Datenschutz Kundeninformation

Ausgabe 13/2019

Juli 2019

Liebe Leserinnen und liebe Leser,

in unserer aktuellen Ausgabe möchten wir Sie wieder über einige spannende Themen im Datenschutz informieren. In dieser Ausgabe lesen Sie unter anderem:

- Datenschutzverstöße
- Verwendung von Microsoft-Cloud-Diensten
- Umgang mit Fotos
- Interdisziplinäre Videokonferenzen
- Aktuelle Rechtsprechungen

ⓘ Quelle: https://www.cmshs-bloggt.de/tmc/datenschutzrecht/100-bussgelder-dsgvo-deutschland-uebersicht/

ⓘ Quelle: https://datenschutz.ekd.de/2019/04/11/verwendung-von-microsoft-clouddiensten-scheint-datenschutzkonform-moeglich/

Datenschutz-Kontakt
datenschutzbeauftragter@factpartner.de

Ein Jahr DSGVO – bereits mehr als 70 Bußgelder in Deutschland verhängt

Seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) sind in Deutschland bereits in über 70 Fällen Bußgelder verhängt worden. Das zeigt eine Umfrage des Handelsblatts unter den Datenschutzbeauftragten der Bundesländer.
Die meisten Strafen für Verstöße erfolgten erwartungsgemäß im bevölkerungsreichsten Land Nordrhein-Westfalen (rund 35).
Die drei bislang höchsten Bußgelder betrugen jeweils 80.000 Euro. Zwei davon verhängte Baden-Württemberg. In einem Fall wurden bei einer digitalen Publikation Gesundheitsdaten veröffentlicht, die versehentlich personenbezogene Daten enthielten.
In dem anderen Fall hatte ein Finanzunternehmen personenbezogene Daten unsachgemäß entsorgt.
Im Falle der dritten Strafe bemängelte die Behörde in Rheinland-Pfalz die Verarbeitung von Daten ohne Rechtsgrundlage sowie unterbliebene Löschung. In Berlin betrug ein Bußgeld 50.000 Euro. Hier hatte eine Bank Kundendaten unbefugt verarbeitet.
Bei einem verhängten Bußgeld in Höhe von 2.000 Euro in Sachsen-Anhalt hatte eine Privatperson wiederholt E-Mails an einen offenen Verteiler versendet (das heißt für alle Personen innerhalb des Verteilers sind auch alle anderen E-Mail-Adressen der übrigen Empfänger sichtbar).

Verwendung von Microsoft-Cloud-Diensten scheint datenschutzkonform möglich

Die Konferenz der Beauftragten für den Datenschutz in der EKD hat auf ihrer diesjährigen Sitzung die Entschließung zur Nutzung von Microsoft Cloud-Diensten verabschiedet.
Eine Verwendung von Microsoft Cloud-Diensten erscheint datenschutzkonform unter den folgenden Voraussetzungen möglich:
• Es wird von Microsoft eine wirksame Zusatzvereinbarung nach § 30 Abs. 5 DSG-EKD angeboten.
• Eine Verschlüsselung der Daten ohne Zugang von Microsoft ist möglich (HYOK = Hold your own Key).
• Die Übersendung von Telemetriedaten kann durch entsprechende Einstellungen unterbunden werden.

Die Datenschutzaufsichtsbehörden gehen davon aus, dass vor Einführung entsprechender Systeme eine Datenschutzfolgenabschätzung durchzuführen ist. Weiterhin sind folgende Themen zu berücksichtigen:
• Externe / Dritte dürfen keinen Zugriff auf Gesundheitsdaten haben (Verstoß gegen § 203 StGB)
• Es muss eine „echte“ End-to-End Verschlüsselung der Daten sein (die Daten bleiben vor, während und nach der Übertragung durchgehend verschlüsselt, gleiches gilt für die Ablage der Daten auf dem Server)
• Gesundheitsdaten müssen 30 Jahre verschlüsselt aufbewahrt werden

Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz verabschiedet

Quelle: https://www.isico-datenschutz.de/blog/2019/06/28/zweites-datenschutz-anpassungsgesetz/

Der Bundestag hat in der Nacht zum 28.06.2019 das zweite Datenschutz-Anpassungs- und Umsetzungsgesetz verabschiedet, das die seit Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) ergänzen soll. Hierdurch werden insgesamt 154 andere Gesetze geändert, wobei sich der Großteil der Änderungen lediglich auf Formulierungen bezieht. D. h. die Wortwahl der nationalen Gesetze werden an den Wortlaut der DSGVO angepasst.
Eine Änderung, die bereits im Vorfeld zu heftiger Kritik führte, sollte jedoch beachtet werden: Die Pflicht der Unternehmen zur Ernennung eines Datenschutzbeauftragten wurde aufgelockert. Während die Schwelle zur Ernennung eines Datenschutzbeauftragten bisher bei 10 Personen, die ständig mit der Verarbeitung von personenbezogenen Daten befasst sind, lag, wird sie für die Zukunft auf 20 erhöht. Als Grund hierfür wurde die finanzielle und regulatorische Entlastung für kleinere Unternehmen angeführt.
Kritiker mahnen allerdings, auch in kleineren Betrieben müsse der Datenschutz gewährleistet sein. Wenn der Experte für Datenschutz im Unternehmen fehle, würde die Einhaltung des Datenschutzes nur schwer von der Hand gehen. Dadurch würden hohe Bußgelder erst recht drohen. Außerdem könne das Vertrauen der Verbraucher und auch anderer Firmen in das Unternehmen leiden.
Fazit: Es sollte nicht voreilig auf die Bestellung eines Datenschutzbeauftragten verzichtet werden.

Umgang mit Fotos

Quelle: https://www.ra-himburg-berlin.de/fotorecht/faq/759-auf-dem-foto-ist-ein-verstorbener-muss-ich-auch-hier-jemanden-fragen-und-wenn-ja-wen.html

Ohne Einwilligung nur bei öffentlichen Veranstaltungen, Personen der Zeitgeschichte, Personen als Beiwerk oder höheres Interesse der Kunst

Quelle: https://www.rechtambild.de/2011/08/fotorechtliche-probleme-bei-der-event-und-partyfotografie/

Das Recht am eigenen Bild ist im Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) geregelt.
Demnach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt.
Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten.
Ohne Einwilligung dürfen Bilder zum Beispiel lediglich von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben (…); verbreitet und zur Schau gestellt werden.

Sanktionen
Handelt man gegen die gesetzliche Regelung kann es ungemütlich bzw. teuer werden, denn mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen den des KunstUrhG ein Bildnis verbreitet oder öffentlich zur Schau stellt.

Fazit / Empfehlung
- Einwilligungen für Fotos sind vorab immer unter Angabe des Verwendungszwecks und der Möglichkeit des Widerspruchsrechts vom Betroffenen einzuholen.
- Da das Recht am eigenen Bild gem. § 22 Satz 3 KunstUrhG erst 10 Jahre nach dem Tod des Abgebildeten endet, dürfen auch Fotos, auf denen Verstorbene abgebildet sind, nicht einfach genutzt werden. Bei einer Nutzung eines Fotos eines Verstorbenen innerhalb von 10 Jahren nach dessen Tod sind die Angehörigen des Verstorbenen um Erlaubnis zu fragen. Dies sind entweder der überlebende Ehegatte oder Lebenspartner, die Kinder oder, wenn diese nicht vorhanden sind, die Eltern des Verstorbenen.

• Bei öffentlichen Veranstaltungen (z.B. auf Events) kann auf eine Einwilligung verzichtet werden, wenn der Fokus nicht auf der einzelnen Person liegt. Man kann weiterhin von einer konkludenten Einwilligung der am Event beteiligten Person ausgehen, dennoch ist mit der Annahme solch konkludenter Einwilligungen vorsichtig umzugehen, da eine korrekte Beurteilung sehr stark vom Einzelfall abhängig ist.

Zum Umgang mit Bildern von Kindern und Jugendlichen hat die Konferenz der Diözesandatenschutzbeauftragten im April 2019 einen neuen Beschluss gefasst: https://www.katholisches-datenschutzzentrum.de/infothek/

Interdisziplinäre Videokonferenzen

Unsere Gesellschaft erlaubt es häufig nicht, dass Mitglieder eines Gremiums bei gemeinsamen Sitzungen am selben Ort sein können. Aber auch bei der Einholung eines Konsils wird der Austausch der erforderlichen Informationen nicht immer persönlich möglich sein. Zunehmend gibt es daher Überlegungen, in der Praxis eigene Videokonferenztools oder sogar die Videofunktion von Messenger-Diensten zu nutzen.

Messenger-Dienste
Von einem Einsatz sollte grundsätzlich abgesehen werden, da viele Dienste ihre Tücken haben und die Handhabung nicht immer praktikabel ist.

Skype
Das Tool geriet 2016 in den Fokus der Landesdatenschutzbeauftragten Nordrhein-Westfalen und Berlin, im Zusammehang mit dessen Einsatz bei Video-Vorstellungsgesprächen. Die Behörden kritisierten insbesondere, dass die Kommunikation für bis zu 90 Tage auf Servern in den USA zwischengespeichert wird, es findet somit eine Datenübermittlung von besonderen Arten personenbezogener Daten (Gesundheitsdaten) in ein Drittland statt.

TeamViewer
Kritikpunkt des Landesdatenschutzbeauftragten Mecklenburg-Vorpommerns war beim Einsatz von TeamViewer, dass im Hinblick auf den für die verschlüsselte Kommunikation erforderlichen öffentlichen Schlüssel nicht sichergestellt werden könne, dass dieser tatsächlich vom angestrebten Kommunikationspartner stammt. Dieser würde vom TeamViewer-Server ohne Identifikationsnachweis übertragen. Aus diesem Grunde sah der Landesdatenschutzbeauftragte eine Anwendung bei Daten mit hohem Schutzbedarf (hierzu gehören Gesundheitsdaten zweifelsohne) als unzulässig an. Als Lösung des Problems wurde zur Nutzung des sogenannten SRP-Protokolls durch TeamViewer geraten. Mittels dieses Protokolls kann geprüft werden, ob beide Parteien, die über TeamViewer miteinander kommunizieren wollen, im Besitz eines gemeinsam vorher festgelegten Passwortes sind. Nur wenn dieser Umstand gegeben ist, sind die Kommunikationspartner diejenigen, die auch tatsächlich miteinander kommunizieren wollen. Mittlerweile kommt das SRP-Protokoll bei TeamViewer zum Einsatz. Damit fällt der einzige bekannte Kritikpunkt weg. Da sich zudem alle TeamViewer-Server innerhalb der Europäischen Union befinden, besteht auch keine Drittland-Problematik.

Fazit
Bei der Auswahl und beim Einsatz eines geeigneten Instruments sollten noch verschiedene Aspekte berücksichtigt werden, mindestens jedoch:

• Nutzung der aktuellsten Software: da die Software nur so sicher ist, wie die

ⓘ Quelle: Datenschutz im Blick. Newsletter für den Datenschutz im Gesundheitswesen. AOK Verlag, Ausgabe April/Mai 2019

Messenger-Dienste und Skype sollen nicht genutzt werden - Teamviewer hat nachgebessert

schwächste eingesetzte Version, ist sicherzustellen, dass immer die aktuellste genutzt wird
• Vertraulichkeit: es ist sicherzustellen, dass bei den Beteiligten nicht weitere Personen unerkannt im Raum anwesend sind und der Konferenz beiwohnen können
• keine Aufzeichnung: es muss gewährleistet werden, dass keiner der Beteiligten die Konferenz - unbemerkt - aufzeichnet)
• Datensparsamkeit: auch bei der Konferenz unter Berufskollegen und -geheimnisträgern gilt der Grundsatz der Datensparsamkeit; es sind nur die Dokumente und Informationen mit den Beteiligten zu teilen, die für die Konferenz oder das Konsil zwingend notwendig sind – auf Namen oder andere Identifikationsdaten kann in der Regel verzichtet werden.

Aktuelle Rechtssprechungen

ⓘ Quelle: RDV – Zeitschrift für Datenschutz, Informations- und Kommunikationsfreiheit Ausgabe 3/2019 S. 137-138

Unterrichtung des Betriebsrates über Arbeitsunfälle von Fremdpersonal
(Bundesarbeitsgericht – Beschluss vom 12. März 2019 – 1 ABR 48/17)
Der Betriebsrat kann vom Arbeitgeber verlangen, über Arbeitsunfälle unterrichtet zu werden, die Beschäftigte eines anderen Unternehmens im Zusammenhang mit der Nutzung der betrieblichen Infrastruktur des Arbeitgebers erleiden.
Nach § 89 Abs. 2 des Betriebsverfassungsgesetzes muss der Betriebsrat vom Arbeitgeber bei allen in Zusammenhang mit dem Arbeitsschutz und der Unfallverhütung stehenden Fragen hinzugezogen werden. Hiermit korrespondiert ein entsprechender Auskunftsanspruch des Betriebsrats. Dieser umfasst im Streitfall auch Unfälle, die Arbeitnehmer erleiden, die weder bei der Arbeitgeberin noch deren Leiharbeiter sind. Aus den Arbeitsunfällen des Fremdpersonals können arbeitsschutzrechtliche Erkenntnisse für die betriebszugehörigen Arbeitnehmer, für die der Betriebsrat zuständig ist, gewonnen werden. Demgemäß ist der Betriebsrat unverzüglich über jeden Arbeitsunfall eines Arbeitnehmers einer Servicepartnerfirma im Betriebsgebäude unter Angabe des Datums, der Uhrzeit des Unfalls, der Unfallstelle, des Unfallhergangs sowie über die erlittenen Verletzungen zu unterrichten.

ⓘ Quelle: RDV – Zeitschrift für Datenschutz, Informations- und Kommunikationsfreiheit Ausgabe 3/2019 S. 141

Anspruch des Betriebsrats auf Einsichtnahme in nicht anonymisierte Bruttolohn- und Gehaltslisten
(Landesarbeitsgericht Sachsen-Anhalt – Beschluss vom 18. Dezember 2019 – 4 TaBV 19/17-)
Die Listen über die Bruttolöhne und -gehälter müssen dem Betriebsausschuss nicht anonymisiert zur Einsichtnahme bereitgestellt werden.
§ 26 Abs. 1 S. 1 BDSG erlaubt ausdrücklich die Datenverarbeitung zum Zwecke der Ausübung von Rechten der Interessenvertretung der Beschäftigten und stellt damit das Einsichtnahmerecht des Betriebsausschusses nach § 80 Abs. 2 S. 2 BetrVG auf eine rechtssichere Grundlage. Durch das Entgelttransparenzgesetz wird das Einsichtnahmerecht des Betriebsrates nach § 80 Abs. 2 S. 2 BetrVG erweitert, der Arbeitgeber hat nicht nur vorhandene Listen zur Verfügung zu stellen, sondern diese noch nach Geschlecht aufzuschlüsseln und so aufzubereiten, dass der Betriebsausschuss im Rahmen seines Einblickrechts seine Aufgaben ordnungsgemäß erfüllen kann.

Impressum
FAC'T GmbH
Hohenzollernring 70
48145 Münster

info@factpartner.de
www.factpartner.de

Telefon 0251 935-3700
Telefax 0251 935-4075