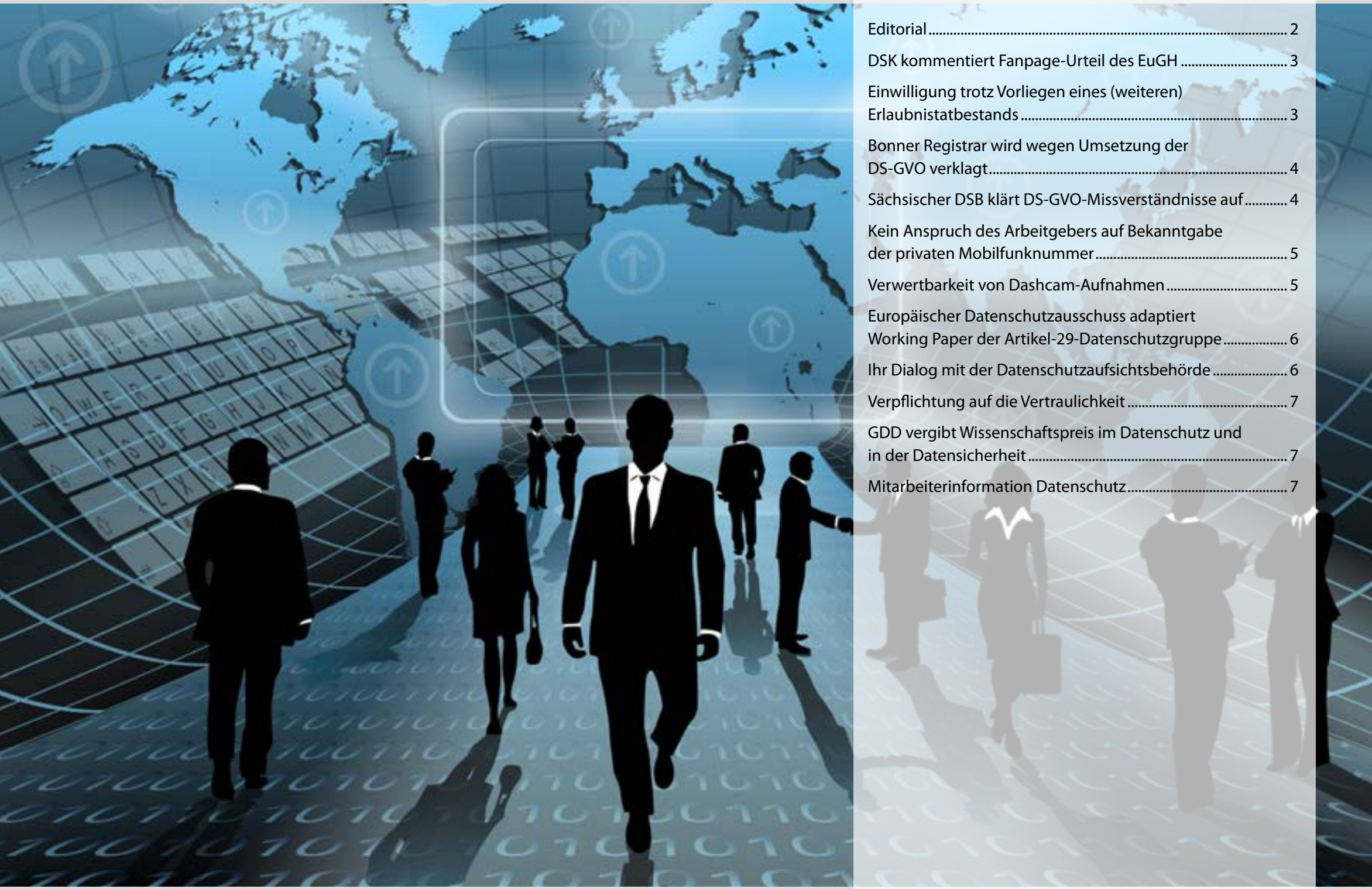
Datenschutz newsbox

Ausgabe 6 2018



DATAKONTEXT

Editorial

Ein paar Wochen nach Inkrafttreten der DS-GVO ist die offensichtlichste Erkenntnis:

Die Welt dreht sich weiter. Wir leben alle noch.

Eine der Befürchtungen der letzten Wochen vor dem 25. Mai 2018 war: Es wird eine „Abmahnwelle" geben. Nach Inkrafttreten der DS-GVO gab es wohl einige Abmahnungen, von einer Abmahnwelle kann aber kaum gesprochen werden: Bei den bisherigen Abmahnungen standen die Verwendung von Google Fonts und eine Datenschutzerklärung im Vordergrund.

Die Angst vor Sanktionen durch die Datenschutzaufsichtsbehörden scheint jedoch weiterhin (in überzogenem Maße) vorhanden zu sein. Das mag damit zusammenhängen, dass – nach Angaben des BITKOM – nur ein Viertel (24 Prozent) der Unternehmen in Deutschland bis zum 25. Mai 2018 aus eigener Perspektive vollständig konform mit den neuen Regeln war sein dürften.

Aktuell lässt sich beobachten, dass die deutschen Aufsichtsbehörden die Chance versäumen, mit einem einheitlicheren Auftreten schon auf nationaler Ebene einen Vorgeschmack auf eine stärkere Harmonisierung des europäischen Datenschutzes zu geben. Zwei Beispiele, dass die Aufsichtsbehörden nach wie vor nicht mit einer Stimme sprechen, sind die sog. Positivlisten gem. Art. 35 Abs. 4 DS-GVO und die Meldung des DSB an die Aufsichtsbehörde gem. Art. 37 Abs. 7 DS-GVO.

Insgesamt zehn Aufsichtsbehörden (inklusive BfDI) haben eine solche Liste veröffentlicht. Eine deutschlandweit einheitliche Liste gibt es also (noch) nicht.

Gemäß Art. 37 Abs. 7 sind die Daten des Datenschutzbeauftragten den Aufsichtsbehörden mitzuteilen. Die Umsetzung der Meldemöglichkeit ist jedoch – je nach Aufsichtsbehörde – sehr unterschiedlich erfolgt. Einige Aufsichtsbehörden stellen für die Meldung ein Online-Formular zur Verfügung. Ansonsten soll bzw. kann die Meldung per Post oder Telefax erfolgen. Die meisten Aufsichtsbehörden haben die Meldung am 25. Mai 2018 erhalten. Andere geben an, dass unterlassene Meldungen der Kontaktdaten der/des Datenschutzbeauftragten während einer Übergangszeit bis zum 31.12.2018 nicht als Datenschutzverstöße verfolgen oder geahndet werden."

Hier dürfte ohne größere Not das Vertrauen in eine kohärentere (Zusammen-)Arbeit der deutschen Aufsichtsbehörden verschenkt worden sein. Auf europäischer Ebene scheint die Zusammenarbeit bereits besser angelaufen zu sein. Der Europäische Datenschutzausschuss (EDSA) hat in seiner ersten konstituierenden Sitzung am 25. Mai 2018 zahlreiche Positionen der der Artikel-29-Datenschutzgruppe bestätigt.

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

DSK kommentiert Fanpage-Urteil des EuGH

Nachdem die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bereits das Urteil des EuGH zur gemeinsamen Verantwortlichkeit von Facebook-Fanpage-Betreibern und Facebook selbst in einer Pressemitteilung kommentiert hatte, hat auch die Datenschutzkonferenz eine Entschließung zu dem Urteil des EuGH veröffentlicht (Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern). Sowohl BfDI als auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
(DSK) sind der Auffassung, dass der vom Gericht festgelegte Grundsatz der gemeinsamen Verantwortlichkeit auch auf die DS-GVO übertragbar ist, auch wenn das Urteil noch auf der vor der Datenschutz-Grundverordnung geltenden Rechtslage beruht.
Die BfDI rät vor allem öffentlichen Stellen, die Entscheidung des EuGH zum Anlass zu nehmen, die Rechtskonformität ihrer Fanpages zu überprüfen und – soweit erforderlich – Facebook zu datenschutzrechtlichen Anpassungen zu bewegen. Die DSK sehe in Konsequenz des Urteils nicht mehr die Möglichkeit, dass sich die Betreiber von Facebook-Fanpages allein auf die Verantwortung von Facebook verweisen. Diese seien jetzt selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzern ihrer Fanpage.
Im Einzelnen sei Folgendes zu beachten:

- Wer eine Fanpage besuche, müsse transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gelte sowohl für Personen, die bei Facebook registriert seien, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
- Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt – sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse – sei grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderungen der DS-GVO erfüllt.
- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern solle in einer Vereinbarung festgelegt werden, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung müsse in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen könnten.

Einwilligung trotz Vorliegen eines (weiteren) Erlaubnistatbestands

Aus der Reihe: „Die Aufsichtsbehörde antwortet …“

Frage 1 des GDD Erfa-Kreises Würzburg:

Ist es falsch bzw. datenschutzrechtlich unrechtmäßig, wenn ich für eine Datenverarbeitung, die mir bereits das Gesetz in z.B. § 28/32 BDSG und Art. 6 I b) ff. DS-GVO (beispielsweise die Verarbeitung von Mitarbeiterdaten in der Personalakte) gestattet, zusätzlich noch eine Einwilligung (mit Widerrufshinweis) einhole?

Antwort des BayLDA:

Es ist falsch, für eine zu Vertragszwecken erforderliche Verarbeitung personenbezogener Daten noch eine Einwilligung einzuholen, da einer solchen Einwilligung keine freie Entscheidung zugrunde liegen kann; die Daten sind ja für den Vertragszweck erforderlich.

Frage 2 des GDD Erfa-Kreises Würzburg:

Wie lange soll man Log-Daten zur Gewährleistung der Eingabekontrolle aufbewahren? Standardmäßig können Log-Daten für eigene Zwecke bis zu sieben Tage aufbewahrt werden. Gilt dies auch für den Zweck der Eingabekontrolle?

Antwort des BayLDA:

Die Eingabekontrolle gibt es unter der DS-GVO nicht mehr. Es stellt sich bei der Frage der Aufbewahrungsdauer immer die Frage, welche Art von personenbezogenen Daten aufgezeichnet wird, und was der konkrete Zweck der Aufzeichnung ist. Soll z.B. in einem Arztinformationssystem nachvollziehbar gemacht werden, wer Daten eines Patienten eingegeben/geändert hat, könnte die Aufbewahrungsdauer dieser Log-Datensätze ebenso lange wie die Dauer der Aufzeichnung der Patientendaten als solche (z.B. so lange eine Behandlung andauert) sein. Dies dürfte in den meisten Fällen deutlich länger als sieben Tage sein.

Bonner Registrar wird wegen Umsetzung der DS-GVO verklagt

Der in Bonn ansässige Domain-Registrar EPAG Domainservices GmbH wird von der Internet-Verwaltung ICANN wegen der Aufbewahrung der WHOIS-Daten für Domains im Rahmen eines einstweiligen Rechtsschutzverfahrens verklagt. Zum Portfolio der EPAG gehört als Domain-Name-Registrar die Registrierung von Internet-Domains. Registrare werden je nach Top-Level-Domain (TLD) von der Internet Corporation for Assigned Names and Numbers (ICANN) oder einer Domain Name Registry akkreditiert. Bei dem Bonner Registrar EPAG handelt es sich um eine Tochter des kanadischen Unternehmens Tucows.

Schon seit geraumer Zeit gibt es Reibungspunkte zwischen Registraren und der ICANN, was die konkrete Umsetzung der DS-GVO angeht. Bereits im Jahr 2016 führten die Bemühungen zweier niederländischer Registrys dotAmsterdam BV und FRLRegistry BVR zur Umsetzung der DS-GVO zu einem Streit mit der ICANN. Der Streit entzündete sich an der Änderung der Whois-Policy der beiden Registrare. dotAmsterdam BV und FRLRegistry BVR gingen dazu über, die Kontaktdaten der Domaininhaber nicht mehr in der Whois-Datenbank zu veröffentlichen. Nach kurzer Zeit kam von der ICANN ein Rüffel und der Hinweis, dass diese eine vorsätzliche Vertragsverletzung in der Handhabung der neuen Whois-Policy sehe. Diese könne zum Entzug der TLDs führen. Der Registrar-Akkreditierungsvertrag mit der ICANN besagt, dass die Registry private Inhaberdaten, wie Name, Adresse, Telefonnummer und Emailadresse, an die ICANN übermitteln muss. Die in diesem Zusammenhang eingeschaltete niederländische Datenschutzbehörde sah in der neuen Whois-Policy jedoch eine rechtskonforme Umsetzung der damals herannahenden DS-GVO.

Auch der Ersuch von gerichtlicher Hilfe durch die ICANN beim Landgericht Bonn in Form des einstweiligen Rechtsschutzverfahrens hat seinen Kern in der Umsetzung der DS-GVO und der Verschlankung der Informationen innerhalb der Whois-Datenbank durch die EPAG. Im Kern stimmen ICANN und Tucows/Epag nicht darin überein, welche Auswirkung die DS-GVO auf den Akkreditierungsvertragsvertrag hat, wie die Geschäftsführerin der EPAG, Ashley La Bolle, in einer aktuellen Stellungnahme bezüglich der Klage wissen lässt.

Die Antwort auf die Frage, ob die Entscheidung, künftig keine Daten zum Tech-C („Technical Contact“) und Admin-C („Administrative Contact“) zu erheben, Teil der notwendigen Umsetzungsmaßnahmen der DS-GVO darstellt, und wenn ja, ob diese dann tatsächlich zu einer Verletzung des Akkreditierungsvertrags zwischen der EPAG und der ICANN führen können, wird eines der Ergebnisse des Verfahrens sein, welche auch für andere Registrare für mehr Rechtssicherheit sorgen dürfte.

Sächsischer DSB klärt DS-GVO-Missverständnisse auf

Auch nach Wirksamwerden der DS-GVO scheinen Missverständnisse und Irritation auf Anwenderseite groß. Der Sächsische Datenschutzbeauftragte klärt über vorhandene Missverständnisse rund um die Anwendung der DS-GVO auf und versucht damit, Unsicherheiten zu beseitigen. Dazu hat sich Andreas Schurig fünf prägnante Beispiele herausgegriffen, um einige der identifizierten Fehleinschätzungen und Missverständnisse aus der Welt zu räumen. Dabei werden die Meldungen, die in Zusammenhang mit der bevorstehenden Anwendbarkeit der DS-GVO kursieren unter die Lupe genommen.

Es kursieren viele Meldungen und Meinungen in Medien, wonach zukünftig insbesondere kleine und mittlere Unternehmen oder auch Vereine mit einem unverhältnismäßigen bürokratischen Aufwand belastet würden, und viele Datenverarbeitungen in der bisher praktizierten Form nicht mehr oder nur noch mit individueller Einwilligung der betroffenen Person zulässig sein sollen. Die DS-GVO mit ihren überzogenen Vorgaben einerseits und den drohenden Sanktionen andererseits werde als großes Risiko für den Fortbestand der Unternehmen dargestellt, so der Sächsische DSB. Dabei werde zumeist übersehen, dass vergleichbare Pflichten auch schon nach alter Rechtslage bestanden haben und der Umsetzungs- und Anpassungsaufwand daher letztendlich gar nicht so groß gewesen sein dürfte wie oftmals dargestellt wird.

Bei den dargestellten Beispielen handelt es sich u.a. bspw. um den Fall einer Handwerksfirma, die selbstverständlich auch Kundendaten verarbeitet. An diesem Beispiel wird der Frage nachgegangen, ob bereits das Ausmessen der Wohnung eines Kunden beispielsweise durch einen Maler oder einen Fußbodenleger nun „unter den Datenschutz fällt“, und der Handwerker protokollieren muss, wie er mit den Daten umgeht. Und dürfen Partei- oder Vereinsvorstände ihren Mitgliedern keine Geburtstagskarten mehr schreiben, weil das Geburtsdatum und die Adresse unter den Datenschutz fallen?

Quelle: Sächsischer Datenschutzbeauftragter

Kein Anspruch des Arbeitgebers auf Bekanntgabe der privaten Mobilfunknummer

Das Thüringer Landesarbeitsgericht (Az.: 6 Sa 442/17 und 6 Sa 444/17) hatte sich mit der Frage zu beschäftigen, ob ein Arbeitnehmer zur Absicherung eines Notfalldienstes außerhalb einer Rufbereitschaft dem Arbeitgeber seine private Mobilfunknummer herausgeben muss.

Das Thüringer Landesarbeitsgericht hat mit Urteil vom 16. Mai 2018 in den entschiedenen Fällen diese Frage verneint und deshalb die eingelegte Berufung des Arbeitgebers zurückgewiesen. Ein kommunaler Arbeitgeber hatte das System seiner Rufbereitschaft zur Einrichtung eines Notdienstes geändert. In diesem Zusammenhang hatte er von den Arbeitnehmern die Bekanntgabe ihrer privaten Mobilfunknummer verlangt, um sie außerhalb des Bereitschaftsdienstes im Notfall erreichen zu können.
Die Pflicht zur Herausgabe der privaten Mobilfunknummer stelle einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar, welcher durch ein berechtigtes Interesse des Arbeitgebers gerechtfertigt sein müsse. Der Abwägungsprozess der beidersei-tigen Interessen müsse ergeben, dass der Eingriff angemessen sei. Eine Pflicht zur Bekanntgabe der privaten Mobilfunknummer greife besonders tief in die persönliche Sphäre des Arbeitnehmers ein. Der Arbeitnehmer könne sich aufgrund der ständigen Erreichbarkeit dem Arbeitgeber ohne Rechtfertigungsdruck nicht mehr entziehen und so nicht zur Ruhe kommen. Auf die Wahrscheinlichkeit, tatsächlich kontaktiert und im Notfall herangezogen zu werden, komme es nicht an. Der Arbeitgeber habe durch die Änderung seines bestehenden Systems der Rufbereitschaft selbst die Problemlage herbeigeführt und ihm stünden andere Möglichkeiten zur Absicherung gegen Notfälle zur Verfügung.
Einer Zulassung der Revision bedürfe es nicht, da die grundlegende Rechtsfrage, dass der Eingriff in das Recht auf informationelle Selbstbestimmung durch ein entgegenstehendes, überwiegendes berechtigtes Interesse gerechtfertigt sein müsse, bereits geklärt sei.

Quelle: Thueringen.de

Verwertbarkeit von Dashcam-Aufnahmen

Der VI. Zivilsenat des Bundesgerichtshofs hat mit seinem Urteil vom 15. Mai 2018 – VI ZR 233/17 über die Verwertbarkeit von Dashcam-Aufnahmen als Beweismittel im Unfallhaftpflichtprozess entschieden.

Der Kläger nahm den Beklagten und seine Haftpflichtversicherung nach einem Verkehrsunfall auf restlichen Schadenersatz in Anspruch. Die Fahrzeuge der Parteien waren innerorts beim Linksabbiegen auf zwei nebeneinander verlaufenden Linksabbiegespuren seitlich kollidiert. Die Beteiligten stritten darüber, wer von beiden seine Spur verlassen und die Kollision herbeigeführt hat. Die Fahrt vor der Kollision und die Kollision wurden von einer Dashcam aufgezeichnet, die im Fahrzeug des Klägers angebracht war. Die Berufung des Klägers hatte das Landgericht zurückgewiesen. Die Aufzeichnung verstoße gegen datenschutzrechtliche Bestimmungen und unterliege einem Beweisverwertungsverbot.
Nach Auffassung der BGH-Richter sei die vorgelegte Videoaufzeichnung nach den geltenden datenschutzrechtlichen Bestimmungen unzulässig. Sie verstoße gegen § 4 BDSG, da sie ohne Einwilligung der Betroffenen erfolgt ist und nicht auf § 6b Abs. 1 BDSG oder § 28 Abs. 1 BDSG gestützt werden könne. Jedenfalls sei eine permanente anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke des Klägers zur Wahrnehmung seiner Beweissicherungsinteressen nicht erforderlich, denn es sei technisch möglich, eine kurze, anlassbezogene Aufzeichnung unmittelbar des Unfallgeschehens zu gestalten, beispielsweise durch ein dauerndes Überschreiben der Aufzeichnungen in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges.
Dennoch sei die vorgelegte Videoaufzeichnung als Beweismittel im Unfallhaftpflichtprozess verwertbar. Die Unzulässigkeit oder Rechtwidrigkeit einer Beweiserhebung führe im Zivilprozess nicht ohne Weiteres zu einem Beweisverwertungsverbot. Über die Frage der Verwertbarkeit sei vielmehr aufgrund einer Interessen- und Güterabwägung nach den im Einzelfall gegebenen Umständen zu entscheiden. Die Abwägung zwischen dem Interesse des Beweisführers an der Durchsetzung seiner zivilrechtlichen Ansprüche, seinem im Grundgesetz verankerten Anspruch auf rechtliches Gehör in Verbindung mit dem Interesse an einer funktionierenden Zivilrechtspflege einerseits und dem allgemeinen Persönlichkeitsrecht des Beweisgegners in seiner Ausprägung als Recht auf informationelle Selbstbestimmung und ggf. als Recht am eigenen Bild andererseits führe zu einem Überwiegen der Interessen des Klägers.

Quelle: BGH

Europäischer Datenschutzausschuss adaptiert Working Paper der Artikel-29-Datenschutzgruppe

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten („Artikel-29-Datenschutzgruppe“) wurde auf der Grundlage des Artikels 29 der Datenschutzrichtlinie (Richtlinie 95/46/EG) errichtet. Sie setzt sich aus Vertretern der nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und der Europäischen Kommission zusammen. Ihre Hauptaufgaben sind die Beratung der Europäischen Kommission in Datenschutzfragen und die Förderung einer einheitlichen Anwendung der Datenschutzrichtlinie in allen Mitgliedstaaten der Europäischen Union sowie in Norwegen, Liechtenstein und Island. Die Artikel-29-Datenschutzgruppe ist unabhängig; die Europäische Kommission stellt ihr ein Sekretariat sowie die Möglichkeit eines Internetangebots zur Verfügung.
Thematisch spezialisierte Untergruppen arbeiten Empfehlungen und Stellungnahmen aus. Diese sind ein wichtiger Beitrag zur einheitlichen Anwendung der europäischen Datenschutzbestimmungen. Mit der Geltung der Datenschutz-Grundverordnung seit dem 25. Mai 2018 wurde die Artikel-29-Datenschutzgruppe durch einen Europäischen Datenschutzausschuss (EDSA) mit erweiterter Verantwortung abgelöst.
Der EDSA ist eine Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit. Er nimmt seine Aufgaben und Befugnisse unabhängig wahr und unterliegt keinen Weisungen. Die Kernaufgabe des Ausschusses ist es, die einheitliche Anwendung der DS-GVO innerhalb der EU sicherzustellen. Im Rahmen dieses Harmonisierungsauftrags weist die Verordnung dem Ausschuss ein umfangreiches Aufgabenspektrum zu. Hierzu gehört die beratende Funktion im Hinblick auf datenschutzpolitische und datenschutzrechtliche Fragestellungen auf EU-Ebene, insbesondere zu Legislativvorschlägen der Europäischen Kommission. Ferner kann der Ausschuss aus eigener Initiative oder auf Ersuchen der Kommission Leitlinien, Empfehlungen und bewährte Verfahren zu datenschutzspezifischen Fragestellungen erarbeiten. Der EDSA verfügt, wie schon die Artikel 29-Gruppe, über Unterarbeitsgruppen, die themenbezogen die Stellungnahmen und Entscheidungen des Ausschusses vorbereiten.

Da die Artikel-29-Datenschutzgruppe schon vor der Geltung der DS-GVO zahlreiche Working-Paper, die als Anwendungshilfe und Anwendungshinweise verstanden werden konnten, veröffentlicht hatte, stand die Frage im Raum, ob und welche dieser bereits entwickelten Arbeitshilfen von dem EDSA adaptiert werden würden. Der EDSA hat nun in seiner ersten konstituierenden Sitzung am 25. Mai 2018 zahlreiche Positionen der der Artikel-29-Datenschutzgruppe bestätigt. Eine Liste der bisher bestätigten Positionen lässt sich hier abrufen:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf
Ggf. werden im Rahmen der anstehenden nächsten Sitzungen weitere Arbeitspapiere der Artikel-29-Datenschutzgrupe adaptiert werden. Die adaptierten Arbeitspapiere sind weiterhin als Empfehlung für die Praxis zu verstehen. Eine verbindliche Wirkung für Gerichte geht von diesen nicht aus. Es kann jedoch angenommen werden, dass auch Gerichte bei Entscheidungen mit DS-GVO-Bezug sich an den Vorgaben der EDSA orientieren werden.

Quelle: European Data Protection Board

Verpflichtung auf die Vertraulichkeit

Das bisherige Datenschutzrecht sah in § 5 BDSG a.F. eine sog. „Verpflichtung auf das Datengeheimnis" vor. Eine vergleichbar klare und eindeutige Regelung ist in der DS-GVO nicht mehr enthalten. Insoweit stellt sich datenverarbeitenden Unternehmen die Frage, ob die klassische Verpflichtung auf das Datengeheimnis weiterhin eine Zukunft hat und als „Verpflichtung auf die Vertraulichkeit" fortlebt.

Die GDD hatte sich bereits in ihrer Praxishilfe DS-GVO XI – Verpflichtung auf die Vertraulichkeit, dahingehend positioniert, dass eine Verpflichtung auf die Vertraulichkeit auch unter dem Regime der DS-GVO ein probates Mittel sein wird, um unmissverständlich auf die Bedeutung und den Umfang datenschutzrechtlicher Regeln hinzuweisen und Mitarbeitern etwaige Risiken von Gesetzesverstößen vor Augen zu führen. Auch das BayLDA vertritt die Ansicht, dass eine Belehrung und Verpflichtung der beschäftigten Personen zur Beachtung der datenschutzrechtlichen Anforderungen auch unter Geltung der DS-GVO als organisatorische Maßnahme geboten bleibt, um die Einhaltung des Datenschutzes so weit wie möglich sicherzustellen. Aufgrund der vielen Nachfragen nach einer Hilfestellung habe man nun einen Mustertext mit Erläuterungen für eine solche Belehrung und Verpflichtung von Beschäftigten veröffentlicht, so das BayLDA.

Interessierte finden das entsprechende Dokument auf der BayLDA-Homepage bei den Informationsblättern in der Infothek (www.lda.bayern.de/de/infoblaetter.html).

Das Kurzpapier Nr. 19 der Datenschutz-Konferenz (DSK) „Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO" geht ebenfalls auf diese Thematik ein. Selbst wenn nach dem Wortlaut der DS-GVO nur die Beschäftigten eines Auftragsverarbeiters zu „verpflichten" sind, trifft inhaltlich diese „verpflichtende Unterrichtung" auch die Verantwortlichen und ihre Beschäftigten. Wie Verantwortliche diese gesetzliche Verpflichtung umsetzen (und ggfls. der Aufsichtsbehörde nachweisen), ist nicht verbindlich geregelt. Es wird empfohlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen. Ein Muster für eine solche Verpflichtung enthält das Kurzpapier ebenfalls als Anlage.

GDD vergibt Wissenschaftspreis im Datenschutz und in der Datensicherheit

Auch in diesem Jahr vergibt die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. erneut einen Wissenschaftspreis für herausragende wissenschaftliche Arbeiten in den Bereichen Datenschutz und Datensicherheit. Der Preis beträgt 5.000,00 €. Der Preis kann auch zwischen mehreren Arbeiten geteilt werden. Er soll bevorzugt an Nachwuchswissenschaftler vergeben werden. Ausgezeichnet werden fertiggestellte oder in der Fertigstellung befindliche Abschlussarbeiten oder Doktorarbeiten. In Betracht kommen neben Arbeiten aus den Rechtswissenschaften, Wirtschaftswissenschaften und der Informatik auch aus andere Wissenschaftsdisziplinen, in denen Fragen aus den Bereichen Datenschutz und Datensicherheit behandelt werden. Voraussetzung für die Vergabe des Wissenschaftspreises ist die Erfüllung der wissenschaftlichen Exzellenzkriterien.

Die Arbeiten müssen mit Befürwortung des betreuenden Hochschullehrers bis zum 31. Juli 2018 bei der GDD-Geschäftsstelle eingereicht werden.

Nähere Informationen zum Wissenschaftspreis stehen als PDF-Datei und Word-Dokument als Download zur Verfügung.