Datenschutz newsbox

Ausgabe 1 2019

DATAKONTEXT

Editorial

Während sich (sogar) Brad Smith, President und Chief Legal Officer von Microsoft, in einem Essay auf der Firmen-Webseite sehr kritisch zum Einsatz einer von künstlicher Intelligenz befeuerten Gesichtserkennung erklärt, wird in einem Besucher-WC im Park von Peking Toilettenpapier mit Hilfe von Gesichtserkennung rationiert. Nach einer erfolgten Gesichtserkennung werden an die Besucher zwischen 60 und 70 cm Toilettenpapier ausgegeben. Auch hierzulande erhitzen sich an dem Thema Gesichtserkennung zu Recht die Gemüter. Man möchte aber meinen, dass die Preisgabe von Grundrechten noch nicht ganz so leichtfertig erfolgt wie in dem stillen Örtchen irgendwo in Peking.

Die im Dezember 2018 und Januar 2019 bekannt gewordenen Veröffentlichungen von Daten aus dem Privatleben zahlreicher Politiker und Prominenter führten zu einer Diskussion über Reformen des IT-Rechts in Deutschland. Die Feststellung, dass die Weiterentwicklung des Rechts womöglich rascher befördert wird, wenn politische Akteure Schaden erleiden, klingt leider zynischerweise schlüssig.

Vielleicht wären die politischen Konsequenzen eines Daten-Leaks mit über 200 Millionen Lebensläufen auch in China anders bewertet worden, wenn es sich um Daten von Politikern oder Prominenten gehandelt hätte?

Dabei besagen Studien, dass jeder zweite Internetnutzer in Deutschland im vergangenen Jahr Opfer von Cyberkriminalität geworden ist. Wie Onlinekriminalität nachhaltig zu bekämpfen ist, müsste damit eine gesellschaftsübergreifende Fragestellung sein. Unabhängig von dem Gefühl für die eigene Sicherheit im Online-Bereich, befürchtet die Mehrheit der Deutschen sogar, dass Deutschland nicht ausreichend auf einen großen Cyberangriff vorbereitet ist.

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

Rechtswidrige Videoüberwachung aufgrund mangelhafter TOMs

In Schwerin betreibt das Land Mecklenburg-Vorpommern eine Videoüberwachungsmaßnahme auf dem Schweriner Marienplatz. Diese zielt nach Angaben des Innenministeriums primär darauf ab, potenzielle Täter von einer Tatbegehung abzuhalten. Der Landesbeauftragte für Datenschutz und Informationsfreiheit, Heinz Müller, erklärt diese nun aufgrund von unzureichenden technischen und organisatorischen Maßnahmen (TOM) für rechtswidrig.
Der Landesbeauftragte war schon seit Ende 2016 in die Planungen des Landesministeriums für Inneres und Europa für die Videoüberwachung einbezogen. Die Videoaufnahmen durch acht auf dem Marienplatz installierte Kameras werden demnach drahtlos in das Schweriner Polizeizentrum übermittelt. Für eine sichere Übertragung müssten die Daten so verschlüsselt werden, dass sie an keiner Stelle des Übertragungsweges von Unbefugten mitgelesen werden können. Die dafür erforderliche Ende-zu-Ende-Verschlüsselung findet jedoch nicht statt. Deswegen kommt der Landesbeauftrage Müller zu dem Schluss: „Die Videoüberwachung auf dem Marienplatz ist rechtswidrig, weil eine angemessene Sicherheit der dabei verarbeiteten personenbezogenen Daten der Bürgerinnen und Bürger nicht gewährleistet ist."
Die Ende-zu-Ende-Verschlüsselung war von den für die Videoüberwachung verantwortlichen Stellen von Anfang an vorgesehen. Die Erforderlichkeit dieser Maßnahme zum Schutz der übertragenen Daten stand nie in Frage. Am 21. Dezember 2018 nahm das Ministerium für Inneres und Europa den geplanten vorläufigen Wirkbetrieb der Videoüberwachung auf. Eine Ende-zu-Ende-Verschlüsselung war dafür jedoch nicht eingerichtet worden. Daraufhin sprach der Landesbeauftragte wegen des darin liegenden Verstoßes gegen die Datenschutz-Grundverordnung (DS-GVO) eine formelle Warnung nach Art. 58 Abs. 2 lit. a DS-GVO aus. Das Innenministerium nahm die Anlage dennoch in Betrieb. Noch dazu verlängerte es den vorläufigen Wirkbetrieb bis zum 31. Januar 2019.
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung durch geeignete technische und organisatorische Maßnahmen wie die Verschlüsselung der Daten ein. Als verantwortliche Stelle muss das Innenministerium im Sinne seiner Rechenschaftspflicht nachweisen können, dass bei der Videoüberwachung des Schweriner Marienplatzes die Vorschriften des Datenschutzrechts eingehalten werden. Ohne TOMs kann der Nachweis aber jedenfalls nicht vollständig erbracht werden.

Quelle: DataAgenda

Namensschilder und Auftragsverarbeitung?

Frage des GDD-Erfa-Kreises Würzburg:
Unternehmen A beschäftigt Arbeiter, die spezielle Arbeitskleidung tragen. Diese wird von einem Dienstleister B gereinigt. Auf der Arbeitskleidung ist der Name des Arbeiters angebracht. Ist in den folgenden Konstellationen jeweils ein Auftragsverarbeitungs-vertrag zu schließen?
a) Der Dienstleister holt die Kleidung bei A, reinigt diese bei sich und bringt diese wieder zu A. Dort sortiert er die Kleidung nach Namen in die mit Namen beschrifteten Spinde der betroffenen Arbeiter.
b) Die betroffenen Arbeiter gehen zu B und werden dort vermessen, um individuell passende Kleidung zu erhalten. Die Vermessungsdaten werden personenbezogen bei B gespeichert. Die Reinigung der Kleidung erfolgt wie bei a).
c) Der Dienstleister holt/bekommt die Kleidung, reinigt diese und bringt diese nur zum Empfang von A, eine Verteilung an die Arbeiter erfolgt durch B nicht.

Antwort BayLDA:
Siehe hierzu die von uns veröffentlichte Übersicht zur Abgrenzung zwischen Auftragsverarbeitung und anderen Sachverhalten unter https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf. Demnach ist die Reinigung von Berufskleidung mit Namensschildern nicht als Auftragsverarbeitung einzustufen, da es bei dieser Leistung nicht im Kern um eine Verarbeitung personenbezogener Daten geht, sondern um eine Dienstleistung anderer Art (eben Reinigung), und die personenbezogenen Daten hier nur Beiwerk darstellen. Eine Differenzierung nach den Fallgruppen a) -c) sehen wir nicht als sachgerecht an; keiner dieser Fälle stellt Auftragsverarbeitung dar.

Die ePrivacy-Reform steckt fest: Rat findet keine Position

Der bereichsspezifische Datenschutz in der elektronischen Kommunikation sollte nach ursprünglicher Planung gemeinsam mit der Datenschutz-Grundverordnung (DS-GVO) fertig reformiert werden. Der Vorschlag für eine ePrivacy-Verordnung liegt seit Anfang des Jahres 2017 auf dem Tisch, das EU-Parlament ist seit Herbst 2017 startklar. Nur bei den Mitgliedstaaten im Rat passiert seit fast zwei Jahren wenig.
Die für Telekommunikation zuständigen EU-Minister haben sich am 4. Dezember 2018 in Brüssel unter anderem zur geplanten ePrivacy-Verordnung beraten. Diese soll die EU-Regeln zur Vertraulichkeit der Kommunikation modernisieren, etwa hinsichtlich der zunehmenden Nutzung von Messengerdiensten. Diese sog. OTT-Dienste (over the top-Dienste) sind vom aktuellen ePrivacy-Recht noch gar nicht erfasst.
Bis jetzt ist es der konservativen österreichischen Ratspräsidentschaft nicht gelungen, eine gemeinsame Position zu finden.
Die sogenannten Triloge, die Verhandlungen von EU-Parlament, Kommission und Mitgliedstaaten über einen Gesetzesvorschlag, können erst beginnen, wenn sich neben den Abgeordneten auch die EU-Staaten auf eine erste Position geeinigt haben. Es bleibt wohl wenig Hoffnung, dass dies unter der österreichischen Ratspräsidentschaft in den verbleibenden zwei Wochen im Jahr 2018 noch gelingt. Danach wird sich Rumänien in seiner ersten EU-Ratspräsidentschaft überhaupt dem Thema weiter widmen müssen. Im Rahmen dessen könnte eine Einigung unter den Mitgliedstaaten in diesem Bereich einen bedeutsamen Erfolg darstellen.

Übermittlung personenbezogener Daten ins Drittland nach DS-GVO

Frage des GDD-Erfa-Kreises Würzburg:
Unternehmen A (z. B. Produktion) ist Teil eines Konzerns und sitzt in einem Nicht-EU-Land, z. B. China. Das Unternehmen B des Konzerns (Hauptverwaltung) mit Sitz in Bayern ist für die weltweite Personalverwaltung zuständig. Muss man Art. 3 DS-GVO dahin interpretieren, dass A als Auftraggeber mit B als Auftragnehmer (!) einen Auftragsverarbeitungsvertrag bzw. EU-Standardvertragsklauseln abschließen muss oder richtet sich die Übertragung der personenbezogenen Daten der Beschäftigten von A ausschließlich nach dem Datenschutzrecht des Landes von A, hier China?

Antwort BayLDA:
Es ist zu prüfen, welche Funktion B hier hat. „Zuständigkeit für die weltweite Personalverwaltung" könnte bedeuten, dass B Teile der Arbeitgeberfunktionen (auch) des Unternehmens A übertragen bekommen hat – dann wäre B insoweit Verantwortlicher. Es könnte aber auch bedeuten, dass B lediglich Auftragsverarbeiter für A ist, soweit es um Daten von Beschäftigten von A geht. D.h. es muss anhand der praktischen Gegebenheiten geklärt werden, ob B Auftragsverarbeiter oder Verantwortlicher ist.
Wenn B Verantwortlicher ist, muss B natürlich als Verantwortlicher die DS-GVO gemäß Artikel 3 Abs. 1 DS-GVO einhalten, auch bezüglich der Daten, die von Beschäftigten des A stammen.
Dies bedeutet unter anderem auch, dass für die (Rück-)Übermittlung der Daten dieser Beschäftigten von B an A nach China ein Standardvertrag abzuschließen ist (einschlägig ist ein Standardertrag für Übermittlungen von Verantwortlichem an Verantwortlichen, d.h. „Controller-to-Controller").
Wenn B Auftragsverarbeiter ist, gelten für B nur die Pflichten eines Auftragsverarbeiters, wie sie in der DS-GVO definiert sind, also z.B. die Pflicht zur Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO. Allerdings zählt dazu auch die Pflicht, als Auftragsverarbeiter mit A einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO abzuschließen, da auch dies (nach Ansicht der Datenschutzbehörden) eine Pflicht (auch) des Auftragsverarbeiters ist. Wenn B lediglich Auftragsverarbeiter ist, muss B mit A für die (Rück-) Übermittlung der Daten der chinesischen Beschäftigten keinen Standardvertrag abschließen, da diese Konstellation nach unserer Auffassung keine „Übermittlung in ein Drittland" im Sinne der Artikel 44 bis 49 DS-GVO darstellt.

TOMs für den E-Mail-Versand

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) erläutert in einem aktuellen Beitrag, welche technischen Anforderungen und welche technischen und organisatorischen Maßnahmen ihrer Meinung nach bei dem Versand einer E-Mail beachtet werden sollten.
Zunächst wird darauf hingewiesen, bei einer datenschutzrechtlichen Beurteilung sowohl die Inhaltsdaten (d.h. dem Text und ggf. vorhandener Anhänge) einer E-Mail, als auch deren sog. Metadaten (bspw. Absender, Empfänger, Zeitstempel etc) zu betrachten sind, da sowohl Inhalts- als auch Metadaten personenbezogene Daten beinhalten können.
Danach werden die unterschiedlichen Anforderungen bei der Übermittlung von E-Mails zwischen einer Verschlüsselung auf Inhaltsebene und einer Verschlüsselung auf Transportebene ausgearbeitet.
Die nach Ansicht der LDI NRW zu beachtenden TOMs werden abschließend wie folgt zusammengefasst:

- Die Kommunikation per E-Mail bedarf mindestens der Transport-Verschlüsselung, wie sie von den namhaften europäischen Providern standardmäßig angeboten wird.
- Die Transportverschlüsselung sollte entsprechend der Technischen Richtlinie „BSI TR-03108 Sicherer E-Mail-Transport“ implementiert sein. In Abhängigkeit vom Schutzbedarf der versendeten Daten und dem Risiko können Abweichungen von der Richtlinie statthaft sein.
- Es ist zu berücksichtigen, dass bei einer Transportverschlüsselung die E-Mails auf den E-Mail-Servern im Klartext vorliegen und grundsätzlich einsehbar sind. Bei besonders schützenswerten Daten (z.B. Kontobewegungsdaten, Finanzierungsdaten, Daten zum Gesundheitszustand, Mandantendaten von Rechtsanwälten und Steuerberatern, Beschäftigtendaten) ist eine alleinige Transportverschlüsselung möglicherweise nicht ausreichend. Zusätzliche technische und organisatorische Maßnahmen, wie z. B. eine Ende-zu-Ende-Verschlüsselung können geboten sein. Sollte dies nicht gewährleistet werden können, sind ggf. alternative Übertragungswege denkbar: Hierzu zählen der elektronische Austausch über eine gesicherte Verbindung (Web-Portal des Verantwortlichen mit Zugangsbeschränkungen) oder die klassische postalische Zusendung.
- Der Betreff der E-Mail sollte keine personenbezogenen Daten enthalten.

Die LDI NRW weist daraufhin, dass die DSK aktuell Empfehlungen zur datenschutzkonformen E-Mail-Kommunikation ausarbeitet, so dass die Ausführungen der LDI NRW unter dem Vorbehalt späterer Anpassungen an die Empfehlungen stehen.

Anwaltverein stellt Unterlagen zur DS-GVO bereit

Der Deutsche Anwalt Verein (DAV) stellt seinen Mitgliedern verschiedene Unterlagen zur Umsetzung der DS-GVO zum Download bereit. Die seit dem 25. Mai 2018 wirksame Datenschutz-Grundverordnung (DS-GVO) gilt selbstverständlich auch für Anwaltskanzleien, so dass Datenschutzbehörden auf Beschwerden von Mandanten, Mitarbeitern, Prozessgegnern und anderen Dritten mit förmlichen Verfahren reagieren müssen. Für sie stellt der DAV Merkblatt, Muster und Checkliste bereit.
Der DAV weist darauf hin, dass die Rechte für das DAV-Merkblatt und die DAV-Muster beim Deutschen Anwaltverein liegen. Mitglieder eines dem DAV angeschlossenen Anwaltvereins können das DAV-Merkblatt und die DAV-Muster nutzen, um in ihrer Kanzlei die Anforderungen der Datenschutz-Grundverordnung zu erfüllen. Sie sind nicht für die Nutzung durch Dritte, insbesondere für die Bearbeitung von Mandaten, bestimmt.
Einen Überblick, was den Umsetzungsbedarf hinsichtlich der DS-GVO insbesondere für Anwaltskanzleien betrifft, gibt ein DAV-Merkblatt zum Thema. Daneben kann der interessierte Anwalt auf die Hinweise zur Datenverarbeitung (zur Übergabe bei Mandatsbeginn) zurückgreifen. Die Datenschutzerklärung (für die Kanzlei-Website) sowie die technischen und organisatorische Maßnahmen der Datensicherheit (zur Dokumentation und zur Vorlage bei Überprüfungen) ergänzen das Paket. Das DAV-Musterverzeichnis der Verarbeitungstätigkeiten (xls) nach Art. 30 DSGVO (zur Dokumentation und zur Vorlage bei Überprüfungen) rundet die Dokumente ab.

Quelle: *Deutscher Anwaltverein*

Sog. „Streckengeschäft“ als Auftragsverarbeitung?

Frage des GDD-Erfa-Kreises Würzburg:
Unternehmen A ist Produzent von Waren. Er verkauft diese an den Händler B. Händler B verkauft die Ware entweder an einen Endverbraucher C oder einen weiteren Händler. A wird von B angewiesen, die Ware direkt an C zu liefern und übergibt A für diesen Zweck die Adresse von C. Ist in solchen Konstellationen ein Auftragsverarbeitungsvertrag zwischen B und A zu schließen?

Antwort BayLDA:
Bei dieser herkömmlicherweise als Streckenlieferung/Streckengeschäft bezeichneten Konstellation liegt nach unserer Auffassung kein Fall von Auftragsverarbeitung vor, vielmehr ist A beim Umgang mit den Endverbraucherdaten selbst als Verantwortlicher einzustufen (auch diese Konstellation haben wir in unserem Papier zur Abgrenzung zwischen Auftragsverarbeitung und anderen Fallgestaltungen erwähnt, https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf).

GDD-Ratgeber „Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG“ in zweiter Auflage

Das GDD-Institut für Datenschutzbeauftragte befasst sich kontinuierlich mit Aufgaben und Rechtsstellung von Datenschutzbeauftragten sowie der Entwicklung von Standards zur Aus- und Weiterbildung von Datenschutzverantwortlichen.

Der Datenschutzbeauftragte hat eine zentrale Rolle im Hinblick auf die Gewährleistung des Datenschutzes im Unternehmen. Er berät die Unternehmensleitung sowie die Fachabteilungen, die mit personenbezogenen Daten umgehen, im Hinblick auf den Datenschutz und überwacht die Einhaltung der bestehenden datenschutzrechtlichen Vorgaben beim Verantwortlichen bzw. Auftragsverarbeiter. Hierdurch leistet er einen wichtigen Beitrag zum Persönlichkeitsrechtsschutz und hilft zugleich Unternehmensrisiken zu reduzieren, welche sich vor dem Hintergrund der immensen Bußgeldandrohungen der DS-GVO in neuem Maße ergeben. Die Aufgabe des Datenschutzbeauftragten erschöpft sich dabei nicht bloß in der Unterrichtung des Verantwortlichen bzw. Auftragsverarbeiters über dessen Verpflichtungen. Er ist vielmehr aktiver Berater in der Weise, dass er an der Legalisierung legitimer Verarbeitungen mitwirkt und Lösungswege aufzeigt. Er unterstützt bei konkreten datenschutzrechtlichen Fragen, Prozesseinführungen sowie -änderungen.

Der vorliegende Ratgeber beleuchtet im Detail, unter welchen Voraussetzungen ein Datenschutzbeauftragter zu benennen ist und welche Aufgaben und welche Rechtsstellung ihm zukommen. Abgerundet werden die Ausführungen durch praxisrelevante Muster und Materialien.

Der Ratgeber ist für GDD-Mitglieder im geschlossenen Bereich abrufbar.

Krankmeldung per WhatsApp

Wer sich morgens zu schlapp für die Arbeit fühlt, ist froh, wenn er leidend liegen bleiben darf oder schafft es vielleicht gar nicht erst bis zum Arzt. Da muss man möglicherweise gar nicht hin. Bei „AU-Schein.de“ kann man Krankheitssymptome von „Nase verstopft“ bis „Niesen“ anklicken und per WhatsApp an einen Arzt schicken. Weitere Angaben, etwa zum Kontakt mit Risikogruppen oder wie lange man sich schon und voraussichtlich noch krank fühlt, runden das per Mausklick skizzierte Krankheitsgefühl ab. Wenn es sich mit der Prüfung des Arztes am anderen Ende des Datenkanals deckt, schickt er den gelben Schein zur Weiterleitung an den Arbeitgeber zunächst per WhatsApp und später per Post.
Das ist eine Art Telemedizin, die irritierend, aber praktisch ist. Arztrechtlich diskutabel ist sie zumindest in Schleswig-Holstein, weil das Berufsrecht dort einen weitreichenden Einsatz von Telemedizin gestattet. Dort sitzt der Arzt, der den Krankenschein ausstellt. Sensible Gesundheitsdaten WhatsApp anzuvertrauen, ist ein Datenschutzrisiko, über das der Anbieter der App umfassend informieren muss. Ein weiteres Risiko ist die Akzeptanz der Krankmeldung durch den Arbeitgeber. Vielleicht erkennt er sie ohne persönlichen Kontakt zum Arzt nicht an und begreift das Fernbleiben von der Arbeit als unentschuldigt. Bei einer Kündigung wegen Arbeitsverweigerung muss man dem Richter nicht nur nachweisen, dass man krank war, sondern auch, dass die Krankmeldung auch wirklich rechtlich wirksam war.

Quelle: *DataAgenda*

Handlungsleitfaden: Wirtschaftsspionage und Konkurrenzausspähung

In dem vom BMBF geförderten Projekt *Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa*, kurz WISKOS, stand die systematische Analyse der Bedrohung kleiner und mittlerer Unternehmen (KMU) durch Wirtschaftsspionage und Konkurrenzausspähung im Mittelpunkt. Zusätzlich beschäftigte sich das Projekt mit den Gefahren für Wissenschaftsorganisationen sowie mit der polizeilichen Perspektive auf den Deliktsbereich.
Das vorrangige Interesse bestand in der Herausarbeitung von Möglichkeiten zur Prävention von Know-how-Verlusten und dem Schutz vertraulicher Informationen. Mit diesem Ziel vor Augen verfolgte das Forscherteam einen geografisch wie methodisch breit gefächerten Ansatz.

Zum Abschluss des Projekts wurden Informationsmaterialien und Handlungsleitfäden für KMU, Wissenschaftsorganisationen und die Polizei entwickelt.

Quelle: *Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.*