Datenschutz
newsbox

Ausgabe
3
2019

DATAKONTEXT

Editorial

Spannend zu beobachten ist, wie gleichlautende Fragestellungen unter den deutschen Datenschutz-Aufsichtsbehörden, aber auch vom Datenschutz-Fachpublikum unterschiedlich bewertet werden.

Im Streit darüber, ob im Falle der reinen Lohn- und Gehaltsabrechnung oder bei sonstigen, rein technischen Dienstleistungen auch bei Steuerberatern von einer Auftragsverarbeitung auszugehen ist, hat sich eine weitere Aufsichtsbehörde „zu Wort gemeldet". Bislang hatten sich das LDI NRW (http://t1p.de/ewvo) und das BayLDA (http://t1p.de/82g6) mit gegensätzlichen Bewertungen zum Thema geäußert (vgl. Editorial Datenschutz Newsbox 11/2018, https://t1p.de/gx6a) .

Gefühlt kippt die Meinung zu Gunsten derer, die dafür plädieren, dass es sich dabei um eine Auftragsverarbeitung handelt. Neu im Ring ist die Aufsichtsbehörde Baden-Württemberg, die sich bereits in ihrem aktuellen Tätigkeitsbericht (Ziffer 1.10) damit beschäftigt hat und ebenfalls zu dem Schluss kommt, dass Auftragsverarbeitung anzunehmen ist. Diese Ansicht wird mit weiteren Entscheidungen u.a. des BverfG und Argumenten in der neuesten Auskopplung des Themas intensiviert und weiter untermauert.

Am Ende ist die Verunsicherung beim Rechtsanwender natürlich nicht unbedingt kleiner, nur weil eine weitere Aufsichtsbehörde nun die eine oder andere Meinung propagiert. Die Aussage, dass die Debatte auch (intern) unter den Aufsichtsbehörden läuft, lässt jedoch vermuten, dass in naher Zukunft eine einheitliche Wertung die erhoffte Rechtssicherheit bringen wird, 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

Beauskunftung gem. Art. 15 DS-GVO nur vor Ort?

Eine betroffene Person sollte gem. Art. 15 DS-GVO ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.
Wie soll sich ein Verantwortlicher (Klinikkonzern) verhalten, wenn ein Betroffener Auskünfte erhalten möchte, die naturgemäß auch Gesundheitsdaten beeinhalten (können)?
Ein in Südniedersachsen wohnhafte Betroffene hatte von der Muttergesellschaft eines Klinikkonzerns mit Sitz in Hamburg per E-Mail eine schriftliche und kostenfreie Auskunft über die zu seiner Person gespeicherten Daten gemäß Art. 15 DS-GVO und Zusendung der Auskunft in Form einer vollständigen Kopie der personenbezogenen Daten angefordert. Die Verantwortliche teilte der Betroffenen mit, eine Kopie der vorhandenen Daten könne der Betroffene nur gegen Vorlage seines Personalausweises bei der verantwortlichen Stelle in Hamburg erhalten, da es sich bei den Daten um besonders geschützte Gesundheitsdaten handele, die weder elektronisch noch per Post übermittelt werden dürften. Damit wollte die Verantwortliche ausschließen, dass eine Lücke bei der Übermittlung der Daten oder der Identitätsfeststellung gegen den Konzern verwendet werden könne. Der Postversand möge sicher sein, aber wenn die Gesundheitsdaten auf dem Postwege abhanden kämen, läge eine Datenpanne vor.
Als weiteres Argument gegen die von der Betroffenen begehrten Weg der Beauskunftung führte die Verantwortliche an, dass beim Postversand das Problem der Identitätsfeststellung bestünde. Wer tatsächlicher Absender der bei ihr eingegangenen E-Mail mit dem Antrag auf Auskunft nach Art. 15 DS-GVO sei, könne nicht zweifelsfrei festgestellt werden.
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI), dem die Angelegenheit zur Prüfung vorlag (27. Tätigkeitsbericht, Seite 95), befand, dass ein elektronisch gestellter Antrag auf Zusendung einer Datenkopie im Sinne von Art. 15 Abs. 3 Satz 1 DS-GVO nicht dadurch erfüllt wird, dass dem Betroffenen die persönliche Aushändigung einer Datenkopie gegen Vorlage des Personalausweises beim mehrere Stunden entfernten Verantwortlichen angeboten wird. Der HmbBfDI wies die Verantwortliche u.a. darauf hin, dass gem. Art. 12 Abs. 1 DS-GVO Auskünfte in „leicht zugänglicher Form“ erteilt werden sollen; Art. 15 Abs. 3 Satz 3 DS-GVO besage, dass bei einem elektronisch gestellten Antrag die begehrten Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen sind.
Auch nach ErwG 63 DS-GVO soll der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.

Quelle: HmbBfDI – 27. Tätigkeitsbericht Datenschutz für das Berichtsjahr 2018

BSI aktualisiert Kompendium zum IT-Grundschutz

Das IT-Grundschutz-Kompendium ist neben den BSI-Standards die grundlegende Veröffentlichung des IT-Grundschutzes. Die Bausteine sind in zehn Schichten aufgeteilt und beschäftigen sich mit unterschiedlichsten Themen der Informationssicherheit.
Seit dem 1. Februar 2018 dient das IT-Grundschutz-Kompendium als Prüfgrundlage für Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das IT-Grundschutz-Kompendium aktualisiert und stellt es in der neuen Edition 2019 zur Verfügung. In dieser Edition sind insgesamt 94 IT-Grundschutz-Bausteine enthalten, 14 Bausteine sind zu neuen Themen aufgenommen worden. Das IT-Grundschutz-Kompendium ist auf die Sicherheitsanforderungen in Unternehmen und Behörden zugeschnitten.
Die neue Edition steht online auf der BSI-Webseite und als Loseblattwerk zur Verfügung. Die nun veröffentlichte Edition 2019 ist zertifizierungsrelevant und löst damit die Edition 2018 ab. Diese ist für aktuelle Zertifizierungsprozesse noch bis zum 30. September 2019 gültig.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik (BSI)*

Erstellung von Bildaufnahmen

Frage des GDD-Erfa-Kreises Würzburg:
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) DS-GVO 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 Fotoaufnahmen 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. Modellvertrag)?

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.

DSK veröffentlicht Kurzpapier zur Einwilligung nach der DS-GVO

Die Europäische Datenschutzgrundverordnung (DS-GVO) führt den bisher geltenden Grundsatz des Verbots mit Erlaubnisvorbehalt fort. Datenverarbeitungen sind demnach generell verboten, es sei denn es liegt ein gesetzlicher Erlaubnistatbestand oder eine Einwilligung der betroffenen Person vor.
Eine Einwilligung ist nach Art. 4 Nr. 11 DS-GVO „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.
Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung.
Mit dem Thema Einwilligung nach der DS-GVO hatte sich von Seiten der Aufsichtsbehörden erstmals das BayLDA mit einem Kurzpapier beschäftigt. Der Bayerische Landesbeauftragte für den Datenschutz veröffentlichte ebenfalls ein eigenes Papier, in dem auch ausgewählte Fragen zur Einwilligung aufgearbeitet wurden. Praxishinweise rundeten das Papier ab. Nun hat auch die Datenschutzkonferenz, d.h. die unabhängigen Datenschutzbehörden des Bundes und der Länder ein Kurzpapier veröffentlicht, welches sich mit der Einwilligung beschäftigt. Darin werden bspw. sowohl die Voraussetzungen und Unterschiede zu dem bis zum 24. Mai 2018 geltenden Recht behandelt, als auch die Problematik der Fortgeltung von Einwilligungen.

DSK äußert sich zum Brexit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hatte bereits Mitte Januar 2019 auf seiner Internetseite eine zusammengefasst, welche Bestimmungen verantwortliche Stellen in der EU, und damit auch in Rheinland-Pfalz im Falle eines Brexit berücksichtigen müssen.
Nun hat sich auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu diesem Thema geäußert. In der gemeinsamen Stellungnahme weisen die Aufsichtsbehörden Unternehmen, Behörden und andere Institutionen in Deutschland auf die Rechtslage bei einem Austritt („Brexit“) des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union (EU) hin. Dabei werden zwei Szenarien sowohl eines geregelten als auch eines ungeregelten Austritts durchgespielt.
Abschließend weist die DSK darauf hin, dass Verantwortliche, die personenbezogene Daten ohne die nach Kapitel V DS-GVO notwendigen Sicherheiten in das Vereinige Königreich übermitteln, rechtswidrig handeln. Die Aufsichtsbehörden könnten dann Datenübermittlungen per Anordnung aussetzen (Art. 58 Abs. 2 lit. j DS-GVO) und Geldbußen verhängen (Art. 83 Abs. 5 lit. c DS-GVO).

Quelle: DSK

BayLfD bietet Orientierungshilfe zur DSFA mit CNIL-PIA-Tool

Die Commission Nationale de l'Informatique et des Libertés (CNIL; deutsch Nationale Kommission für Informatik und Freiheiten, die nationale Datenschutzbehörde Frankreichs mit Sitz in Paris, hat bereits Ende 2017 eine Software für die Durchführung einer sog. Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO veröffentlicht.
Die sog. PIA-Software (Privacy Impact Assessment) ist Teil eines Prozesses zur Unterstützung der für die Verarbeitung Verantwortlichen bei der Umsetzung der Pflichten aus der DS-GVO. Das Tool ist in französischer, englischer und auch deutscher Sprache verfügbar und soll die Datenschutz-Folgenabschätzung erleichtern und die Verantwortlichen bei der Durchführung einer Datenschutz-Folgenabschätzung begleiten, die seit Mai 2018 für einige Verarbeitungen obligatorisch ist. Dieses Instrument zielt auch darauf ab, die von der CNIL veröffentlichten Leitfäden zum Thema Datenschutz-Folgenabschätzung zu erleichtern.
Das Tool richtet sich vor allem an Verantwortliche, die mit dem PIA-Ansatz nicht vertraut sind. Es handelt sich um eine „ready to use"-Version, die einfach auf einem Rechner gestartet werden kann. Das Tool wird auch in einer sog. portable-Version angeboten, die keiner Installation bedarf. Es ist auch möglich, das Tool auf Servern einzusetzen, um es in bereits intern im Unternehmen eingesetzte Tools zu integrieren.
Verantwortliche können den Inhalt des Tools an Ihre spezifischen Bedürfnisse oder Ihren Tätigkeitsbereich anpassen, indem Sie beispielsweise ein DSFA-Modell erstellen, welches dupliziert und für ähnliche Behandlungen verwendet werden kann. Außerdem gestattet es die Lizenz den Quellcode des Tools zu modifizieren, um Funktionalitäten hinzuzufügen oder es in bereits intern veröffentlichte Tools zu integrieren.
Die Software kann frei verwendet und weiterentwickelt werden (GPL v3.0) und ist für Windows, Linux und für Mac OS als eigenständiges Programm sowie auch als Web-Anwendung verfügbar. Sie kann auch auf der Homepage des Bayerischen Landesbeauftragten für den Datenschutz in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz Folgenabschätzung" in einer von der Aufsichtsbehörde geprüften deutschen Version heruntergeladen werden. Auf der Webseite der CNIL finden sich darüber hinaus Informationen zum PIA-Tool und zur Durchführung einer DSFA in französischer und englischer Sprache.

Quelle: *BayLfD*

Datenschutzkonforme Nutzung von Bodycams durch private Sicherheitsunternehmen

Als Bodycams werden kleine an der Uniform getragene Videokameras bezeichnet. Der Begriff grenzt die verschiedenen Nutzerkreise, Uniformträger und Privatpersonen voneinander ab. Privat genutzte Kameras, die am Körper oder der Ausrüstung getragen werden, bezeichnen die Begriffe „Action Cam“ oder „Action Camcorder“.
Unter anderem in Baden-Württemberg, Bayern, Berlin, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, im Saarland und bei der Bundespolizei testeten Polizisten in mehreren Pilotstudien die kleinen Kameras.
Dass der Einsatz von Bodycams durch private Sicherheitsdienste nicht durch entsprechende Polizeigesetze legitimiert werden kann, versteht sich von selbst. Ob ein datenschutzgerechter Einsatz der Bodycam durch private Sicherheitsdienste ggf. gem. Art. 6 Abs. 1 Buchst. f Datenschutzgrundverordnung (DS-GVO), § 4 Bundesdatenschutzgesetz (BDSG) erlaubt sein kann, ist eine der Fragen, mit dem sich die Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen beschäftigt.
Da auch immer mehr private Sicherheitsunternehmen ihre Beschäftigten mittlerweile mit Bodycams ausrüsten, dürfte die Orientierungshilfe eine geeignete Möglichkeit sein, etwas mehr Rechtssicherheit in dieser Frage zu erlangen. Als Gründe führen die Sicherheitsdienste den Schutz der Beschäftigten vor Übergriffen, Beschaffung von Beweismitteln für zivilrechtliche Ansprüche oder eine abschreckende bzw. deeskalierende Wirkung an.

Quelle: LDI NRW

BSI erfragt Lagebild der IT-Sicherheit in Deutschland

Um das Lagebild zur IT-Sicherheit in Deutschland weiter zu verbessern, führt das Bundesamt für Sicherheit in der Informationstechnik (BSI) seine jährliche Cyber-Sicherheitsumfrage durch.
Wie viele Unternehmen waren im Jahr 2018 von Angriffen mit Erpresser-Software betroffen? Welche Schutzmaßnahmen wirkten bei den meisten Institutionen gegen Malware-Angriffe? Welche Schäden verursachten DDoS-Angriffe, beispielsweise auf Webangebote wie Online-Shops? Diese und viele weitere Fragen sollen mit den Ergebnissen dieser Umfrage beantwortet werden.
Unternehmen, Organisationen und Institutionen jeder Größe und aus allen Branchen sind aufgerufen, sich ab sofort daran zu beteiligen. Die Ergebnisse der Umfrage fließen in das Lagebild des BSI ein, auf dessen Grundlage die nationale Cyber-Sicherheitsbehörde aktuelle Bedrohungsszenarien und Trends erkennen und einschätzen sowie seine IT-Sicherheitsempfehlungen für Anwender in Staat, Wirtschaft und Gesellschaft weiter konkretisieren und anpassen kann. Ziel ist es unter anderem, ein dauerhaft hohes Cyber-Sicherheitsniveau in Deutschland zu gewährleisten.
Die Teilnahme an der Umfrage ist ab sofort und bis zum 4. März 2019 online möglich. Hintergrundinformationen zu Datenschutz, Berichtszeitraum und Nutzung der Ergebnisse sind in einer FAQ-Liste abrufbar.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Zulässigkeit der Kopplung in der DS-GVO

Frage des GDD-Erfa-Kreises Würzburg:

1.Kopplung mit Nutzerprofilen:

Wäre es zulässig, mit der Erteilung der Einwilligung zugleich die Einwilligung in die Erstellungvon Nutzerprofilen einzuholen? Der Sinn soll darin bestehen, dem Kunden einen individualisierten Newsletter anbieten zu können, sodass der Prozess als eine erteilte Einwilligung (undnicht als Kopplung) anzusehen wäre.

In dem 33. Tätigkeitsbericht des LFDI BW (33. Tätigkeitsbericht 2016/2017, S. 120) wird die Kopplung von Newslettern mit Nutzungsprofilen mit dem Hinweis thematisiert, dass es beider Kopplung an der Freiwilligkeit fehlen würde. In dem von der Aufsichtsbehörde beschriebenen Fall wurden in mehreren Schritten Daten der Nutzer abgefragt. Würde eine andereBewertung erfolgen, wenn lediglich die für eine Personalisierung erforderlichen Angaben abgefragt werden und der Betroffene transparent in den DS-Hinweisen über den Prozess informiert wird?

Antwort BayLDA:

Wir halten es für vertretbar, mit der Erteilung der Einwilligung für eine Newsletter-Zusendung zugleich eine Einwilligung in die Erstellung von Nutzerprofilen einzuholen. Dabei muss derNutzer natürlich transparent über alle Zwecke der vorgesehenen Verarbeitung seiner Daten aufgrund seiner Einwilligung informiert werden, Art. 13 Abs. 1 c) DS-GVO, Art. 4 Nr. 11 DS-GVO.

Frage des GDD-Erfa-Kreises Würzburg:

2. Kopplung mit Gewinnspielen:

In dem aktuellen Tätigkeitsbericht des LFDI BW wurde ebenfalls die Kopplung mit einem Gewinnspiel thematisiert (33. Tätigkeitsbericht 2016/2017, S. 124 f.). Hiernach mangelt es ebenfalls an der Freiwilligkeit, wenn eine Einwilligung erteilt werden muss, um eine Leistung zu erhalten. Kommt die Aufsichtsbehörde zu einem anderen Ergebnis, wenn der im Rahmen des Gewinnspiels zu erfüllende Vertrag als eine Art „Austauschvertrag" qualifiziert wird. Die Leistung wäre in diesem Zusammenhang die Möglichkeit, an einem Gewinnspiel teilzunehmen.

Die Gegenleistung des Kunden wäre in dem Einverständnis zum Erhalt des Newsletters zu sehen. Der Austausch der Leistungen (insbesondere die Einbindung der Gegenleistung desNutzers) würde hinreichend transparent dargestellt werden

Antwort BayLDA:

Wir sehen es als möglich an, im Rahmen der allgemeinen Vertragsfreiheit einen „Austauschvertrag" über die Teilnahme an einem Gewinnspiel anzubieten, bei dem der Teilnehmer im Gegenzug zu einer Verwendung seiner Kontaktdaten, z. B. E-Mail-Adresse, für werbliche Zusendungen zustimmt. Der Vertragsinhalt mit Leistung und Gegenleistung muss natürlich klar und verständlich dargelegt werden, Art. 13 Abs. 1 c) DS-GVO; ebenso muss ein Hinweis auf das Werbewiderspruchsrecht nach Art. 21 Abs. 4 und Art. 13 Abs. 2 b) DS-GVO erfolgen. Siehe dazu auch das DSK-Kurzpapier Nr. 3, dort Seite 2, rechte Spalte unten, mit folgenden Ausführungen: *„Bei „kostenlosen" Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen" (z. B. kostenloser E-Mail-Account gegen Zustimmung für Newsletter-Zusendung als „Gegenfinanzierung"), muss diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar und verständlich dargestellt werden. Nur dann besteht keine Notwendigkeit mehr für eine Einwilligung."*