Datenschutz newsbox

Ausgabe 10 2019

DATAKONTEXT

Editorial:

Diesen Monat hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen jährlichen Bericht zur Lage der IT-Sicherheit vorgestellt.
Der Bericht zur Lage der IT-Sicherheit in Deutschland 2019 gibt einen Überblick über die Entwicklung der Bedrohungslage im Cyber-Raum vom 1. Juni 2018 bis zum 31. Mai 2019 und über die Aktivitäten und Maßnahmen des BSI in diesem Zeitraum. Ein wesentliches Risiko für Anwender in Gesellschaft, Wirtschaft und Staat ging dabei von der Schadsoftware „Emotet" aus, die für erhebliche Schäden im Berichtszeitraum verantwortlich war, so der Bericht.

Insgesamt haben Ransomware-Angriffe, auch unabhängig von „Emotet" zugenommen und neben zahlreichen Produktionsausfällen in der Wirtschaft zu teils erheblichen Beeinträchtigungen in Einrichtungen des Gemeinwesens geführt. So seien mehrere Krankenhäuser sowie kommunale Einrichtungen wie etwa Stadtverwaltungen in Deutschland von solchen Angriffen betroffen. Nicht betroffen war die Informationstechnik der Bundesverwaltung, für deren Sicherheit das BSI zuständig ist.

Im Vorwort des Berichts verkündet der Bundesminister des Innern, für Bau und Heimat, Horst Seehofer, dass mit dem IT-Sicherheitsgesetz 2.0 dem BSI der Verbraucherschutz als zusätzliche Aufgabe zugewiesen werden wird. Auch die Handlungsfähigkeit staatlicher Einrichtungen ist Voraussetzung für das Vertrauen in die Handlungsfähigkeit des Staates und damit auch Garant für die Innere Sicherheit der Bundesrepublik Deutschland. Zum KRITIS-Sektor „Staat und Verwaltung" gehören, neben der Regierung und Verwaltung sowie Parlament, auch die Justizeinrichtungen.

Angesichts der Berichte über die Lage der IT-Sicherheit im Berliner Kammergericht drängt sich jedoch die Frage auf, ob die dortigen Defizite tatsächlich ein Einzelfall sind. Sonst heißt es womöglich auch in anderen Gerichten in Zukunft des Öfteren: „Das Kammergericht ist bis auf Weiteres nur telefonisch, per Fax und postalisch zu erreichen.", fürchtet Ihr

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

Europäischer Datenschutzausschuss konkretisiert Art. 6 Abs.1 lit. b DS-GVO

Am 8. Oktober 2019 haben die im Europäischen Datenschutzausschuss (EDPB) versammelten nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte ihre „Leitlinie 2/2019 zur Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. b DS-GVO im Rahmen der Bereitstellung von Online-Diensten für betroffene Personen“ verabschiedet. Diese Leitlinien betreffen den Geltungsbereich und die Anwendung von Art. 6 Abs. 1 lit. b DS-GVO im Zusammenhang mit Diensten der Informationsgesellschaft.
Die Leitlinien 2/2019 konzentrieren sich auf die Anwendbarkeit von Art. 6 Abs. 1 lit. b DS-GVO. Dabei geben sie Aufschluss über die Verarbeitung personenbezogener Daten im Rahmen von Verträgen für Onlinedienste, unabhängig davon, wie die Dienste finanziert werden. Zu diesem Zweck enthalten die Leitlinien:

- eine Darstellung der Elemente der rechtmäßigen Verarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO und
- eine Betrachtung des Begriffs „Notwendigkeit“, wie er „für die Erfüllung eines Vertrags erforderlich“ gilt (Seite 8-14).

Die Leitlinien enthalten darüber neben allgemeine Bemerkungen zu Datenschutzgrundsätzen auch Ausführungen zum Zusammenwirken von Art. 6 Abs. 1 lit. b DS-GVO mit anderen Rechtsgrundlagen.
Zunächst ist darauf hinzuweisen, dass der Begriff des für die Ausführung eines Vertrags Erforderlichen nicht nur eine Bewertung dessen darstellt, was in den Vertragsbedingungen zulässig oder niedergeschrieben ist. Der Begriff der „Erforderlichkeit“ hat im Recht der Europäischen Union eine eigenständige Bedeutung , welche die Ziele des Datenschutzgesetzes widerspiegeln muss. Hierzu gibt die Leitlinie Aufschluss.
Die Leitlinien befassen sich auch mit der Beendigung des Vertrags und dem damit einhergehenden Wegfall der Rechtsgrundlage (Art. 6 Abs. 1 lit. b DS-GVO). Gerade im Falle der Bündelung getrennter Dienstleistungen ist das Vertragsende von besonderer Bedeutung.

Evaluation der DS-GVO kommt in Fahrt

Gemäß Art. 97 Abs. 2 DS-GVO muss die Evaluation der DS-GVO bis zum 25. Mai 2020 vorgenommen werden. Zur Vorbereitung eines Standpunkts des Rates haben zahlreiche Mitgliedstaaten vorab Kommentare abgegeben. Die Bundesregierung vertritt hierbei die Position, dass die Bewertung der DS-GVO ganzheitlich erfolgen sollte. Der Fokus auf die Kapitel V und VII entbinde nicht von einer Überprüfung des übrigen Regelungswerkes. Während des Prozesses einer solchen Evaluation müsste so insbesondere die Erfahrung von Praktikern und Interessengruppen berücksichtigt werden, ebenso sollte von der Möglichkeit aus Art. 97 Abs. 3 Gebrauch gemacht werden, Informationen der Aufsichtsbehörden einzuholen. Zudem sollte nach Auffassung der Bundesregierung berücksichtigt werden, dass der nationale legislative Umsetzungsprozess der Verordnung noch nicht komplett abgeschlossen sei.

Zentrale Frage der Rechtmäßigkeit: Art. 6 und/oder Art. 9 DS-GVO

Die Anwendung der Verarbeitungsvoraussetzungen in Art. 6 Abs. 1 und Art. 9 DS-GVO scheinen in der Praxis schwer verständlich zu sein. Noch dazu werden diese Verarbeitungstatbestände in den Mitgliedstaaten unterschiedlich interpretiert, weshalb es hier einer genaueren Anleitung bedarf. Diese Chance bietet die bevorstehende Evaluation nun. So muss die Dogmatik geklärt werden im Verhältnis von Art. 6 zu Art. 9 DS-GVO. Infrage steht zudem, wie die Weiterverarbeitung zu einem anderen Zweck für besondere Datenkategorien nach Art. 9 DS-GVO praktisch erfolgen kann und nach welchen Regeln Datenverarbeitung auf eine andere rechtliche Bestimmung gestützt werden kann nach einem Widerruf der Einwilligung.

Meldung von Verstößen gegen personenbezogene Daten

Das Problem bei der Meldung von Verstößen gegen personenbezogene Daten gem. Art. 33 Abs. 1 DS-GVO liegt in der Praxis in der Anforderung, bereits bei geringen Risiken für die Rechte und Freiheiten natürlicher Personen Aufsichtsbehörden zu benachrichtigen. Im Gegensatz dazu verlangt Art. 34 DS-GVO ein „hohes Risiko" und führt in Absatz 3 Ausnahmen auf, die sich in Art. 33 DS-GVO nicht finden. So kamen laut Medienberichten bis zum 30. April 2019 allein in Deutschland 22.756 Meldungen bei Aufsichtsbehörden bzgl. Art. 33 DS-GVO zusammen, während sich diese in der EU auf insgesamt 89.000 beliefen. Dies indiziert, dass die Erheblichkeitsschwelle in Art. 33 DS-GVO vom Verordnungsgeber zu niedrig angesetzt ist.

Bußgelder

Aufgrund der höheren Grenzen für Bußgelder wäre die Definition von einheitlichen transparenten Kriterien für die Aufsichtsbehörden wünschenswert, um so eine Vergleichbarkeit und eine einheitliche Durchsetzung zu gewährleisten.

Neues DataAgenda-Arbeitspapier: Welche Folgen hat der Brexit für den Datenschutz?

Unabhängig davon, wann der Brexit nun tatsächlich kommt – der Brexit macht das Vereinigte Königreich (UK) zum „unsicheren Drittstaat" in datenschutzrechtlicher Hinsicht. Wie die Datenverarbeitung nach dem Brexit aussehen kann, zeigt ein neues DataAgenda-Arbeitspapier auf.

Das neue Arbeitspapier zeigt den Umgang und die Anforderungen mit verschiedenen Austrittsszenarien auf. Dazu befasst es sich mit dem Datenschutzniveau im Vereinigten Königreich ohne Angemessenheitsbeschluss der EU-Kommission und stellt hilfreiche Übermittlungstatbestände vor, welche die Praxis zur Fortführung von Datenübermittlungen nach UK gut gebrauchen kann.

Erstellung von Bildaufnahmen

Frage des GDD-Erfa-Kreises Würzburg zur Erstellung von Bildaufnahmen:
Bei der Erstellung und Veröffentlichung von Foto- und Filmaufnahmen von Mitarbeitern und externen Personen entstehen zum einen Arbeitsdaten (Bild- oder Videodatei) und zum anderen Arbeitsergebnisse (z.B. Beitrag im Intranet des Unternehmens, Veröffentlichung in sozialen Netzwerken). Rechtsgrundlage der Datenverarbeitungen für die Erstellung und Veröffentlichung der Fotos zu den genannten Zwecken ist aktuell die Einwilligungserklärung nach Art. 6 Abs. 1 a) DS-GVO bzw. § 22 KUG.

- Es stellen sich folgende Fragen (jeweils für Mitarbeiter und externe Personen):
- Dürfen die Arbeitsergebnisse und Arbeitsdaten auf Grundlage von Art. 6 Abs. 1 f) DSGVO archiviert werden (Zweck: Nachhalten der Unternehmenshistorie, Abgleich neuer und alter Beiträge im Intranet und Internet)?
- Oder sollte die Einwilligung auch für die Archivierung der Arbeitsdaten und Arbeitsergebnisse als Rechtsgrundlage herangezogen werden, sodass die Archivierung noch als Zweck mit aufgenommen werden müsste? Hierbei wäre jedoch zu berücksichtigen, dass die Einwilligungserklärung frei widerruflich ist.

Antwort BayLDA:
Ja, für den Zweck „Archivierung“ kann die Speicherung der Bildaufnahmen auf Art. 6 Abs. 1 f) DS-GVO gestützt werden.

Frage des GDD-Erfa-Kreises Würzburg:
Bestandteil einer Einwilligungserklärung ist auch die zivilrechtliche Abtretungserklärung der Nutzungsrechte für Foto- und Filmaufnahmen. Diese erfolgt derzeit noch zeitlich unbeschränkt. Dies steht jedoch im Widerspruch zu Art. 5 Abs. 1 f) DS-GVO. Hiernach dürfen Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Wie könnte dieser Widerspruch gelöst werden? Ändert sich etwas, wenn als Rechtsgrundlage nicht die Einwilligung, sondern ein Vertrag herangezogen wird (z.B. Modelvertrag)?

Antwort BayLDA:
Ja, bei einem Vertrag gibt es kein allgemeines datenschutzrechtliches Widerrufsrecht. Die Parteien können vereinbaren, unter welchen Umständen eine weitere Veröffentlichung z.B. nach Kündigung des Arbeitsverhältnisses zulässig ist.

Setzen von Cookies erfordert die aktive Einwilligung

Mit Urteil vom 01.10.2019 hat der EuGH entschieden, dass die für die Speicherung und den Abruf von Cookies auf dem Gerät des Besuchers einer Website erforderliche Einwilligung nicht wirksam durch ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, erteilt werden kann.
Es mache insoweit keinen Unterschied, ob es sich bei den im Gerät des Nutzers gespeicherten oder abgerufenen Informationen um personenbezogene Daten handele oder nicht. Das Unionsrecht solle den Nutzer nämlich vor jedem Eingriff in seine Privatsphäre schützen, insbesondere gegen die Gefahr, dass „Hidden Identifiers“ oder ähnliche Instrumente in sein Gerät eindringen.
Der EuGH stellt klar, dass die Einwilligung für den konkreten Fall erteilt werden muss. Die Betätigung der Schaltfläche für die Teilnahme am Gewinnspiel stelle deshalb noch keine wirksame Einwilligung des Nutzers in die Speicherung von Cookies dar. Der Gerichtshof stellte ferner klar, dass der Diensteanbieter gegenüber dem Nutzer hinsichtlich der Cookies u. a. Angaben zur Funktionsdauer und zur Zugriffsmöglichkeit Dritter machen muss.

Der Bundesgerichtshof (Deutschland) ersuchte den EuGH um die Auslegung des Unionsrechts über den Schutz der Privatsphäre in der elektronischen Kommunikation.

Quelle: Europäischer Gerichtshof

Einheitliche Schutz-Standards für Whistleblower

Die EU-Kommission hat einen weiteren Schritt im Hinblick auf den Schutz von Hinweisgebern, den sog. Whistleblowern getan.

Neue EU-Regeln sollen Whistleblowern, künftig EU-weit einheitliche Standards für ihren Schutz garantieren. Die jüngst von den Mitgliedstaaten beschlossenen Vorschriften verpflichten öffentliche und private Organisationen als auch Behörden dazu, sichere Kanäle für die Meldung von Missständen einzurichten, so dass Hinweisgeber Verstöße gegen das EU-Recht möglichst gefahrlos melden können. Die Mitgliedstaaten haben zwei Jahre Zeit, um die Vorschriften in nationales Recht umzusetzen.

Die neuen Regeln decken ein breites Spektrum an EU-Rechtsbereichen ab, unter anderem die die öffentliche Auftragsvergabe, Finanzdienstleistungen, Geldwäsche, Produkt- und Verkehrssicherheit, nukleare Sicherheit, die öffentliche Gesundheit sowie den Verbraucher- und Datenschutz.
Die neuen Vorschriften umfassen im Wesentlichen folgende Punkte:

- Einrichtung von Meldekanälen innerhalb von Unternehmen und Verwaltungen
- Hierarchie der Meldekanäle
- Zahlreiche Profile, die durch die neuen Vorschriften geschützt werden
- Ein breiter Anwendungsbereich
- Unterstützung und Schutzvorkehrungen für Hinweisgeber
- Rückmeldepflichten für Behörden und Unternehmen

Eine FAQ-Sammlung zum Schutz von Hinweisgebern pflegt die Kommission unter folgender URL:
https://europa.eu/rapid/press-release_MEMO-18-3442_de.htm

Quelle: Europäische Kommission

Hinweise zum Einsatz von Facebook-Fanpages durch Unternehmen

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) berichtet, dass die jüngsten Gerichtsentscheidungen sowie das Positionspapier der Datenschutzkonferenz vom 01.04.2019 zu den Facebook-Fanpages bei den betroffenen Wirtschaftsunternehmen zu einer erheblichen Verunsicherung geführt haben.
Mehrfach sei an die GDD die Frage herangetragen worden, ob unternehmenseigene Facebook-Fanpages noch weiterbetrieben werden können oder diese sofort abzuschalten sind.

Die GDD nimmt daher auf ihrer Internetseite wie folgt Stellung:
Den Ausgangspunkt der aktuellen Verunsicherung bildet eine EuGH-Entscheidung aus dem Jahr 2018 zu den Facebook-Fanpages (Urteil vom 05.06.2018 – C-210/16). In dieser Entscheidung hat der EuGH den Betreiber einer Facebook-Fanpage als mitverantwortlich für die Datenverarbeitung im Zusammenhang mit der Fanpage angesehen, obgleich dieser selbst keinerlei Zugriff auf die Datenverarbeitung hatte und die Ergebnisse der Verarbeitung nur in anonymisierter Form in Form von Besucherstatistiken erhielt. Der Fanpage-Betreiber konnte im Rahmen der Einrichtung der Fanpage lediglich beeinflussen, nach welchen Parametern die Statistiken erstellt werden, z.B. Alter, Geschlecht und geografische Daten (Facebook Insight). Facebook hat auf diese EuGH-Entscheidung reagiert, indem es seine Nutzungsbedingungen um eine Vereinbarung im Sinne von Art. 26 DS-GVO („Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“) ergänzt hat.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) vertritt allerdings die nicht im Detail begründete Auffassung, dass die von Facebook vorgelegte Vereinbarung den Vorgaben der DS-GVO nicht genügt. Die Aufsichtsbehörden weisen darüber hinaus auf die Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) der Fanpage-Betreiber hin. Ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, seien Verantwortliche nicht in der Lage, zu bewerten, ob diese Verarbeitungstätigkeiten rechtskonform durchgeführt werden. Bestünden Zweifel, gehe dies zulasten der Verantwortlichen, die es in der Hand hätten, solche Verarbeitungen zu unterlassen, so die Datenschutzkonferenz. Nach dieser Ansicht können Facebook-Fanpages derzeit nicht rechtskonform betrieben werden.
Die jüngste Entscheidung in Sachen Facebook-Fanpages erging am 11.09.2019 durch das Bundesverwaltungsgericht (BVerwG 6 C 15.18). Danach muss die Datenschutzaufsicht, wenn sie die bei Aufruf der Fanpage ablaufende personenbezogene Datenverarbeitung als rechtswidrig erachtet, nicht vorrangig gegen Facebook selbst vorgehen, sondern darf aus Effektivitätserwägungen das die Fanpage betreibende Unternehmen zur Deaktivierung der Fanpage verpflichten.

Mehr auf DataAgenda

Anwendungspraxis der DS-GVO

Der Beginn der Anwendungspflicht der DS-GVO führte in Deutschland einerseits zu einer erhöhten Sensibilisierung bzgl. Datenschutz, andererseits zu einer wahrnehmbaren Überforderung einiger Unternehmen und Behörden. Und das obwohl dem 25. Mai 2018 ein zweijähriger Umsetzungszeitraum voranging und einige der für Verwirrung sorgenden Instrumente wie z.B. Datenschutzbeauftragte oder Aufzeichnungen der Verarbeitungstätigkeiten bereits Teil des existierenden BDSG waren. Deutschland unterstützt den Ansatz der Kommission einer einheitlichen Anwendung der DS-GVO durch eine enge Koordination und Zusammenarbeit der Aufsichtsbehörden. Dies gilt insbesondere u.a. für die Berücksichtigung der besonderen Anliegen von Kindern im Rahmen des Art. 6 Abs. 1 lit. f, die Frage, wie freiwillig eine Einwilligung sein kann, wenn eine gesonderte Einwilligung für verschiedene Operationen zur Verarbeitung persönlicher Daten nicht möglich ist oder die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit nicht in angemessener Weise vorhanden sind.

Aufsichtsbehörden legen Konzeptpapier für Bußgeldzumessung vor

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat ihr angekündigtes Konzept zur Zumessung von Geldbußen bei Verstößen gegen die DS-GVO durch Unternehmen vorgelegt. Das Konzept gestaltet im Wesentlichen die Vorgaben des Art. 83 der Datenschutz-Grundverordnung aus und ist auf Fortentwicklung angelegt. Ziel des Konzepts sei es, den Datenschutzaufsichtsbehörden eine einheitliche Methode für eine systematische, transparente und nachvollziehbare Bemessung von Geldbußen zur Verfügung zu stellen.
Mit der Veröffentlichung der vorliegenden Fassung des Konzeptes zur Bemessung von Geldbußen soll ein Beitrag zur Transparenz im Hinblick auf die Durchsetzung des Datenschutzrechts geleistet werden, so die DSK in ihrem Konzeptpapier. Es soll Verantwortliche und Auftragsverarbeiter in die Lage versetzen, die Entscheidungen der Aufsichtsbehörden nachzuvollziehen.
Die Aufsichtsbehörden weisen in ihrem Papier darauf hin, dass die vorgestellten Leitlinien nicht als erschöpfend zu verstehen sind und die Konkretisierung der Festsetzungsmethodik späteren Leitlinien des EDSA (Europäischer Datenschutzausschuss) vorbehalten bleibe.

Quelle: Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)