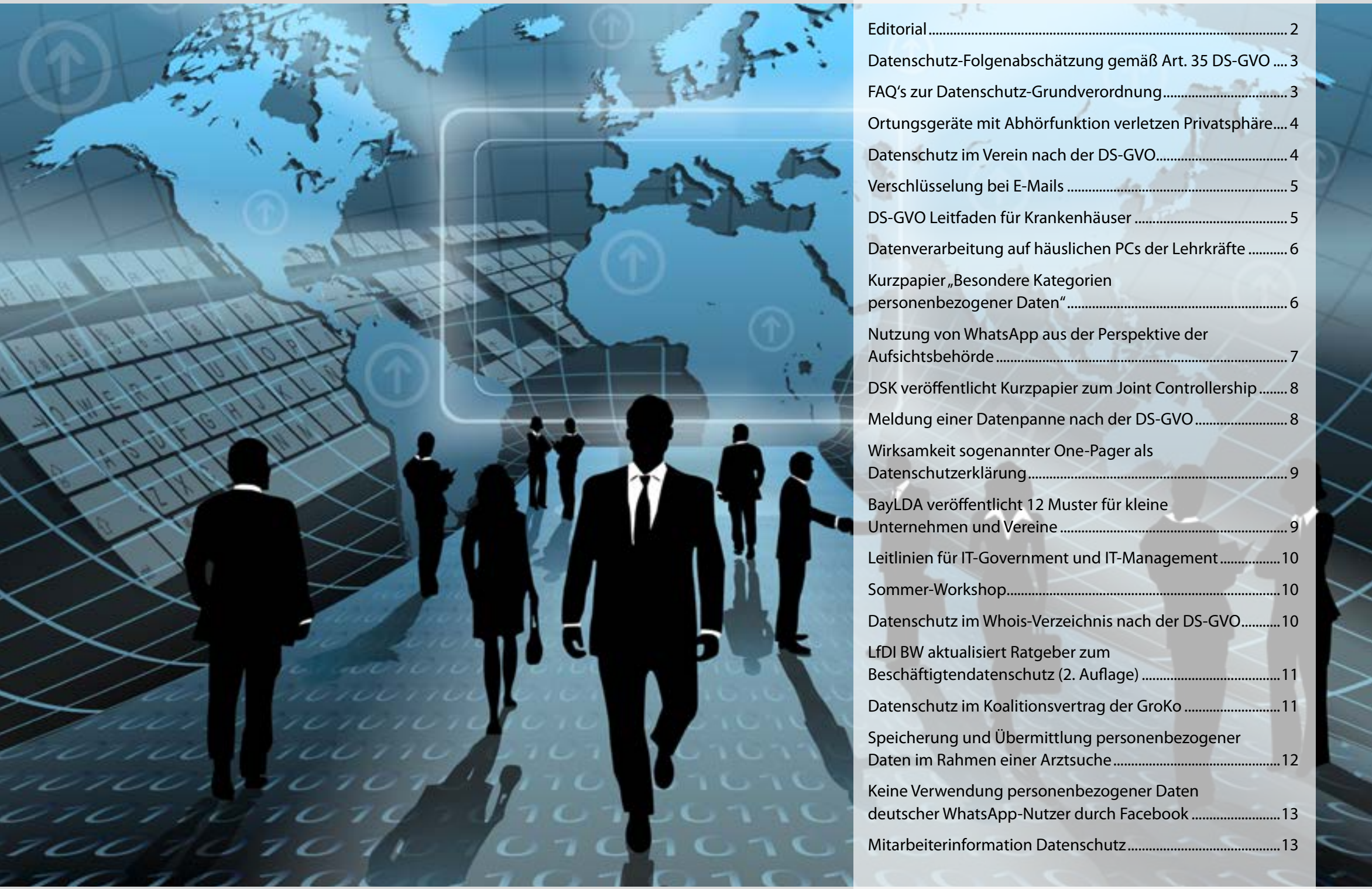
Datenschutz newsbox

Ausgabe 4 2018



DATAKONTEXT

Editorial

Im Rahmen einer Kleinen Anfrage der Fraktion Bündnis 90/Die Grünen wurde bereits im Jahre 2016 das Thema „Datenschutz im Kinderzimmer“ thematisiert. Mehr als jedes dritte Kind habe ein „Lieblingsspielzeug“, das aus dem Mobil-, Computer- oder Konsolenbereich komme, und neuartiges, vernetztes Spielzeug erobere den Markt.

Die Bundesnetzagentur richtete sich 2017 mit einem ungewöhnlichen Aufruf an die Besitzer der Puppe „My friend Cayla“. Technisch betrachtet, stelle diese eine verbotene Sendeanlage dar. Dadurch sei eine unbemerkte Fernüberwachung möglich. Ähnliche Sorgen löste die WLAN-Puppe „Hello Barbie“ im Jahre 2015 bei Eltern und Datenschützern aus. Und auch aktuell erhitzt eine Smartwatch für Kinder die Datenschutz-Gemüter. Sie wurde entwickelt, damit Eltern ihre Kinder via GPS überwachen und orten können. Obwohl in der Produktbeschreibung explizit darauf hingewiesen wird, dass die Uhr über keine Abhörfunktion verfügt, könne diese problemlos in eine Wanze verwandelt werden.

Auf die Frage, warum insbesondere viele Geräte für das Internet der Dinge teilweise erhebliche Sicherheitsmängel aufweisen, geht die LDI NRW (23. TB 2017, Ziffer 13.3) ein.
„IT-Sicherheit wird von Herstellern primär als Kostenfaktor wahrgenommen. Zudem stellen sie häufig nach kurzer Zeit keine Updates mehr für die Geräte zur Verfügung. Bekannte Sicherheitslücken werden damit nicht mehr behoben. Für Hersteller hat die Vernachlässigung der IT-Sicherheit in der Regel keine negativen Konsequenzen. Eine ausschließliche Nutzung der Daten auf den Geräten ist jedoch oftmals bereits aufgrund des technischen Designs der Hersteller ausgeschlossen. Regelmäßig ist die Einbindung eines Gerätes in die Cloud obligatorisch, lokale Schnittstellen fehlen. Teilweise sind vom Hersteller beworbene Funktionalitäten nur über einen Cloud-Dienst nutzbar, ohne dass eine technische Notwendigkeit ersichtlich ist.“

Fraglich ist, ob diese „Nachlässigkeiten“ mit Anwendbarkeit der DS-GVO ausgemerzt werden. Die Ausführungen der LDI NRW lassen sich dahingehend verstehen:
„Die DS-GVO verpflichtet Hersteller dazu, angemessene Maßnahmen zu treffen, um die Einhaltung der Datenschutzgrundsätze sicherzustellen. Zum einen gehört hierzu, bei der Produktentwicklung auch die IT-Sicherheit zu berücksichtigen und notfalls zeitnah Updates bereitzustellen, um Vorfälle wie die oben beschriebenen zu vermeiden. Zum anderen gehört hierzu aber auch, Daten wo immer möglich, nur in anonymisierter oder pseudonymisierter Form zu verarbeiten. Die Daten sind zu löschen, sobald sie für den Zweck, zu dem sie erhoben wurden, nicht mehr benötigt werden. Dies wird als ‚Datenschutz durch Technikgestaltung‘ bezeichnet.“

Des Weiteren fordert die DS-GVO „datenschutzfreundliche Voreinstellungen“. Im Auslieferungszustand ist die Verarbeitung personenbezogener Daten daher auf das erforderliche Minimum zu beschränken.

Wenn mit Anwendbarkeit der DS-GVO Datenschutz durch Technikgestaltung und der Grundsatz der datenschutzfreundlichen Voreinstellungen von den Herstellern vernetzter Spielzeuge ausreichend berücksichtigt werden, könnte dies dazu führen, dass wir im Idealfall auch in den Kindezimmern mehr Datenschutz vorfinden können, hofft

Ihr Levent Ferik

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

Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

Eine verbandsübergreifende Arbeitsgruppe, bestehend aus Vertretern des Bundesverbandes Gesundheits-IT e.V. (bvitg), der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS, Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“) sowie der Deutsche Krankenhausgesellschaft e.V., hat eine gemeinsame Veröffentlichung zur Datenschutz-Folgenabschätzung vorgestellt.

Als Zielgruppe nennen die Autoren Verarbeiter von personenbezogenen Daten im Gesundheitswesen. Insbesondere versorgende Einrichtungen/Institutionen und medizinische Forscher sollen in dieser Ausarbeitung eine Unterstützung beim Umgang mit der DSFA finden.

Eine Datenschutz-Folgenabschätzung (abgekürzt DSFA) soll in den Fällen, in denen eine Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, helfen, die Risiken zu minimieren und durch Darstellung der Maßnahmen zur Reduzierung der Risiken auch für Dritte nachvollziehbar aufzeigen, wie Verantwortliche für die Datenverarbeitung mit diesen Risiken umgehen.

Dabei beschreibt Art. 35 DS-GVO verschiedene Fälle, in denen eine DSFA erfolgen muss. Unabhängig davon steht es jedem Verantwortlichen selbstverständlich frei, auch in anderen Fällen eine DSFA durchzuführen, beispielsweise zur Darstellung der Einhaltung der Vorgaben der DS-GVO hinsichtlich der Sicherheit der Verarbeitung. Art. 35 DS-GVO definiert die Mindestanforderungen an die Inhalte einer DSFA.

Demzufolge sind diese Mindestinhalte:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge;
b) eine systematische Beschreibung der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
c) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
d) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DS-GVO;
e) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Anforderungen der DS-GVO eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen wird.

In dieser Praxishilfe wird auf Hinweise der Artikel-29-Datenschutzgruppe ebenso wie auf international bestehende Erfahrungen zur DSFA zurückgegriffen und dargestellt, wie mit dieser Thematik umgegangen werden kann.

Quelle: Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.

FAQ’s zur Datenschutz-Grundverordnung

Ein zentraler Baustein der Datenpolitik ist das Datenschutzrecht. Egal, ob es um Datenverarbeitung durch staatliche Stellen oder durch Unternehmen geht – der Umgang mit personenbezogenen Daten betrifft jeden. Aufgabe des Datenschutzrechts ist es, einen zeitgemäßen Ordnungsrahmen für die Verarbeitung personenbezogener Daten zu schaffen. Hierbei müssen das Interesse von Staat und Wirtschaft an der Verarbeitung personenbezogener Daten und die Auswirkungen auf die betroffenen Personen angemessenen ausgeglichen werden. Das Bundesministerium des Innern ist das, für das allgemeine Datenschutzrecht auf Bundesebene, zuständige Ressort. Es ist insbesondere für das Bundesdatenschutzgesetz zuständig. Zudem wirkt das Bundesministerium des Innern federführend für die Bundesrepublik an den aktuellen Entwicklungen des allgemeinen Datenschutzrechts auf europäischer und internationaler Ebene mit.

Das BMI hat im Rahmen dieser Zuständigkeit zu den häufigsten Fragen rund um die DS-GVO eine Info-Seite aufgebaut. Die Beiträge geben Antworten auf die wichtigsten Fragen zu den Neuerungen der Datenschutz-Grundverordnung. Sie sollen den Einstieg in die Rechtsmaterie erleichtern, erheben jedoch keinen Anspruch auf Vollständigkeit und ersetzen keine einzelfallbezogene Beratung durch die Aufsichtsbehörden oder andere spezialisierte Einrichtungen.

Quelle: Bundesministerium des Innern

Ortungsgeräte mit Abhörfunktion verletzen Privatsphäre

Die Bundesnetzagentur geht gegen den Verkauf von GPS-/GSM-Trackern vor. Hierbei handelt es sich um Ortungsgeräte, die per GPS oder GSM die eigenen Positionsdaten ermitteln. Diese würden immer häufiger zum Orten von Personen eingesetzt, oft auch von Kindern. Wenn diese zugleich über ein Mikrofon verfügten und mit ihnen Gespräche unbemerkt mitgehört werden könnten, handele es sich um eine verbotene Sendeanlage, so Jochen Homann, Präsident der Bundesnetzagentur. In diesem Fall würden die Geräte aus dem Verkehr gezogen, um die Privatsphäre der Träger und der Umgebung der Ortungsgeräte zu schützen.
Die Anwendungsbereiche der Ortungsgeräte reichen von der privaten Nutzung zur Standortbestimmung von gestohlenen Fahrzeugen oder entlaufenen Haustieren bis hin zur geschäftlichen Nutzung durch Einbau in Firmenfahrzeuge oder LKW-Flotten. Auch in Schulranzen für Kinder sollen GPS-/GSM-Tracker Einzug halten. Zusätzlich zu dieser Ortungsfunktion verfügen manche GPS-/GSM-Tracker über eine Abhörfunktion. Diese Funktion kann der Besitzer per App oder SMS-Befehl aus der Ferne aktivieren und anschließend Gespräche unbemerkt abhören. Diese Abhörfunktion kann grundsätzlich jeder aktivieren, der Kenntnis von der Telefonnummer der SIM-Karte des GPS-/GSM-Trackers hat. Eine derartige Abhörfunktion ist in Deutschland verboten. Gegen eine vergleichbare Abhörfunktion ging die Bundesnetzagentur kürzlich im Zusammenhang mit Kinderuhren vor.
Käufern wird geraten, zunächst zu prüfen, ob ihr GPS-/GSM-Tracker über eine Abhörfunktion verfügt. Dies kann man daran erkennen, dass in der Produktbeschreibung bzw. der Bedienungsanleitung des Geräts etwa beschrieben wird, dass dieser über eine „Monitorfunktion" oder „Mithörfunktion" verfügt. Häufig wird beschrieben, dass der GPS-/GSM-Tracker zur Gesprächsüberwachung genutzt werden kann. Sofern Käufer von GPS-/GSM-Trackern mit Abhörfunktion der Bundesnetzagentur bekannt werden, fordert sie diese auf, das Gerät zu vernichten und einen Nachweis hierüber an die Bundesnetzagentur zu senden.
Besitzern dieser Geräte wird empfohlen, die Tracker unschädlich zu machen und Vernichtungsnachweise hierzu aufzubewahren. Wie ein Vernichtungsnachweis im Falle eines Anschreibens durch die Bundesnetzagentur geführt werden kann, finden Sie unter www.bundesnetzagentur.de/spionagekameras. Bei Rückfragen zu diesem Thema können sich Verbraucher und Unternehmen vorzugsweise auf elektronischem Weg an die Bundesnetzagentur wenden per Mail an: spionagegeraete@bnetza.de.

Quelle: Bundesnetzagentur

Datenschutz im Verein nach der DS-GVO

Wenn die Datenschutz-Grundverordnung (DS-GVO) in Deutschland und in allen anderen Mitgliedstaaten der Europäischen Union ab dem 25. Mai 2018 geltendes Recht wird, entfaltet sie ihre Wirkung nicht nur für gewerbliche Unternehmen, sondern auch für alle Vereine. Auch diese haben die Verpflichtung staatliche Regeln zu befolgen, auch jene zum Schutz der persönlichen Daten von Mitgliedern, Mitarbeitern und Vereinspartnern. Auch Vereinsvorstände befassen sich daher seit geraumer Zeit mit den Fragen des Datenschutzes rund um die DS-GVO.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Stefan Brink, hat dies zum Anlass genommen, eine Orientierungshilfe zu dieser Thematik vorzustellen. Der Landesbeauftragte hierzu: „Für Vereine ist jetzt die Zeit gekommen, die neuen Datenschutz-Anforderungen in Angriff zu nehmen, damit der Übergang auf das neue Datenschutzrecht glatt über die Bühne gehen kann. Mit unserer Orientierungshilfe möchten wir den Vereinen zur Seite stehen und sie bei dieser Aufgabe unterstützen."

Die jetzt vorgelegte Orientierungshilfe richtet sich in erster Linie an Vereinsvorstände, Datenschutzbeauftragte und Datenschutzberater – und stellt klar, nach welchen Maßstäben der LfDI ab dem 25. Mai 2018 im Bereich der Vereine vorgehen wird. In der vorgelegten Orientierungshilfe werden auf knapp über 30 Seiten alle relevanten Themen wie Rechtsgrundlagen, Veröffentlichungen im Internet, Einwilligungen sowie Datenübermittlungen angesprochen.

Die Orientierungshilfe kann auf der Internetseite des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (www.badenwuerttemberg.datenschutz.de) unter der Rubrik „Service/Orientierungshilfen" abgerufen werden.

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Verschlüsselung bei E-Mails

Frage (1) des GDD Erfa-Kreises Coburg:

Ein Unternehmen betreibt eine Website. Dort stellt es sich und sein Leistungsangebot allgemein vor. Ein Karriereportal oder Bewerbungstool gibt es nicht, es wird auch nicht zur Zusendung von (Initiativ-) Bewerbungen aufgefordert. Das Unternehmen bietet lediglich

- Eine allgemeine Kontakt-E-Mail-Adresse kontakt@unternehmen.de an und
- ein Kontaktformular, mittels dessen eine E-Mail an das Unternehmen generiert wird.

a) Muss das Unternehmen jeweils für eine verschlüsselte Übertragung sorgen, weil damit zu rechnen ist, dass Initiativbewerbungen auf die Adresse/ über die Maske erfolgen?

Antwort BayLDA:

Ja. Der Grund ist einerseits, da die E-Mail kontakt@ klar kommuniziert, dass damit die übliche Unternehmenskommunikation stattfindet – dazu gehören auch Bewerbungen.

Ein Kontaktformular, das mittels eines HTTP-Requests die Daten an einen Webserver überträgt (der daraus eine E-Mail generiert), muss grundsätzlich HTTPS-verschlüsselt werden. Unter der DS-GVO wird dieser Mangel im Allgemeinen mit einem Bußgeld sanktioniert werden. Bei Bewerbungen muss zusätzlich zur verschlüsselten Übertragung (HTTPS bei Webseiten, STARTTLS bei E-Mail-Server) eine Option zu einer Inhaltsverschlüsselung angeboten werden (oder ein vergleichbares Sicherheitsniveau, z.B. mittels eines Bewerbungsportals erreicht werden).

Frage (2) des GDD Erfa-Kreises Coburg:

b) Sofern Frage 1 a) mit Ja zu beantworten wäre:
Könnte das Unternehmen auf eine Verschlüsselung verzichten, wenn es dazu auffordern würde, von Bewerbungen über das Internet abzusehen und solche nur auf dem Postweg zu schicken?

c) Zusatzfrage: Wäre dann der Hinweis tauglich: „Wir bitten Sie, davon Abstand zu nehmen, uns Bewerbungsunterlagen über das Internet zukommen zu lassen. Bitte haben Sie Verständnis dafür, dass wir ausschließlich Bewerbungen zur Kenntnis nehmen, die uns auf dem Postweg erreichen“?

Antwort BayLDA:

Ja.
Anmerkung: Die Implementierung einer Transportverschlüsselung ist heutzutage sehr einfach und kostengünstig/kostenlos möglich. Auch eine Inhaltsverschlüsselung mittels PGP ist kostenlos in wenigen Minuten aufgesetzt. Deswegen stellt sich die Frage, ob es für das Unternehmen sinnvoll ist, sich den gängigen digitalen Kommunikationsmitteln zu verschließen.

DS-GVO Leitfaden für Krankenhäuser

Ab dem 25. Mai 2018 führt die europäische Datenschutz-Grundverordnung auch im Krankenhausbereich zu zahlreichen Neuerungen. Um hier die Umstellung zu erleichtern, haben die beiden bayerischen Datenschutzaufsichtsbehörden gemeinsam einen Leitfaden zu den „Anforderungen an das Datenschutzmanagement in bayerischen öffentlichen und privaten Krankenhäusern“ erstellt.

Die Datenschutz-Grundverordnung bringt ab Mai 2018 zahlreiche Änderungen mit sich, die in der Praxis schon heute oftmals für Verunsicherung sorgen. Branchenspezifische Hilfestellungen – gerade im Krankenhausbereich – sind derzeit allerdings noch rar. Hier wollen die beiden bayerischen Datenschutzaufsichtsbehörden anknüpfen. Um bestehende Unsicherheiten abzubauen und erste Hinweise zur Auslegung der neuen Regelungen zu geben, haben der Bayerische Landesbeauftragte für den Datenschutz und das Bayerische Landesamt für Datenschutzaufsicht einen gemeinsamen Leitfaden zur Umsetzung der Datenschutz-Grundverordnung für alle bayerischen öffentlichen und privaten Krankenhäuser erarbeitet. Sie folgen hiermit der bewährten Zusammenarbeit im Krankenhausbereich. Schon im Sommer 2016 wurde gemeinsam ein Leitfaden zum Einsatz externer Dienstleister durch bayerische Krankenhäuser veröffentlicht.

Der Leitfaden steht auf www.datenschutz-bayern.de unter„ Datenschutzreform 2018“ bzw. unter http://www.lda.bayern.de/media/leitfaden_krankenhaus.pdf zum Abruf bereit.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Datenverarbeitung auf häuslichen PCs der Lehrkräfte

Aufgabe des Datenschutzes in der öffentlichen Verwaltung ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten durch öffentliche Stellen in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht). Datenschutz hat Verfassungsrang. Artikel 4 Abs. 2 der Landesverfassung konstituiert aber nicht nur den Anspruch des Einzelnen auf Schutz seiner personenbezogenen Daten, sondern bestimmt auch, dass Eingriffe in das Recht auf informationelle Selbstbestimmung nur im überwiegenden Interesse der Allgemeinheit auf Grund eines Gesetzes zulässig sind.

Das Datenschutzgesetz NRW enthält die allgemeinen Vorgaben für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen in Nordrhein-Westfalen. Lehrern ist die Nutzung privater Computer und Smartphones unter Einhaltung gewisser Voraussetzungen erlaubt. Ein wesentlicher Grundsatz ist dabei, dass sich die Verarbeitung auf den erforderlichen Umfang beschränken muss und dass Daten grundsätzlich nur für die Zwecke verarbeitet werden dürfen, für die sie erhoben wurden. Wesentlich ist auch das Recht der oder des Betroffenen auf Auskunft, Berichtigung, Sperrung und Löschung.

Die Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I) bestimmt auch die Voraussetzungen für die Verarbeitung von Schülerdaten durch die Lehrkräfte auf ihrem privaten häuslichen PC (§ 2 Abs. 2 VO DV I). Private PCs können von den Lehrerinnen und Lehrern für die Erledigung ihrer dienstlichen Aufgaben eingesetzt werden, wenn die Schulleitung die Verarbeitung von Schüler- und Elterndaten schriftlich genehmigt. Mit der Dienstanweisung ADV ist ein Genehmigungsvordruck, der alle rechtlichen und technischen Bedingungen enthält, verbindlich vorgegeben. Voraussetzung für die Genehmigung ist unter anderem, dass ein hinreichender technischer Zugriffsschutz auf die gespeicherten Daten besteht (z.B. Passwortschutz, abschließbares Arbeitszimmer). Nur die jeweilige Lehrerin oder der jeweilige Lehrer darf auf die Daten zugreifen können. Welche Daten verarbeitet werden dürfen, ist in Anlage 3 der VO-DV I im Einzelnen festgelegt.

Zum Ausfüllen des Genehmigungsvordrucks hat die Medienberatung eine Handreichung zur Verfügung gestellt.

Quelle: Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen

Kurzpapier „Besondere Kategorien personenbezogener Daten“

Die Datenschutzkonferenz(DSK) hat das Kurzpapier Nr. 17 veröffentlicht, welches sich dem Thema „Besondere Kategorien personenbezogener Daten“ widmet.

Wie bisher werden auch künftig besondere Kategorien personenbezogener Daten bestimmt, die eines speziellen Schutzes bedürfen. Zu den bislang im Bundesdatenschutzgesetz genannten Kategorien – Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit (vgl. Art. 4 Nr. 15 DS-GVO, ErwGr. 35) oder Sexualleben – treten in Art. 9 DS-GVO nun auch genetische Angaben sowie biometrische Daten (Art. 4 Nr. 13 DS-GVO, ErwGr. 34; Art. 4 Nr. 14 DS-GVO, ErwGr. 51) zur eindeutigen Identifizierung einer Person. Wurden bisher auch philosophische Überzeugungen als besonders schutzbedürftig klassifiziert, fällt diese Kategorie jetzt unter den Begriff der „weltanschaulichen“ Überzeugungen, ohne dass damit inhaltliche Änderungen verbunden wären.

Von den in Art. 9 Abs. 2 lit. b, g, h, i und j DS-GVO benannten Öffnungsklauseln hat der Bundesgesetzgeber in den §§ 22 Abs. 1, 27 und 28 BDSG-neu in Verbindung mit den jeweiligen konkreten spezialgesetzlichen Regelungen Gebrauch gemacht. § 22 Abs. 2 BDSG-neu enthält darüber hinaus beispielhaft aufgezählte Maßnahmen zur Wahrung der Interessen der betroffenen Personen, die jeden Verantwortlichen und damit jeden, der besondere Kategorien personenbezogener Daten verarbeitet, treffen. Ob und wenn ja, wie weit die Regelungen des BDSG-neu zur Einschränkung der Betroffenenrechte wegen des bestehenden Anwendungsvorrangs der DS-GVO angewendet werden können, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Nutzung von WhatsApp aus der Perspektive der Aufsichtsbehörde

Frage (1) des GDD Erfa-Kreises Würzburg:

Die Nutzung von WhatsApp für die unternehmensinterne Kommunikation ist, nach Ansicht der Aufsichtsbehörden, unzulässig. Da aber, nach aktuellen Zahlen, WhatsApp von ca. 50 % der deutschen Bevölkerung genutzt wird (ca. 37 Mio. aktive Nutzer), wird WhatsApp zu einem unverzichtbaren Kommunikationsmittel beim Kontakt mit Kunden, insbesondere im Mediensektor.

Als Paradebeispiel sei der Bayrische Rundfunk genannt, der WhatsApp als offizielles Kommunikationsmittel anbietet und die Nachrichten und Tonaufzeichnungen der Nutzer sogar im Programm abspielt, bzw. vorliest. Weiterhin bekommt man sogar regionale Nachrichten per WhatsApp auf das eigene Smartphone geschickt, wenn man sich anmeldet. Wie steht die Aufsichtsbehörde zu diesem Nutzungsszenario?

Antwort BayLDA:

Wegen der Sicherheits- und Datenschutzrisiken bei der WhatsApp-Kommunikation, siehe Frage (2) unten, und der für eine unternehmensinterne Kommunikation zur Verfügung stehenden anderweitigen Produkte, halten wir insoweit den Einsatz von WhatsApp nicht für datenschutzkonform (Nr. 22.1 unseres Tätigkeitsberichts 2015/2016, https://www.lda.bayern.de/media/baylda_report_07.pdf.

Der Bayerische Rundfunk unterliegt nicht unserer Aufsicht, so dass wir dort nicht tätig werden können. Siehe dazu allgemein auch unter https://www.baden-wuerttemberg.datenschutz.de/duerfen-lehrer-whatsapp-benutzen/ oder „Dürfen Lehrkräfte Facebook und Messengerdienste, wie z. B. WhatsApp für die dienstliche Kommunikation mit ihren Schülerinnen und Schülern und den Eltern benutzen?“, https://www.datenschutzzentrum.de/artikel/1052-.html

Frage (2) des GDD Erfa-Kreises Würzburg:

Eine weitere Frage ergibt sich bei der Nutzung von WhatsApp für die allgemeine Kundenkommunikation:
Insbesondere Unternehmen, die hauptsächlich mit Endverbrauchern zu tun haben, haben mehr und mehr die Anforderungen auch per WhatsApp mit ihren Kunden kommunizieren zu können. Dies gilt insbesondere für die Bereiche Vertrieb, Marketing und Support. Auch im Bereich der B-to-B Kommunikation wird WhatsApp immer wichtiger. In vielen Ländern ist dies oft sogar das einzige echte Kommunikationsmittel geworden. Dies gilt insbesondere für den Vertrieb und Support-Anfragen. Wie steht die Aufsichtsbehörde zu diesen beiden Nutzungsszenarien?

Antwort BayLDA:

WhatsApp hat nach eigenen Angaben zwar inzwischen eine Ende-zu-Ende-Verschlüsselung für die Kommunikationsinhalte eingeführt, problematisch bleiben aber weiterhin u. a. die Verarbeitung von Metadaten zu den Nachrichten in den USA sowie die von dort erfolgende Erhebung der Kontaktdaten aus dem Adressbuch, einschließlich dem zwischenzeitlichen „Zusammenwirken“ von WhatsApp und Facebook.

Wir beurteilen es im Moment so, dass einerseits das Angebot zur WhatsApp-Kommunikation durch ein Unternehmen an Kunden grundsätzlich dann nicht beanstandet wird, wenn vom Unternehmen auf die Datenschutzbedenken hingewiesen und den Kunden gleichzeitig parallel ein anderer sicherer Kommunikationsweg angeboten wird; der Kunde kann sich dann frei für oder gegen eine WhatsApp-Kommunikation entscheiden.
Andererseits bewerten wir eine WhatsApp-Kommunikation innerhalb eines Unternehmens unter den Beschäftigten wegen der grundsätzlichen Datenschutz-Bedenken als zu vermeidendes Sicherheitsrisiko. Auch, weil hier unschwer sichere elektronische Kommunikationswege eingerichtet und genutzt werden können.“

DSK veröffentlicht Kurzpapier zum Joint Controllership

Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es nach Art. 26 DS-GVO einer klaren Zuteilung der Verantwortlichkeiten. Dies betrifft auch Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines Verantwortlichen durchgeführt wird.
Die Datenschutzkonferenz (DSK) führt die Reihe ihrer sog. Kurzpapiere fort und hat nun das „Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO" veröffentlicht. Dieses Rechtsinstitut war zwar bereits in der EG-Datenschutzrichtlinie (RL 95/46/EG) angelegt, dort allerdings nicht detailliert ausgestaltet, und spielte in Deutschland bisher – wenn überhaupt – nur eine äußerst geringe Rolle, da es im BDSG-alt nicht ausdrücklich erwähnt war. Die DSK geht davon aus, dass die ausdrückliche Regelung der gemeinsamen Verantwortlichkeit in der DS-GVO gerade für die Praxis in Deutschland erhebliche Auswirkungen haben wird.
Weiter geht die DSK davon aus, dass eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 DS-GVO angesichts der Komplexität moderner Datenverarbeitungs-vorgänge bei sehr unterschiedlichen Fallgestaltungen in Betracht kommen kann. Es sei nicht möglich, hierzu eine abschließende Liste zu erstellen, vielmehr bedürfe es einer gewissen Flexibilität, um einen effektiven Schutz der Rechte und Freiheiten der betroffenen Personen zu gewährleisten. Das Kurzpapier enthält jedoch einige exemplarisch genannte Fälle, die aufzeigen sollen, in welchen Fällen ggf. eine gemeinsame Verantwortlichkeit in Betracht kommen kann.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Meldung einer Datenpanne nach der DS-GVO

Frage des GDD Erfa-Kreises Bayreuth:
Nach Art. 33 Abs. 1 DS-GVO ist der Verantwortliche zur Meldung einer Datenpanne an die Aufsicht binnen 72 Stunden nach Kenntnis verpflichtet. Der Auftragsverarbeiter selbst ist nach Art. 33 Abs. 2 DS-GVO zur unverzüglichen Meldung an den Verantwortlichen verpflichtet, wenn er Anhaltspunkte für eine Datenpanne hat.
Nach dem Wesen der Auftragsverarbeitung bilden Auftragsverarbeiter und Auftraggeber eine Handlungs-/Haftungseinheit. Wird die Aufsicht vor diesem Hintergrund eine Anrechnung schon beim Auftragsverarbeiter bis zur Eigenmeldung an den Verantwortlichen abgelaufener Meldefristanteile beim Auftraggeber vornehmen/anstreben? Würde also die (verbleibende) Meldefrist für den Auftraggeber auf 60 Stunden verkürzt, wenn der Auftragsverarbeiter selbst 12 Stunden ins Land gehen lässt, bis er den Auftraggeber über eine Datenpanne bei ihm informiert?
Wenn dies entsprechend dem Gesetzeswortlaut nicht der Fall ist: Ist „unverzüglich" hinsichtlich des Auftragsverarbeiters so zu verstehen, dass er selbst auch 72 Stunden zur Meldung von Datenschutzverletzungen an den Auftraggeber hat oder gilt hier ein abweichender Maßstab bzw. welche Zeitspanne würde hier aufsichtlich toleriert?

Antwort BayLDA:
Die 72 Stunden beginnen ab Kenntniserlangung durch den Verantwortlichen, d.h. ab dem Zeitpunkt, an dem der Auftragsverarbeiter den Verantwortlichen informiert hat. Die Zeitspanne, in der der Auftragsverarbeiter den Verantwortlichen informiert, muss so kurz wie möglich – auch weniger als 72 Stunden sein. Wie weit „unverzüglich" ausgelegt wird, wird sich im Rahmen der Harmonisierung des europäischen Vollzugs zeigen.

Wirksamkeit sogenannter One-Pager als Datenschutzerklärung

Bereits im Rahmen des Nationalen IT-Gipfels 2015 hatte die vom Bundesministerium der Justiz und für Verbraucherschutz und IBM geleitete Plattform „Verbraucherschutz in der digitalen Welt" ein Muster für Datenschutzhinweise„ auf einer Seite" vorgestellt – den „One-Pager". Der „One-Pager" ist eine einfache, konzentrierte Information über die wesentlichen Datenverarbeitungen. Ziel ist es, damit zusätzlich zur förmlichen Datenschutzerklärung, auf einer Seite Informationen zur Datenverarbeitung bei digitalen Angeboten so aufzuarbeiten, dass Verbraucherinnen und Verbraucher auf den ersten Blick schnell, einfach und umfassend alle wesentlichen Informationen zur Datenverarbeitung bekommen.
Durch ein „Mouseover" oder mit einem Link können Nutzer dann weitere Details erfahren. Mit dem „One-Pager" können Unternehmen auf einfache Weise ihre Datenverarbeitung gegenüber Verbraucherinnen und Verbrauchern im Internet transparent machen. Er ersetzt damit zwar nicht die förmliche Datenschutzerklärung nach dem Telemediengesetz, versucht aber als zusätzliches Informationsangebot wesentliche Aussagen zur Datenverarbeitung nutzerfreundlich aufzubereiten.

Bislang gab es jedoch keine belastbaren Erkenntnisse, ob der „One-Pager" zu einer höheren Informiertheit von Verbraucherinnen und Verbrauchern beiträgt. Die ConPolicy GmbH hat dazu eine Studie vorgenommen und stellt die Ergebnisse nun zur Verfügung. Die Studie fasst die inhaltlichen Ergebnisse des Forschungsvorhabens „Entwicklung und Validierung von Handlungsoptionen zur Förderung informierter Datenschutz-Einwilligungen (Einwilligung 2.0)" zusammen. Das Vorhaben wurde vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) durch die Bundesanstalt für Landwirtschaft und Ernährung (BLE) im Zeitraum vom 01.08.2016 bis zum 30.11.2017 gefördert.

Die ConPolicy-Studie zielt deshalb darauf ab, die Wirksamkeit des „One-Pagers" zu evaluieren, die Ergebnisse einzuordnen sowie weitere Lösungsansätze zu prüfen und hieraus Handlungsempfehlungen zur Förderung einer besseren Informiertheit im Datenschutz abzuleiten. Übergeordnet geht es der Studie darum, aufzuzeigen, durch welche Maßnahmen Entscheidungssituationen bei Einwilligungsprozessen zur Datenverarbeitung so ausgestaltet werden sollten, dass Verbraucherinnen und Verbraucher möglichst einfach, informiert und gemäß ihren individuellen Datenschutzpräferenzen handeln können.

Die gesamte Studie ist hier abrufbar. Eine Zusammenfassung der Studie (Policy Paper) findet sich hier.

Quelle: ConPolicy GmbH

BayLDA veröffentlicht 12 Muster für kleine Unternehmen und Vereine

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat erste Handreichungen für Vereine und kleine Unternehmen wie Handwerksbetriebe, Online-Shops und Arztpraxen erstellt. Die veröffentlichten Informationen sollen die wesentlichen Anforderungen des neuen europäischen Datenschutzrechts für diese Gruppe von Verantwortlichen möglichst kompakt und verständlich aufzeigen. Day BayLDA adressiert dabei gezielt kleine Organisationen wie z. B. kleine Handwerksbetriebe, Vereine, Online-Shops usw., um Handreichungen zu erstellen, um so klar wie möglich zu kommunizieren, welche wesentlichen Anforderungen diese Betriebe tatsächlich nach der DS-GVO zu erfüllen haben. Für folgende unterschiedlichen Arten von Verantwortlichen hat das BayLDA daher heute erste Muster veröffentlicht:

(1) Verein,
(2) Kfz-Werkstatt,
(3) Handwerksbetrieb,
(4) Steuerberater,
(5) Arztpraxis,
(6) WEG-Verwaltung,
(7) Produktionsbetrieb,
(8) Genossenschaftsbank,
(9) Online-Shop,
(10) Bäcker,
(11) Beherbergungsbetrieb und
(12) Einzelhändler

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Leitlinien für IT-Government und IT-Management

Zwei Monate vor Wirksamwerden der DS-GVO hat der Europäische Datenschutzbeauftragte (EDSB) zwei neue Leitlinien veröffentlicht. Die Leitlinien sollen den EU-Institutionen bei der Umsetzung des neuen EU-Datenschutzes eine Hilfestellung bieten, welches sich insbesondere durch die eine strengere Rechenschaftspflicht auszeichnet. Die Leitlinien behandeln Datenschutzanforderungen für das Management und die Steuerung der IT-Infrastruktur im Allgemeinen und für Cloud-Computing-Dienste im Besonderen. Sie bauen auf den Grundsätzen der GDPR auf, die in den Mitgliedstaaten ab dem 25. Mai 2018 gelten.

Die veröffentlichten Leitlinien sollen die jüngsten Bemühungen flankieren, die Organe, Agenturen und Einrichtungen der EU auf das neue Datenschutzrecht vorzubereiten.

Die Dokumente sind unter nachfolgenden URLs abrufbar:
https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf
https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf

Quelle: Der Europäische Datenschutzbeauftragte

Datenschutz im Whois-Verzeichnis nach der DS-GVO

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (sog. Berlin Group), die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Frau Maja Smoltczyk, geleitet wird, hat auf ihrer 62. Sitzung am 27. und 28. November 2017 in Paris (Frankreich) Empfehlungen für den Datenschutz von Webseiteninhaberinnen und -inhabern im WHOIS-Verzeichnis bei ICANN verabschiedet.

ICANN steht für Internet Corporation for Assigned Names and Numbers. Diese Organisation koordiniert die Vergabe von Namen und Adressen im Internet, um sicherzustellen, dass jede Webseitenadresse eindeutig ist. Bei der Registrierung von Webseiten werden nach den Regularien der ICANN zwingend personenbezogene Daten der Personen, die eine Webseite registrieren lassen (sog. Registranten), im WHOIS, dem Verzeichnis aller Inhaberinnen und Inhaber von Webseiten weltweit, veröffentlicht. Das Verzeichnis ist eine unbeschränkt zugängliche und frei durchsuchbare Datenbank. Auf die darin veröffentlichten Daten greifen die unterschiedlichsten Akteure für Werbe-, Marktforschungs-, Rechtsschutz-, Verbraucherschutz-, Strafverfolgungs- und andere Zwecke zu.

Die Berlin Group befasst sich bereits seit Jahren mit den daraus resultierenden datenschutzrechtlichen Problemen und hat diese im nun veröffentlichten Arbeitspapier zu Fragen der Privatsphäre und des Datenschutzes im Zusammenhang mit Daten von Registranten und dem WHOIS-Verzeichnis bei ICANN zusammengefasst. Dabei mahnt die Berlin Group insbesondere an, die Erforderlichkeit der Veröffentlichung von Daten an dem ursprünglichen Zweck des WHOIS-Verzeichnisses – Daten zur Kontaktaufnahme bei vorrangig technischen Problemen bereitzustellen – zu messen. Darüber hinaus hat die Arbeitsgruppe konkrete Empfehlungen für ICANN formuliert, an welchen Stellen aus Datenschutzsicht dringend nachgebessert werden muss.

Das Arbeitspapiere können sowohl in deutscher als auch englischer Sprache abgerufen werden.

Quelle: Berliner Beauftragte für Datenschutz und Informationsfreiheit

LfDI BW aktualisiert Ratgeber zum Beschäftigtendatenschutz (2. Auflage)

Die wachsende Zahl der beim LfDI eingehenden Beschwerden ist nur ein Indiz dafür, welch hohen Stellenwert der Arbeitnehmerdatenschutz inzwischen hat. Eigentlich selbstverständlich, wenn man überlegt, dass sich fast jeder von uns früher oder später im Arbeitsalltag wiederfindet – ob auf Seiten des Arbeitgebers oder auf der anderen Seite als Arbeitnehmer. Und wieviel Zeit man am Arbeitsplatz verbringt und dabei eine Flut an personenbezogenen Daten hinterlässt.

Gerade, weil der Bereich des Beschäftigtendatenschutzes fast jeden betrifft, hat der LfDI die bei ihm eingegangenen Beschwerden zum Anlass genommen, einen praxisbezogenen Ratgeber herauszugeben. Er spiegelt die interessante und vielfältige Arbeit aus dem Bereich des Beschäftigtendatenschutzes wider und präsentiert echte Fälle und deren Lösung.
Dieser praxisbezogene Ratgeber zum Beschäftigtendatenschutz ist ab sofort in einer überarbeiteten und der DS-GVO angepassten Version erhältlich.

Die 2. Auflage des Ratgebers finden Sie unter nachfolgender Adresse:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/Ratgeber-ANDS-2.-Auflage.pdf

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Datenschutz im Koalitionsvertrag der GroKo

Das „Forum Privatheit"-Policy Paper zum Koalitionsvertrag Datenschutz stärken, Innovationen ermöglichen – Wie man den Koalitionsvertrag ausgestalten sollte, bietet eine Analyse des Koalitionsvertrags in Bezug auf Digitalisierung und Datenschutz sowie Empfehlungen, welche konkreten Maßnahmen nötig sind, um die im Koalitionsvertrag noch abstrakt formulierten Ziele zu erreichen.

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 Koalitionsvertrag zwischen CDU, CSU und SPD verspricht einen „neuen Aufbruch für Europa", eine „neue Dynamik für Deutschland" und einen „neuen Zusammenhalt für unser Land". Dazu wollen die Koalitionäre umfangreiche Modernisierungen anstoßen. Als politische Grundlage der Großen Koalition ist der Koalitionsvertrag jedoch ein Kompromiss, der nur das konkret benennt, worauf sich die Koalitionäre inhaltlich einigen konnten. Vieles wird nur angedeutet, bleibt im Ungefähren und Abstrakten.

Daher hat der Expertenkreis „Forum Privatheit" untersucht, welche Maßnahmen ergriffen werden sollten, um die im Koalitionsvertrag genannten Ziele Innovationsförderung und Datenschutz inhaltlich auszugestalten. Es erläutert, welche Maßnahmen nun folgen müssen, um die Ziele Innovationsförderung und Datenschutz zu verbinden.

Quelle: Forum Privatheit

Speicherung und Übermittlung personenbezogener Daten im Rahmen einer Arztsuche

Die Parteien streiten um die Aufnahme der klagenden Ärztin in das Arztbewertungsportal der Beklagten.

Die Beklagte betreibt unter der Internetadresse www.jameda.de ein Arztsuche- und Arztbewertungsportal, auf dem Informationen über Ärzte und Träger anderer Heilberufe kostenfrei abgerufen werden können. Als eigene Informationen der Beklagten werden die sogenannten „Basisdaten" eines Arztes angeboten. Zu ihnen gehören – soweit der Beklagten bekannt – akademischer Grad, Name, Fachrichtung, Praxisanschrift, weitere Kontaktdaten sowie Sprechzeiten und ähnliche praxisbezogene Informationen. Daneben sind Bewertungen abrufbar, die Nutzer in Form eines Notenschemas, aber auch von Freitextkommentaren, abgegeben haben. Die Beklagte bietet den Ärzten den kostenpflichtigen Abschluss von Verträgen an, bei denen ihr Profil – anders als das Basisprofil der nichtzahlenden Ärzte – mit einem Foto und zusätzlichen Informationen versehen wird. Daneben werden beim Aufruf des Profils eines nichtzahlenden Arztes als „Anzeige" gekennzeichnet, die Profilbilder unmittelbarer Konkurrenten gleicher Fachrichtung im örtlichen Umfeld mit Entfernungsangaben und Noten eingeblendet. Demgegenüber blendet die Beklagte bei Ärzten, die sich bei ihr kostenpflichtig registriert und ein „Premium-Paket" gebucht haben, keine Konkurrenten auf deren Profil ein.

Die Klägerin ist niedergelassene Dermatologin und Allergologin. Im Portal der Beklagten wird sie als Nichtzahlerin gegen ihren Willen ohne Bild mit ihrem akademischen Grad, ihrem Namen, ihrer Fachrichtung und ihrer Praxisanschrift geführt. Bei Abruf ihres Profils auf dem Portal der Beklagten erscheinen unter der Rubrik „Hautärzte (Dermatologen) (mit Bild) in der Umgebung" weitere (zahlende) Ärzte mit demselben Fachbereich und mit einer Praxis in der Umgebung der Praxis der Klägerin. Dargestellt wird neben der Note des jeweiligen anderen Arztes die jeweilige Distanz zwischen dessen Praxis und der Praxis der Klägerin. Die Klägerin erhielt in der Vergangenheit mehrfach Bewertungen. Sie beanstandete durch ihre früheren Prozessbevollmächtigten im Jahr 2015 insgesamt 17 abrufbare Bewertungen auf dem Portal der Beklagten. Nach deren Löschung stieg die Gesamtnote der Klägerin von 4,7 auf 1,5.

Die Klägerin verlangt mit der vorliegenden Klage von der Beklagten die vollständige Löschung ihres Eintrags in www.jameda.de, die Löschung ihrer auf der Internetseite www.jameda.de veröffentlichten Daten, auf Unterlassung der Veröffentlichung eines sie betreffenden Profils auf der genannten Internetseite sowie Ersatz vorgerichtlicher Rechtsanwaltskosten. Das Landgericht hat die Klage abgewiesen. Die Berufung der Klägerin blieb ohne Erfolg. Mit der vom Berufungsgericht zugelassenen Revision verfolgt die Klägerin ihre Klageanträge weiter.

Die Entscheidung des Senats:

Die Revision hatte Erfolg. Der Senat hat der Klage stattgegeben.

Nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Dies war vorliegend der Fall.

Der Senat hat mit Urteil vom 23. September 2014 – VI ZR 358/13 (BGHZ 202, 242) für das von der Beklagten betriebene Bewertungsportal bereits im Grundsatz entschieden, dass eine Speicherung der personenbezogenen Daten mit eine Bewertung der Ärzte durch Patienten zulässig ist.

Der vorliegende Fall unterscheidet sich vom damaligen in einem entscheidenden Punkt. Mit der vorbeschriebenen, mit dem Bewertungsportal verbundenen Praxis verlässt die Beklagte ihre Stellung als„neutraler" Informationsmittler. Während sie bei den nichtzahlenden Ärzten dem ein Arztprofil aufsuchenden Internetnutzer die „Basisdaten" nebst Bewertung des betreffenden Arztes anzeigt und ihm mittels des eingeblendeten Querbalkens „Anzeige" Informationen zu örtlich konkurrierenden Ärzten bietet, lässt sie auf dem Profil ihres „Premium"-Kunden – ohne dies dort dem Internetnutzer hinreichend offenzulegen – solche über die örtliche Konkurrenz unterrichtenden werbenden Hinweise nicht zu. Nimmt sich die Beklagte aber in dieser Weise zugunsten ihres Werbeangebots in ihrer Rolle als „neutraler" Informationsmittler zurück, dann kann sie ihre auf das Grundrecht der Meinungs- und Medienfreiheit (Art. 5 Abs. 1 Satz 1 GG, Art. 10 EMRK) gestützte Rechtsposition gegenüber dem Recht der Klägerin auf Schutz ihrer personenbezogenen Daten (Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK) auch nur mit geringerem Gewicht geltend machen. Das führt hier zu einem Überwiegen der Grundrechtsposition der Klägerin, so dass ihr ein „schutzwürdiges Interesse an dem Ausschluss der Speicherung" ihrer Daten (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG) zuzubilligen ist.

Bundesgerichtshof: Urteil vom 20. Februar 2018 – VI ZR 30/17

Keine Verwendung personenbezogener Daten deutscher WhatsApp-Nutzer durch Facebook

Das Hamburgische Oberverwaltungsgericht hat entschieden, dass die Facebook Ireland Ltd. (Facebook) die personenbezogenen Daten deutscher WhatsApp-Nutzer vorerst nicht auf der Grundlage der bisher abgeforderten Einwilligung erheben und speichern darf (5 Bs 93/17). Damit bestätigt es die vorausgegangene Entscheidung des Verwaltungsgerichts Hamburg, das einen Eilantrag von Facebook gegen eine sofort vollziehbare Untersagungsverfügung des Hamburgischen Beauftragten für Datenschutz und Informationssicherheit (Datenschutzbeauftragter) abgelehnt hatte (13 E 5912/16).

Zur Begründung hat das Hamburgische Oberverwaltungsgericht im Wesentlichen ausgeführt: Es sei offen, ob die beanstandete Untersagungsverfügung rechtmäßig sei. Offen sei insbesondere, ob deutsches Datenschutzrecht zur Anwendung gelange und – wenn ja – ob der Datenschutzbeauftragte gegen Facebook mit Sitz in Irland vorgehen dürfe. In diesem Fall erweise sich die beanstandete Untersagung allerdings nicht als offensichtlich rechtswidrig. Denn die seit August 2016 abgeforderte Zustimmung der WhatsApp-Nutzer zu den neuen Nutzungsbedingungen und Datenschutzrichtlinien entspreche voraussichtlich nicht den deutschen Datenschutzvorschriften. Die vor diesem Hintergrund vorzunehmende Interessenabwägung führe zu einem Überwiegen der Interessen deutscher WhatsApp-Nutzer am Schutz ihrer personenbezogenen Daten.

AZ: 5 Bs 93/17
http://justiz.hamburg.de