern. Beginnend mit dem allgemeinen Verständnis, was es mit den Nullen und Einsen im Binärsystem auf sich hat, entwickelt sich sehr bald ein Verständnis dafür, wie moderne Rechner aufgebaut sind. Die theoretisch erworbenen Kenntnisse dürfen die Studierenden dann sofort in der Praxis bei der Programmierung eines Mikroprozessors anwenden. Zu diesem Zweck wurden für die Studierenden Arduino-Boards beschafft. Dies sind Experimentierpakete, die mit einem fertigen Mikroprozessorboard und einer ganzen Palette an unterschiedlichen Bauteilen bestückt werden können. Die Studierenden schaffen es sehr schnell, eine Reihe von LEDs aufleuchten zu lassen oder auch mal ein Weihnachtslied auf dem eingebauten Summer abzuspielen.

? DataAgenda: Herr Franck, Sie sind als Professor für IT-Recht für die Rechtsthemen zuständig. Werden die Studierenden von Ihnen sofort ins kalte Wasser geworfen?

Franck: Natürlich nicht! In den ersten beiden Semestern werden die Grundlagen gelegt. Zunächst steht unter anderem das Verwaltungsrecht im Vordergrund, denn ohne Verwaltungsrecht wäre ein Studiengang zum Diplom-Verwaltungswirt oder zur Diplom-Verwaltungswirtin kaum denkbar. Wir haben allerdings bereits jetzt erste Ausflüge ins Informationsrecht unternommen, wenn zum Beispiel in unseren Übungsfällen Fragen des IFG oder die elektronische Kommunikation mit Behörden thematisiert wurden. Hierauf kann im Hauptstudium aufgebaut werden, wenn es um das Datenschutzrecht, das IT-Sicherheitsrecht oder das E-Government-Recht geht.

? DataAgenda: Es klingt nach einem sehr breiten Themenspektrum, das hier bedient wird ...

Bergmann: Alle Themen legen den Grundstein für die spätere Spezialisierung zu Themen der Cyber Security oder Digital Administration. Schon bei der Planung des Curriculums wurde daher stets auf eine ausgewogene Mischung zwischen Theorie, Praxis und praktischen Übungsaufgaben gelegt.
Das vollständige Interview finden Sie auf DataAgenda

Foto: HS Bund

Einsicht in die Patientenakte (§ 630g BGB) vs. Auskunftsrecht nach Art. 15 DS-GVO

Foto: momius, Adobe Stock

Wenn sich Patienten über den Inhalt der Behandlungsdokumentation, also ihrer Patientenakte, informieren möchten, kommen mehrere Rechtsnormen in Betracht, auf die sie dieses Begehren stützen können.

In ihrem 29. Tätigkeitsbericht (Abschnitt 3.22) weist die Landesbeauftragte für Datenschutz und Informationsfreiheit im Saarland darauf hin, dass insbesondere das Verhältnis des datenschutzrechtlichen Auskunftsanspruchs gemäß Art. 15 DS-GVO zu dem in § 630g BGB normierten Recht auf Einsichtnahme in die Patientenakte nicht abschließend geklärt zu sein scheint, obwohl die Abgrenzung in der Praxis eine erhebliche Relevanz besitze. Ein Unterschied dürfe bereits darin bestehen, dass Art. 15 Abs. 3 DS-GVO einen Anspruch auf eine kostenlose Kopie der personenbezogenen Daten begründe, während nach § 630g BGB die Kosten für die Kopie der Behandlungsdokumentation dem Patienten in Rechnung gestellt werden dürften.

Das Unabhängige Datenschutzzentrum Saarland stelle bisher bei der Bearbeitung von Anfragen oder Beschwerden in diesem Zusammenhang darauf ab, welches Anliegen der betroffene Patient im konkreten Fall verfolge. Gehe es dem Patienten vorrangig um die Verarbeitung seiner personenbezogenen Daten (z.B. Empfänger, Speicherdauer), könne von einem Auskunftsersuchen nach Art. 15 DS-GVO ausgegangen werden. Stehe dagegen der Inhalt des Behandlungsverlaufs im Vordergrund, wie beispielsweise in Fällen, in denen der Patient seine Akte bei einem Wechsel der Praxis zum neuen Arzt mitnehmen möchte und deshalb eine vollständige Kopie benötige, erscheine § 630g BGB als einschlägige Rechtsgrundlage, zumal der Umfang der Datenkopie, die nach Art. 15 Abs. 3 DSGVO verlangt werden kann, nach wie vor umstritten sei. Lesen Sie den Beitrag weiter auf DataAgenda

Aufsichtsbehörde: Mehr Schutz für Studierende bei Online-Prüfungen

Foto: fizkes, Adobe Stock

In jüngster Vergangenheit mussten sich Gerichte mit der Frage der Zulässigkeit der Einhaltung datenschutzrechtlicher Anforderungen im Rahmen der Durchführung von Kontrollen beschäftigen, die in Zusammenhang mit Online-Prüfungen standen.
Studierende müssen aufgrund der Corona-Pandemie häufig auf Online-Veranstaltungen ausweichen. Prüfungen müssen sie ebenfalls Online ablegen, auch im eigenen Interesse, um keine wertvolle Studienzeit zu verlieren. Um Online-Prüfungen zu beaufsichtigen, setzen Hochschulen häufig digitale „Tools" ein, die mittels Kamera und Mikrofon die Prüfungen überwachen. Auf diese Weise sollen etwaige Betrugsversuche unterbunden und die Chancengleichheit gewahrt werden. Digitale Formate zur Kontrolle von Prüfungen – Online-Proctoring – können aber auch massiv in die Rechte von Studierenden eingreifen. Schützenhilfe erhalten die Studierenden aktuell vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW). Dr. Stefan Brink gibt bekannt, dass seine Behörde das Thema Online-Proctoring jetzt in den Fokus nehme. „Online-Prüfungen sollen Wissen und Fähigkeiten abfragen, nicht Studierende übermäßig überwachen. Online-Proctoring kann maßlos sein und Studierende in äußerst unangenehme Situationen bringen", so der LfDI BW. Es ist nicht so fernliegend, dass der Technik-Einsatz für Studierende in einem starken Maß belastend wirkt, da beim Online-Proctoring Studierende mitunter aufgefordert, die Webcam und das Mikrofon am Gerät dauerhaft während der Prüfung einzuschalten und sicherzustellen, dass keine unerlaubten Hilfsmittel und niemand anderes im Privatraum des Studierenden sind. Auch Eyetracking und das Auslesen der Browserhistorie kommen teilweise zum Einsatz.

Quelle: Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)

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