NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
8/2021

DATAKONTEXT

Levent Ferik

EDITORIAL

Ob nun in der griechischen Antike oder in der Bibel: Oft wird den Überbringern schlechter Nachrichten eine Behandlung zuteil, die sie nicht verdienen und für deren Inhalt sie vor allem nichts können. Wenn die Überbringerin einer solchen Nachricht aber durch die Beschreibung der Umstände, sogar lediglich zu einer Verbesserung des Zustandes für den Verantwortlichen beitragen will, ist diese Behandlung noch weniger nachvollziehbar.

Ein aktuelles Bespiel hierfür dürfte der Umgang der CDU mit den zu Tage getretenen Schwachstellen ihrer App „CDU*connect*“ sein. Die CCC-Aktivistin Lilith Wittmann entdeckte im Mai 2021, dass eine Schwachstelle der App dazu führte, dass zumindest die persönlichen Daten von 18.500 Wahlkampfhelferinnen, mit E-Mail-Adressen & Photos und die persönlichen Daten von 1.350 Unterstützerinnen der CDU inklusive Adresse, Geburtsdatum und Interessen sowie eine halbe Million Datensätze über politische Einstellungen kontaktierter Personen ungeschützt und frei über das Netz zugänglich waren.

In so einem Fall gab im Wesentlichen zwei Offenlegungsmöglichkeiten für Lilith Wittmann:

Direkt die Öffentlichkeit informieren (Full Disclosure) oder erst eine Abstimmung mit den verantwortlichen Stellen durchführen und Einzelheiten zu der Schwachstelle erst dann ggf. veröffentlichen, wenn die Entwickler des Verantwortlichen genügend Zeit hatten, diese zu beheben (Responsible Disclosure). Die CCC-Aktivistin entschied sich für die, vor allem für den Verantwortlichen vorteilhaftere Variante und meldete die Schwachstellen den verantwortlichen Stellen der CDU, dem Bundesamt für Sicherheit in der Informationstechnik und der Berliner Datenschutzbeauftragten (BlnBDI).

Ergebnis: Die CDU schaltete die unsichere Datenbank der App ab UND stellte einen Strafantrag beim LKA Strafantrag gegen Lilith Wittmann. Auf eine solche Reaktion der CDU erfolgte die wohl verdiente Gegenreaktion der Netzgemeinde und des CCC: Unverständnis, Häme (Netzgemeinde) und eine Erklärung des CCC, solche Funde zumindest im Falle der CDU nur noch im Wege des Full Disclosure öffentlich zu machen.

Ob der involvierte Berliner Datenschutzbeauftragte den Datenschutzvorfall als eine Datenpanne im Sinne des Art. 33 DS-GVO bewerten wird, dürfte eine weitere interessante Frage sein. Vor dem Hintergrund der Tatsache, dass es sich hier um Verletzung des Schutzes personenbezogener Daten, die zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten, die unter Art. 9 DS-GVO subsumiert werden können geführt haben könnte, erscheint dieser Ausgang nicht unwahrscheinlich. Informationen nach Art. 9 DS-GVO können regelmäßig besonders kompromittierend sein. Der BlnBDI geht etwa bei unbefugter Kenntnisnahme Dritter von Gesundheitsdaten per se davon aus, dass schwerwiegende Beeinträchtigungen drohen (vgl. BlnBDI TB 2011, S. 166; BlnBDI TB 2014, S. 150, vgl. Franck in Heidelberger-Kommentar DS-GVO/BDSG, Rdnr. 52). Angesichts solcher Reaktionen von Verantwortlichen ist es zudem nachvollziehbar, warum Regelungen wie der Whistleblower-Richtlinie unbedingt auch Vorkehrungen für den Schutz von Hinweisgebern enthalten müssen (vgl. Art. 6 des Entwurfs: „Voraussetzungen für den Schutz von Hinweisgebern“).

Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: MclittleStock, Adobe Stock

Bundeskartellamt bemängelt Daten-schutz-Defizite bei Apps

Die am 09. Juni 2017 in Kraft getretene 9. GWB-Novelle verschafft dem Bundeskartellamt die Befugnis, sogenannte Sektoruntersuchungen auch im Bereich des Verbraucherschutzes durchzuführen.
Das Bundeskartellamt hat in diesem Rahmen die Möglichkeit, Unter-suchungen anzustellen und Problemfelder aufzuzeigen. Im Gegensatz zu seinen kartellrechtlichen Zuständigkeiten, hat das Bundeskartellamt hier jedoch nicht die Möglichkeit, etwaige Rechtsverstöße auch behörd-licherseits abzustellen oder zu sanktionieren.

Weiter auf DataAgenda lesen

Foto: metamorworks, Adobe Stock

Nutzung von Cloud-Diensten durch Bundesverwaltung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Mindeststandard zur Mitnutzung externer Cloud-Dienste in der neuen Version 2.0 veröffentlicht. Der nun durch das BSI 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. Im neuen Mindeststandard sind erstmals zwei Publikationen in einer Veröffentlichung zusammengefasst: Neben dem Mindeststandard zur Nutzung externer Cloud-Dienste gab es bislang einen weiteren Mindeststandard zur Mitnutzung externer Cloud-Dienste. Dieser befasste sich mit dem Sonderfall, dass eine Behörde einen Cloud-Dienst nutzt, aber kein eigenes Vertragsverhältnis mit einem Diensteanbieter besteht, beispielsweise im Rahmen einer Zusammenarbeit mit Dritten. In der Version 2.0 wurde dieses Thema in einem eigenen Kapitel integriert, sodass es nun einen Mindeststandard für beide Nutzungsszenarien gibt.

Bei der klassischen Cloud-Nutzung hat die Bundesbehörde einen Bedarf an einer IT-Leistung, die nicht durch eigene IT-Ressourcen, sondern über einen externen Cloud-Dienst erbracht werden soll. Die Einrichtung nimmt somit die Rolle des Auftraggebers ein.

Hinzu kommen jedoch auch Bereiche, die hier als Mitnutzung bezeichnet werden. Dabei nehmen IT-Anwender einer Einrichtung externe Cloud-Dienste in Anspruch, ohne dass zwischen der Einrichtung und dem eigentlichen Cloud-Anbieter ein Vertragsverhältnis besteht. Somit ist die Einrichtung in diesen Fällen nicht Auftraggeber des Cloud-Dienstes. Insbesondere wenn IT-Anwender im Rahmen von (internationalen) Projekten oder Arbeitsgruppen institutionsübergreifend zusammenarbeiten wollen, wird diese Form der Mitnutzung immer häufiger gewählt.

Foto: MQ-Illustrations, Adobe Stock

Datenschutz im Personalratsbüro

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bietet eine ganze Reihe an Infobroschüren zum Download an, die über den Internetauftritt des BfDI bezogen werden können. Diese geben einen tieferen Einblick in die verschiedenen Aspekte von Datenschutz und Informationsfreiheit. Außerdem sind in den Broschüren jeweils die wichtigsten Gesetze zu den Themen abgedruckt. Als ganz besonderer „Service" können einige der Publikationen in gedruckter Form kostenfrei bestellt werden.
Zum Thema Datenschutz in Zusammenhang mit der Personalaktentenführung oder Umgang mit personenbezogenen Daten im Personalratsbüro existierten bislang nur einzelne Ausführungen, die in den FAQ zum Themenschwerpunkt „Beschäftigtendatenschutz" zu finden waren. Genau diesem Thema hat der BfDI nun einen eigenen Leitfaden mit dem Titel "Leitfaden zur Datenverarbeitung im Personalrat" gewidmet und zusammengefasst, was Personalräte bei der Verarbeitung personenbezogener Daten zu beachten haben. Der Leitfaden soll den Personalvertretungen bei den öffentlichen Stellen des Bundes als Orientierung für den Umgang mit personenbezogenen Daten von Beschäftigten dienen. Er soll einen Überblick über die Rechtslage verschaffen und als Einstieg zu sich konkret stellenden Fragen zulässiger Datenverarbeitung in der Personalratsarbeit weiterhelfen. Der Leitfaden dürfte aber auch geeignet sein, die im Rahmen der Betriebsratsarbeit zu beachtenden Themen ausfindig zu machen (wie bspw. die Problematik „Betriebsrat als eigener Verantwortlicher"), auch wenn der Leitfaden selbstverständlich nicht explizit das BetrVG betrachtet.
Seit Inkrafttreten des sog. Betriebsrätemodernisierungsgesetzes (18.06.2021) dürfte mit der Aufnahme des § 79a BetrVG geklärt sein, dass die datenschutzrechtliche Verantwortlichkeit immer beim Arbeitgeber liegt, auch wenn der Betriebsrat (qua Amt) personenbezogene Daten der Beschäftigten verarbeitet. Diesen Aspekt beleuchtet der Leitfaden im Kapitel „3.1 Datenschutzverantwortung und -kontrolle". Der Personalrat ist zwar nicht Verantwortlicher im Sinne der Datenschutzgrundverordnung – trotzdem trägt er Verantwortung für den Schutz der durch ihn verarbeiteten personenbezogenen Daten der Beschäftigten, so der BfDI in seinem neuen Leitfaden.

Quelle: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Foto: Maksym Yemelyanov, Adobe Stock

Datenschutz und digitale Prüfungsaufsicht

Pandemiebedingt mussten sich auch Hochschulen mit einem Aspekt der Digitalisierung beschäftigen, der bislang wenig im Fokus stand.
Studierende mussten und müssen nach wie vor 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.

Weiter auf DataAgenda lesen

Schufa-Daten zur Insolvenz: Löschungsanspruch möglich

Nach einer aktuellen Entscheidung (Schleswig-Holsteinisches Oberlandesgericht, Urteil vom 2. Juli 2021, Az. 17 U 15/21, Revision ist zugelassen) hat ein Insolvenzschuldner einen Löschungsanspruch gegen die Schufa Holding AG, wenn sie diese Daten aus dem Insolvenzbekanntmachungsportal ohne gesetzliche Grundlage länger speichert und verarbeitet als in der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (InsoBekVO) vorgesehen. Im Jahre 2019 wurde im sog. Insolvenzbekanntmachungsportal die Information veröffentlicht, dass über das Vermögens des Klägers das Insolvenzverfahren eröffnet und ihm am 11. September 2019 durch das Amtsgericht die Restschuldbefreiung erteilt wurde. Diese dort veröffentlichten Informationen pflegte die Schufa in ihren eigenen Datenbestand ein. Der Zweck dieser Datenverarbeitung durch die Schufa: Wie üblich sollten diese Informationen Vertragspartnern bei Auskunftsanfragen zum Kläger mitgeteilt werden.

Weiter auf DataAgenda lesen

Foto: Marco2811, Adobe Stock

BSI veröffentlicht IT-Sicherheitsleitfaden

Foto: hkama, Adobe Stock

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) versucht, Politikerinnen und Politiker mit einem „IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen“ für die Gefahren im Cyberraum zu sensibilisieren.
Die 20 Seiten starke Broschüre, die sich vornehmlich an alle Fraktionen des Bundestages und allen weiteren Parteien richtet, die bei der Bundestagswahl antreten, mag zwar unter dem Eindruck und der Befürchtung entstanden sein, dass Hacker versuchen, mit gezielten Attacken auf Abgeordnete an Material für eine Einflussnahme auf den Bundestagswahlkampf zu erlangen. Jedoch kann angesichts der behandelten generischen Themen festgestellt werden, dass die Inhalte für jede Person einen Mehrwert haben dürften, die sich um Informationssicherheit, Datensicherheit und Datenschutz Gedanken machen (müssen). Die dabei behandelten Themen umfassen:

- Wie können Benutzerkonten und Endgeräte sicher eingerichtet und sicher gehalten werden?
- Hinweise zur Einrichtung von WLAN-Routern und zur Auswahl von Anwendungen.
- Verschlüsselung und Absicherung von Daten mit Backups.
- Umgang mit Kommunikationskanälen wie E-Mail, Messengern und sozialen Netzwerken.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Foto: kittyfly, Adobe Stock

Abgrenzung von Verantwortlichem, Auftragsverarbeiter und Joint Controller

Letztes Jahr hatte der Europäische Datenschutzausschuss (EDSA) im Rahmen einer Konsultation zu den Begriffen „Verantwortlicher, Gemeinsam Verantwortlicher und des Auftragverarbeiter" den Versuch gestartet, eine noch klarere Orientierung für die Praxis zu finden, was die Abgrenzung zwischen diesen angeht. Dazu hatte der EDSA einen Entwurf für eine Stellungnahme zur Abgrenzung von Verantwortlichem, Auftragsverarbeiter und gemeinsam Verantwortlichen veröffentlicht (Guidelines 07/2020 on the concepts of controller and processor in the GDPR).

Die Begriffe „für die Verarbeitung Verantwortlicher", „gemeinsam für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" spielen bei der Anwendung der DS-GVO eine entscheidende Rolle, da sie bestimmen, wer für die Einhaltung der verschiedenen Datenschutzvorschriften verantwortlich ist und wie betroffene Personen ihre Rechte in der Praxis ausüben können. Die genaue Bedeutung dieser Begriffe und die Kriterien für ihre korrekte Auslegung müssen im gesamten Europäischen Wirtschaftsraum (EWR) hinreichend klar und einheitlich sein. Die Begriffe „für die Verarbeitung Verantwortlicher", „gemeinsam für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" sind insofern funktionale Begriffe, als sie darauf abzielen, die Verantwortlichkeiten entsprechend den tatsächlichen Rollen der Parteien zuzuweisen.

Die EDSA hat die finale Version ihrer Guidelines zu „Verantwortlichkeit, Auftragsverarbeitung und gemeinsame Verantwortlichkeit" endlich veröffentlicht.

Eine Service-Offensive für eine leichtere Handhabung der DS-GVO und eine verständlichere Lektüre hat wieder einmal der LfDI Baden-Württemberg gestartet, in dem der zu den neuen Leitlinien des EDSA FAQS (Stand 14.07.2021) erstellt hat. Dort werden die Kernaussagen zusammengefasst. Damit soll ein verständlicher Überblick über die doch recht komplexen Rechtsfragen gegeben werden.
Damit erleichtert der Frage-Antwort-Katalog auch dem Laien den Einstieg in das umfassende Dokument des EDSA und stellt Querverweise zur Verfügung, um die im Einzelfall relevanten Ausführungen zu finden. Zusätzlich tragen konkrete Praxisbeispiele zum Verständnis bei und helfen bei der praktischen Umsetzung, so der LfDI Baden-Württemberg.
Die FAQ des LfDI BW sind hier abrufbar.

Foto: denisismagilov, Adobe Stock

DS-GVO gilt nicht für abgeschaltete Überwachungskameras

Die DS-GVO findet gem. Art. 1 Abs. 1 DS-GVO nur dann Anwendung, wenn auch tatsächlich personenbezogene Daten verarbeitet werden. Zu beachten ist, dass durch sogenannte Kamera-Dummys der Eindruck einer Überwachung und Datenverarbeitung entsteht, sodass auch Videokameras ohne tatsächliche Funktion das Persönlichkeitsrecht betroffener Personen beeinträchtigen können. Eine Datenverarbeitung findet aber nicht statt. Daher können die Vorschriften der DS-GVO und des BDSG keine Anwendung finden (Vgl. ULD, Praxisreihe Datenschutzbestimmungen praxisgerecht umsetzen, Ziffer 8).

Weiter auf DataAgenda lesen

DATA AGENDA
PODCAST

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

Folge #**5**

Geschäfte mit Datenschutzverstößen – Der schmale Grat zwischen Rechtsmissbrauch und Rechtsbehelf

Tim Wybitul

Folge #**6**

Von der Risikoorientierung bis zu einem Rechtsrahmen für künstliche Intelligenz – Datenschutz in Europa zukunftsoffen gestalten

Axel Voss

Folge 5: Geschäfte mit Datenschutzverstößen – Der schmale Grat zwischen Rechtsmissbrauch und Rechtsbehelf

Schadensersatz sieht die DS-GVO als Sanktion neben Bußgeldern vor. In der Praxis mehren sich solche Ansprüche und werden für Wirtschaftsunternehmen zum Problem. Die GDD weist auf provozierte Datenschutzverstöße hin, die zum Geschäftsmodell werden. Darf man mit Schadensersatzansprüchen Geschäfte machen? Wo liegt die Grenze zum Rechtsmissbrauch? Um was für Fälle geht es in laufenden Gerichtsverfahren? Steckt ein Geschäftsmodell hinter diesen Verfahren? Wie wird der EuGH sich wohl positionieren? Welche Möglichkeiten haben nationale Aufsichtsbehörden und der Gesetzgeber, möglichem Rechtsmissbrauch entgegenzuwirken?
Zum Podcast bitte hier klicken.

Folge 6: Von der Risikoorientierung bis zu einem Rechtsrahmen für künstliche Intelligenz – Datenschutz in Europa zukunftsoffen gestalten

Im DataAgenda Datenschutzpodcast mit dem EU-Datenschutzpolitiker Axel Voß geht es um Perspektiven für den europäischen Datenschutz unter der Überschrift „Von der Risikoorientierung bis zu einem Rechtsrahmen für künstliche Intelligenz – Datenschutz in Europa zukunftsoffen gestalten“. Hat sich der risikobasierte Ansatz der DS-GVO bisher bewährt? Wie geht es mit der ePrivacy-VO weiter und guckt sich der europäische Gesetzgeber in Zukunft vielleicht etwas vom TTDSG in Deutschland und den Regelungen zu Datentreuhändern ab, um einen fairen Wettbewerb zu ermöglichen? Und in die Zukunft geblickt: Was unternehmen wir, wenn Maschinen schlauer werden als Menschen? Wie sieht es mit den rechtlichen Vorgaben Europas für Künstliche Intelligenz aus?
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