Datenschutz newsbox

Ausgabe 1 2018

DATAKONTEXT

Editorial

Hätten Sie gedacht, dass man Google Street View nutzen kann, um Wählerverhalten mittels Big-Data-Techniken und einer Prise KI zu prognostizieren?

Lassen sich mittels KI und Gesichtserkennung tatsächlich Aussagen darüber treffen, ob eine Person homosexuell ist? Und wenn ja, wofür sollte diese „Technologie" gut sein?

Die Befürchtung, dass Vorhaben dieser Art nicht immer zum Wohle der Betroffenen führen, ist nicht ganz von der Hand zu weisen. So plant China, bis zum Jahr 2020 ein sog. social credit System zu etablieren. Diese soll sowohl für juristische als auch natürliche Personen verpflichtend sein. Das System soll in der Lage sein, aus unterschiedlichen Daten wie Nutzungsverhalten im Internet, Kreditwürdigkeit, Zuverlässigkeit ein Score zu bilden. Ein hoher Score käme dann einem Statussymbol gleich. Der Score könnte Auswirkungen auf den Zugang zu Schulen, Ausbildung, Jobs und weiteren Lebensbereichen haben.

Bei solch einer digitalen Dystopie, in der die neuen Technologien als Kontroll- und Überwachungsinstruments für mehr als eine Milliarde Menschen missbraucht werden könnten, klingen die „Aufreger" hierzulande fast harmlos. Aber hier, wie in anderen Bereichen muss gelten: „Wehret den Anfängen!", meint Ihr

Levent Ferik

Leitfaden für das Forderungsmanagement nach DS-GVO

Der Bundesverband Deutscher Inkasso-Unternehmen (BDIU) hat einen Leitfaden zur Anwendung und Umsetzung der Datenschutz-Grundverordnung (DS-GVO) im Forderungsmanagement veröffentlicht. Damit möchte der Verband vor allem seine Mitgliedsunternehmen bei der Umstellung der internen Prozesse auf die neuen Anforderungen unterstützen, die ab dem 25. Mai 2018 zu berücksichtigen sind.

Der BDIU gewährt mit dem veröffentlichten »Best Practice Guide 1.0« auch einen Überblick zu den einzelnen Regelungen der Verordnung und gibt darüber hinaus praktische branchenbezogene Tipps, wie die rechtlichen Vorgaben von den Inkassodienstleistern effizient umgesetzt werden können. Der Best Practice Guide beleuchtet die DS-GVO hauptsächlich mit Blick auf die Datenverarbeitung personenbezogener Daten von Forderungsschuldnern. Die Grundsätze zur Verarbeitung müssen aber auch bei anderen natürlichen Personen berücksichtigt werden, z. B. gegenüber Mitarbeitern.

Quelle: Bundesverband Deutscher Inkasso-Unternehmen e.V

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Studie zur praktischen Umsetzung des Rechts auf Datenübertragbarkeit

Ab 2018 können Nutzer ihre Daten von einem Anbieter zu einem anderen mitnehmen – von einem sozialen Netzwerk zum anderen; von einer Versicherung zur nächsten. Neben diesen naheliegenden Möglichkeiten sind auch noch viele andere Datentransfers denkbar. Was nach großer Freiheit für Verbraucher und nach einer Chance klingt, bestehende Monopole im Digitalmarkt aufzubrechen, kann allerdings auch Risiken mit sich bringen.

Zu diesem Ergebnis kommt eine aktuelle Studie der vom Bund gegründeten Stiftung Datenschutz. Denn für die Umsetzung des Rechts auf Datenübertragbarkeit brauchen Wirtschaft und Verbraucher noch Präzisierung und Aufklärung. Die Studienautoren zeigen auf, dass ansonsten Datenschutzrisiken drohen oder das neue Schutzinstrument ins Leere laufen kann.

Aus diesem Grund untersucht die Stiftung Datenschutz in der vorliegenden Studie rechtliche, technische und verbraucherbezogene Implikationen des neuen Rechts und gibt Empfehlungen zur Nutzbarmachung des neuen Instruments. Zunächst wird der Regelungsgegenstand von Art. 20 DSGVO aufgezeigt und auf wesentliche Problemfelder bei der Umsetzung der Norm eingegangen. Sodann werden bestehende nationale und internationale Lösungsansätze zur Datenportabilität vorgestellt und die auf den Call for Papers der Stiftung eingegangenen Beiträge sowie Empfehlungen externer Sachverständiger ausgewertet. Schließlich gibt die Studie Empfehlungen bezüglich der Zielsetzung der Norm, der Bestimmung des Anwendungsbereichs sowie hinsichtlich möglicher Umsetzungsstrategien und technischer Realisierung.

Quelle: Stiftung Datenschutz

BfDI informiert über die ePrivacy-Verordnung

Während die meisten Verantwortlichen noch mit der Umsetzung der Europäischen Datenschutz-Grundverordnung beschäftigt sind, rückt bereits eine andere Verordnung in den Fokus: die sog. ePrivacy-Verordnung.

Hinter dem Begriff E-Privacy verbergen sich europarechtliche Regelungen, die ergänzend zu den allgemeinen datenschutzrechtlichen Vorschriften einen umfassenden Schutz der Privatsphäre sowie der Vertraulichkeit der Kommunikation bei der Nutzung von elektronischen Kommunikationsmitteln gewährleisten sollen. Hiermit soll vorrangig den besonderen Umständen und Herausforderungen bei der elektronischen Kommunikation als Kernelement der fortschreitenden Digitalisierung Rechnung getragen werden. Darüber hinaus dienen die Regelungen auch dazu, europaweit gleiche Wettbewerbsbedingungen für alle betroffenen Marktteilnehmer zu schaffen. Insoweit ist E-Privacy auch einer der Eckpunkte eines digitalen Binnenmarkts.

Ein Infoblatt der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) informiert über die Kernpunkte der Verhandlungen. Nach der Datenschutz-Grundverordnung verhandeln die EU-Institutionen derzeit über den zweiten Baustein der Reform des Europäischen Datenschutzrechts. Während die bereits beschlossene Datenschutz-Grundverordnung ab 25. Mai 2018 technikneutral den Schutz personenbezogener Daten in der EU regelt, soll die ePrivacy-Verordnung speziell den Schutz der Privatsphäre bei der Nutzung elektronischer Kommunikationsmitteln neufassen. Über die Hintergründe der Verhandlungen in Brüssel informiert ein Infoblatt der BfDI aus der Reihe „Datenschutz kompakt“.

Quelle: Download Datenschutz kompakt: E-Privacy-Verordnung (PDF, 111KB)

Aktualisierte Arbeitshilfen zur Datenschutz-Folgenabschätzung

Im vom BMBF geförderten Forum „Privatheit“ setzen sich Expertinnen und Experten aus sieben wissenschaftlichen Institutionen interdisziplinär mit Fragestellungen zum Schutz der Privatheit auseinander. Das Projekt wird vom Fraunhofer ISI koordiniert. Weitere Partner sind das Fraunhofer SIT, die Universität Duisburg-Essen, das Wissenschaftliche Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel, die Eberhard Karls Universität Tübingen, die Ludwig-Maximilians-Universität München sowie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

Der Forschungsverbund Forum „Privatheit“ hat das White Paper „Datenschutz- Folgenabschätzung – Ein Werkzeug für besseren Datenschutz“ aktualisiert und konkretisiert. Die dritte, überarbeitete Auflage soll Unternehmen, Behörden und sonstigen datenverarbeitenden Organisationen sowie den Datenschutz-Aufsichtsbehörden Hilfestellung bei der Ausgestaltung und praktischen Durchführung einer Datenschutz-Folgenabschätzung geben.

Mit Einführung der EU-Datenschutz-Grundverordnung wird die Durchführung einer Folgenabschätzung ab Mai 2018 für Datenverarbeiter verpflichtend. Ziel der Datenschutz-Folgenabschätzung ist es, die durch Datenverarbeitungen entstehenden Risiken für betroffene Personen abzuschätzen und zu minimieren.

Auch die Artikel-29-Datenschutz-Gruppe hat, ihr Working Paper zum Thema „Datenschutz-Folgenabschätzung“ vor einiger Zeit aktualisiert. Seit wenigen Tagen steht das Working Paper mit dem Namen „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA)“ und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ auch in deutscher Sprache zur Verfügung.

Artikel-29-Datenschutzgruppe veröffentlicht neue Working-Paper

Die Artikel-29-Datenschutzgruppe hat zwei neue Working-Paper online gestellt. Das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes begrüßt Kommentare zu den Leitlinien für die Einwilligung gemäß der Verordnung 2016/679 (wp259) und zu den Leitlinien für Transparenz gemäß der Verordnung 2016/679 (wp260). Diese Stellungnahmen sind bis spätestens 23. Januar 2018 an die folgenden Adressen zu richten: JUST-ARTICLE29WP-SEC@ec.europa.eu und presidenceg29@cnil.fr.

Die Working-Paper können wie folgt abgerufen werden:
Guidelines on Consent under Regulation 2016/679, wp259 (pdf)

Artikel-29-Datenschutzgruppe fordert Nachbesserungen am EU-US Privacy-Shield

Vom 18. bis 19. September 2017 fand die erste jährliche Überprüfung der Funktionsweise des „EU-US Privacy Shield“ in Washington D.C. statt. Diese regelmäßige gemeinsame Überprüfung durch die Europäische Kommission und die US-Regierung basiert auf der Angemessenheitsentscheidung zum Privacy Shield. Dieser Prozess entstand nach den Vorgaben des Europäischen Gerichtshofs im wegweisenden Schrems-Urteil (C-362/14) zur Safe Harbor-Entscheidung der Kommission.

An dieser Überprüfung haben sich acht Vertreter der in der Artikel 29-Datenschutzgruppe versammelten europäischen Datenschutzbehörden beteiligt, darunter zwei Vertreter aus Deutschland, einer davon aus der BfDI. Die Vertreter der Datenschutzbehörden haben sich aktiv in die Überprüfungsprozesse eingebracht. Die ausführlichen Ergebnisse der Überprüfung sind in einem Bericht der Artikel 29-Datenschutzgruppe zusammengefasst, der zusammen mit der korrespondierenden Pressemitteilung der Artikel 29-Datenschutzgruppe auf der Website der BfDI abrufbar ist.

Die Artikel 29-Gruppe der europäischen Datenschutzbehörden hat von der EU-Kommission Nachbesserungen am Privacy Shield für die Übermittlung von personenbezogenen Daten in die USA gefordert. Derzeit hält es die Artikel 29-Gruppe für fraglich, ob Daten von EU-Bürgern in den USA so gut geschützt werden wie in der EU.
Die europäischen Datenschutzbehörden haben die Europäische Kommission aufgefordert, in Nachverhandlungen mit der US-Regierung entscheidende Verbesserungen des Privacy Shield-Mechanismus zu erzielen. Die Datenschutzbehörden halten es nach der ersten gemeinsamen Überprüfung des Privacy Shield weiterhin für fraglich, ob das vom Privacy Shield geschaffene Datenschutzniveau in den USA tatsächlich der Sache nach gleichwertig mit dem Datenschutzniveau in der EU ist. Dies hatte der Europäische Gerichtshof (EuGH) im sogenannten Schrems-Urteil gefordert, durch das die Vorgängerregelung Safe Harbor gekippt wurde.

Quelle: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Tool zur Benachrichtigung bei Datenpannen

ENISA (Europäische Agentur für Netz-und Informationssicherheit) hat in Zusammenarbeit mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (bfDI) ein Tool zur Meldung von Verstößen gegen die Datenschutzbestimmungen (Datenpanne) entwickelt. Der Zweck des Tools besteht insbesondere darin, die Online-Vervollständigung und Übermittlung einer Mitteilung über die Verletzung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen an die zuständige Behörde zu ermöglichen. Sie deckt alle Arten von Datenschutzverletzungen und alle Arten von Unternehmensbereichen ab, ob öffentlich oder privat.

Auf der Grundlage der Eingabe der Meldung stellt das Tool der zuständigen Behörde auch eine Bewertung der Schwere des Verstoßes zur Verfügung. Die Bewertung stützt sich auf die einschlägige Methodik zur Bewertung der Schwere von Verstößen gegen personenbezogene Daten, die von der ENISA in Zusammenarbeit mit den Datenschutzbehörden Griechenlands und Deutschlands entwickelt wurde.

Das Tool steht allen interessierten Parteien, insbesondere den zuständigen nationalen Behörden, die die Meldung von Verstößen gegen die Datenschutzbestimmungen durch die für die Verarbeitung Verantwortlichen in ihren Ländern erleichtern möchten, kostenlos zur Verfügung. Interessierte, die das Tool testen möchten, werden gebeten, eine E-Mail an folgende Adresse zu senden: isdp@enisa.europa.eu

EuGH urteilt zum Auskunftsrecht

Gemäß Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person.
In seinem Urteil vom 20. Dezember 2017 hebt der Gerichtshof hervor, dass ein Prüfling in einer berufsbezogenen Prüfung eine natürliche Person ist, die entweder direkt über ihren Namen oder indirekt über eine Kennnummer, die auf der Prüfungsarbeit oder einem Deckblatt der Prüfungsarbeit angebracht sind, identifiziert werden kann. In diesem Zusammenhang sei es unerheblich, ob der Prüfer den Prüfling zum Zeitpunkt der Korrektur und der Bewertung der Prüfungsarbeit identifizieren kann oder nicht.
Die in einer berufsbezogenen Prüfung gegebenen schriftlichen Antworten und etwaige Anmerkungen des Prüfers zu diesen Antworten stellten personenbezogene Daten des Prüflings dar, hinsichtlich derer er grundsätzlich ein Auskunftsrecht hat. Es diene nämlich dem mit dem Unionsrecht verfolgten Ziel, den Schutz des Rechts auf Privatsphäre natürlicher Personen in Bezug auf die Verarbeitung von sie betreffenden Daten sicherzustellen, dem Prüfling ein solches Recht zu gewähren.

Des Weiteren prüft der Gerichtshof in der Rechtssache C-434/16 Peter Nowa /Data Protection Commissioner, ob die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers dazu Informationen über den Prüfling darstellen. Er stellt insoweit klar, dass in der Verwendung des Ausdrucks „alle Informationen“ im Zusammenhang mit der Bestimmung des Begriffs „personenbezogene Daten“ in der Richtlinie das Ziel des Unionsgesetzgebers zum Ausdruck komme, diesem Begriff eine weite Bedeutung beizumessen. Er sei nicht auf sensible oder private Informationen beschränkt, sondern umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen „über“ die in Rede stehende Person handelt. Die letztgenannte Voraussetzung sei erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist. Die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung stellen solche Informationen dar, die mit seiner Person verknüpft sind.
Der Gerichtshof stellt weiter fest, dass die in der Richtlinie vorgesehenen Rechte auf Auskunft und Berichtigung auch in Bezug auf die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers dazu gerechtfertigt sein können.

Quelle: EuGH

BayLDA veröffentlicht Muster zur Auftragsverarbeitung

Zur Anpassung der Datenschutzorganisation an die neuen Anforderungen der DS-GVO gehört unter anderem die Überprüfung bestehender Vertragsverhältnisse sowie die Anpassung der Vertragsmuster für zukünftige Outsourcing-Dienstleistungen. Für den Bereich der Auftragsverarbeitung sind viele Einzelfragen noch in der Diskussion, sei es die Abgrenzung zur Funktionsübertragung oder zur gemeinsamen Verantwortlichkeit, das Fortbestehen der bisherigen Privilegierung von Auftragsverhältnissen oder schlicht die Anwendung auf Fernwartungsvorgänge. Diese Fragen müssen durch Wissenschaft und Praxis und insbesondere durch den noch zu konstituierenden Europäischen Datenschutzausschuss befriedigend gelöst werden.

Welche Änderungen sich bei der Auftragsverarbeitung nach dem neuen Recht grundsätzlich ergeben, hatte das BayLDA bereits im Oktober 2016 in dem Kurzpapier „Auftragsverarbeitung nach der DS-GVO“ (Nr. 10) zusammengefasst und veröffentlicht (siehe: www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf). In Kürze soll ergänzend dazu ein gemeinsames Papier aller deutschen Datenschutzaufsichtsbehörden veröffentlicht werden.

Um den Verantwortlichen eine Orientierung dafür zu geben, wie nach der DS-GVO der erforderliche Vertrag zur Auftragsverarbeitung abgefasst werden sollte, hat das BayLDA nun auch eine Formulierungshilfe entworfen, die in den Grundzügen mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit entwickelt und abgestimmt wurde. Dieses Muster gibt Anhaltspunkte dafür, welche Inhalte in derartigen Verträgen bei vielen Fallkonstellationen geregelt werden sollten. Bei abweichenden Sachverhalten ist selbstverständlich eine entsprechende Anpassung vorzunehmen. Die Formulierungshilfe finden Sie auf der Homepage des BayLDA unter: www.lda.bayern.de/media/muster_adv.pdf

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Fälle aus der Praxis zum Landesinformationsfreiheitsgesetz Baden-Württemberg

Seit dem 1. Januar 2016 müssen sich alle öffentlichen Stellen in Baden-Württemberg mehr Transparenz gefallen lassen. An diesem Tag ist das Landesinformationsfreiheitsgesetz Baden-Württemberg (LIFG) in Kraft getreten. Die spannendsten Fälle in diesem Bereich hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Stefan Brink, Ende Dezember 2017 in einer Pressekonferenz vorgestellt. Für das Treffen mit Journalistinnen und Journalisten hatte der LfDI aus den interessantesten Fällen ein Päckchen geschnürt und diese im Anschluss diskutiert. Neben den wichtigsten Entscheidungen der Gerichte kamen Fälle aus der eigenen Amtsstube zur Sprache.
Eine Zusammenfassung der Fälle finden Sie hier: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/12/Bestenliste-Informationsfreiheit-Pressekonferenz.pdf

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit

LfDI MV: Fragenbogenaktion zum Stand der DS-GVO im Gesundheitsbereich

Sowohl der LfDI Niedersachsen als auch das BayLDA haben schon in der Vergangenheit mit einem Fragenkatalog die entsprechenden Verantwortlichen für die zukünftigen Anforderungen sensibilisiert, die die DS-GVO in wenigen Monaten mit sich bringen wird. Nun wendet sich der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) an die Ärztinnen und Ärzte in Mecklenburg-Vorpommern mit einer Fragebogenaktion zum Stand der Anpassungen an die neue Datenschutz-Grundverordnung. Hintergrund ist natürlich auch hier die Europäische Datenschutzgrundverordnung, die ab dem 25. Mai 2018 in der gesamten Europäischen Union gilt. Sie knüpft vor allen Dingen an die Verarbeitung von Gesundheitsdaten besonders strenge Vorschriften und sie legt fest, dass Bußgelder bei Verstößen abschreckend, das heißt hoch sein müssen. Außerdem droht den Arztpraxen, dass Patienten bei Datenpannen zivilrechtlich Schadenersatz durchsetzen.

Der Landesbeauftragte für Datenschutz in Mecklenburg-Vorpommern, Heinz Müller, ist derjenige, der mit seinen Mitarbeitern Verstöße feststellen und ahnden muss. Er selbst möchte aber viel lieber, dass es gar nicht zu Verstößen kommt. Also heißt seine Devise: Information, Aufklärung, Beratung. „Die bisherigen Beratungsanfragen zur Grundverordnung aus dem Gesundheitsbereich sind jedoch noch überschaubar“, stellt Müller fest. Um vermehrt Ärzte für das Problem zu sensibilisieren und um zielgenau in Schulungen und bei der Öffentlichkeitsarbeit auf die Probleme der Ärztinnen und Ärzte eingehen zu können, führt Müller eine Umfrage zum Datenschutz in den Arztpraxen durch. Fragebögen wurden an eine repräsentative Anzahl zufällig ausgewählter Ärzte aller Fachbereiche in Mecklenburg-Vorpommern verschickt. „Wir wissen, dass Ärzte sich um ihre Patienten kümmern und nicht Papier bearbeiten wollen. Der Fragebogen soll daher mit möglichst geringem Zeitaufwand bearbeitet werden können. Allerdings ist die Beantwortung in einer festgelegten Frist verpflichtend“, erklärt Heinz Müller. Wer als Angehöriger eines Heilberufs den Selbsttest wagen möchte, findet den Fragebogen auch auf der Homepage des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: www.datenschutz-mv.de. Für Rückfragen zu der Aktion sowie allgemein zum Datenschutz in der Arztpraxis steht der Landesbeauftragte für Datenschutz Mecklenburg-Vorpommern gern zur Verfügung.

Quelle: Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV)

Katholische Kirche veröffentlicht Praxisleitfäden zur DS-VO

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands gibt eine neue Schriftenreihe „Praxishilfen“ zum Umgang mit den Bestimmungen des neuen Gesetzes über den kirchlichen Datenschutz (KDG) heraus.

Die Schriftenreihe, die zunächst mit 18 Broschüren zu den zentralen Themen des KDG erscheint, dient als erste Orientierung, wie nach Auffassung der Diözesandatenschutzbeauftragten das KDG im praktischen Vollzug angewendet werden sollte. Sie kann noch keine verbindliche Auslegung bieten, sondern stellt die gegenwärtige Interpretation der neuen Vorschriften durch die Diözesandatenschutzbeauftragten dar.

Die Broschüren stehen mit Erscheinen zum Download auf der Homepage des Katholischen Datenschutzzentrums zur Verfügung:
https://www.katholisches-datenschutzzentrum.de/infothek/

Quelle: Katholisches Datenschutzzentrum