Datenschutz
newsbox

Ausgabe
11
2020

Editorial: 2

LDI NRW veröffentlicht Update zu Corona-FAQ Beschäftigtendatenschutz 3

Rechtliche Zulässigkeit einer "Bonushopper-Datenbank" 4

ENISA veröffentlicht Leitlinien zur Cybersicherheit des Internets der Dinge 4

Infos und Prüfschema des BfDI zu Schrems II 5

GDD Winter-Workshop (Anzeige) 5

Deutsche Ratspräsidentschaft legt neuen Entwurf zur ePrivacy-Verordnung vor und scheitert 6

Microsoft Office 365 und Datenschutz-Folgenabschätzung 7

Löschen nach DS-GVO in der Praxis (Anzeige) 7

DSK veröffentlicht Orientierungshilfe Videokonferenzsysteme 8

Datenschutz-Gutachten: Tesla in der Kritik 8

Interessenkollision bei Personalunion: DSB und IT-Sicherheitsbeauftragter 9

Die Überwachungsaufgabe des Datenschutzbeauftragten nach DS-GVO (Anzeige) 9

Corona: Datenschutz bei Befreiung von der Maskenpflicht 10

IT-Sicherheitslage in Deutschland weiter angespannt 10

DS-GVO-Bußgeld des BfDI hält Urteil des LG Bonn nicht stand 11

DATAKONTEXT

Editorial:

Es gehört ja zum menschlichen Wesen, dass man in der größten Verzweiflung nach jedem Grashalm greift. Die Ankündigung des Europäischen Datenschutzausschusses (EDSA) weiterführende Empfehlungen veröffentlichen zu wollen, wie Datenexporteure personenbezogene Daten auch künftig, will heißen, nach dem Schrems II-Urteil, außerhalb des EWR (Drittstaaten) übermitteln wollen, vorgehen sollen, dürfte sich in den Ohren der meisten leidgeplagten Verantwortlichen (oder um im Bilde zu bleiben: Ertrinkenden) mehr als die vage Hoffnung auf einen Grashalm angehört haben.

Viele Interessierte ließen die lang erwarteten Empfehlungen enttäuscht oder zumindest ratlos zurück. Die Empfehlungen brachten eher interessante Hinweise als belastbare Lösungen. Statt des erwarteten Brots, gab es eher Steine, wie zutreffend festgestellt wurde.

Andere ließen sich jedoch von auf dem 38 Seiten dargestellten Maßnahmenplan nicht abschrecken und versuchten dies für Verantwortliche und Nutzer erfahrbar und visualisierbar zu machen. Dabei wurde das Prüfschema des BfDI um Längen übertroffen. Andere blieben weiter optimistisch und verwiesen darauf, dass es zumindest an anderen Stellen Lichtblicke bei diesem eher düsteren Thema gibt (Entwurfsfassung neuer Standarddatenschutzklauseln).

Wie man es auch dreht und wendet. Die Auswirkungen des Schrems II-Urteils werden sich mit "guten Empfehlungen" nicht so ohne weiteres in Luft auflösen und sorgen dafür, dass sich Datenschutzverantwortliche eingehend und gewissenhaft mit der Problematik befassen müssen.

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

LDI NRW veröffentlicht Update zu Corona-FAQ Beschäftigtendatenschutz

Die LDI NRW informiert auf ihrer Homepage über Fragen und Maßnahmen des Arbeitgebers zum Schutz vor Corona-Infektionen.

Vor dem Hintergrund, dass diese Informationen über die Gesundheit eines Beschäftigten oder Bewerbers gemäß Art. 9 Abs. 1 DS-GVO, § 26 Abs. 3 BDSG, §§ 1, 7, 8 Allgemeines Gleichbehandlungsgesetz (AGG) sowie § 75 Abs. 1 Betriebsverfassungsgesetz einem besonderen Schutz unterliegen und sich im Laufe der anhaltenden Pandemie immer neue Fragestellungen in diesem Zusammenhang ergeben, werden die FAQ weiter gepflegt und aktualisiert.

Bereits zu Beginn der Corona-Pandemie wurde die Frage diskutiert, welche Maßnahmen Arbeitgeber zur Eindämmung der Pandemie und unmittelbar auch zur Aufrechterhaltung der betrieblichen Tätigkeit umsetzen können. In diesem Zusammenhang stellte sich auch oftmals die Frage, ob Arbeitgeber im Rahmen von Zugangskontrollen Fiebermessungen an ihren Beschäftigten vornehmen dürfen.
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit aus Rheinland-Pfalz äußerte sich kritisch zu dieser Fragestellung und kam im Ergebnis zu der Feststellung, dass eine verpflichtende Fiebermessung der Mitarbeiter als Zugangskontrolle unzulässig sei. Nach Auffassung der Aufsichtsbehörde fehle es insbesondere an der notwendigen Erforderlichkeit der Fiebermessung.
Nach Art. 9 Abs. 2 lit. b DS-GVO i.V.m. § 26 Abs. 3 BDSG sei die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses unter anderem zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich sei und kein Grund zu der Annahme bestehe, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.
Die Aufsichtsbehörde ging davon aus, dass die reine Tatsache, dass eine erhöhte Körpertemperatur zu verzeichnen ist, noch nicht automatisch den Schluss auf das Vorliegen einer Corona-Erkrankung zulasse. Umgekehrt müsse sich eine bereits bestehende Corona-Erkrankung, nicht zwangsläufig durch eine erhöhte Körpertemperatur zu erkennen geben. Daher zweifelte die Aufsichtsbehörde sogar bereits an der Geeignetheit der Körpertemperaturmessung.

Auch in dem Papier "Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie" des DSK wird diese Möglichkeit der Pandemiebekämpfung kritisch gesehen. Insoweit heißt es dort: "Im Ergebnis kann daher eine Erforderlichkeit der elektronischen Fiebermessung als Instrument der Zutrittsregulierung zu öffentlichen Verkaufs- und Verkehrsflächen, insbesondere im Bereich der Grundversorgung sowie für Bereiche, deren Nutzung für das tägliche Leben unabdingbar sind (z. B. Bahnhöfe, Flughäfen, Gebäude von Verwaltungsbehörden) nicht bejaht werden."

In den FAQ der LDI NRW scheint diese Maßnahme etwas weniger kritisch betrachtet zu werden (Frage 5). Der interessierte Leser erhält dort auf die Frage "Darf der Arbeitgeber bei den Beschäftigten Fiebermessungen durchführen?" folgende Antwort:
"Kontaktlose Fiebermessungen am Eingang von Betriebsgeländen oder Gebäuden können unter engen Voraussetzungen, gemäß § 26 Abs. 3 Satz 1 BDSG, gerechtfertigt sein. Zwar gibt es derzeit keine gesicherten Erkenntnisse darüber, ob Fieber ein definitives Kriterium zur Feststellung einer Corona-Infektion sind.
Die Temperaturkontrolle kann aber ein geeignetes Mittel sein, um Hinweise auf etwaige Corona-Verdachtsfälle zu erhalten. Ob die Fiebermessung zulässig ist, hängt vom jeweiligen Einzelfall ab. Dabei spielen die konkreten Umstände eine maßgebliche Rolle, etwa, ob es bereits Fälle nachweislich Infizierter im Unternehmen gibt, das Unternehmen in einem Risikogebiet liegt, oder Beschäftigte Kontakt zu Infizierten hatten oder haben. Eine Speicherung der Daten dürfte nicht erforderlich sein, wenn die Fiebermessung lediglich dazu dient, festzustellen, ob jemand für den betreffenden Tag Einlass erhält oder nicht. Bei einer erhöhten Temperatur sollte der oder die Beschäftigte zur weiteren Abklärung der Ursache ein Krankenhaus oder einen Arzt aufsuchen. Arbeitgebern ist zu empfehlen, eine möglichst einvernehmliche Lösung unter Einbeziehung der Beschäftigten, des Betriebs- oder Personalrats sowie der oder dem Datenschutzbeauftragten herbeizuführen. Die Maßnahme kann auch auf der Basis einer freiwilligen Einwilligung der betroffenen Beschäftigten durchgeführt werden. Voraussetzung ist, dass sie über die Verarbeitung ihrer Gesundheitsdaten umfassend informiert werden. In einer Betriebsvereinbarung können die wesentlichen Regelungen hinsichtlich des "Wie" der Durchführung der Maßnahme inklusive des Umgangs mit Verdachtsfällen transparent geregelt werden."

Rechtliche Zulässigkeit einer "Bonushopper-Datenbank"

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wird bei ihrer Arbeit durch Arbeitskreise unterstützt. Die Arbeitskreise arbeiten der Datenschutzkonferenz zu und bereiten deren Entscheidungen vor.
Aktuell arbeitet der Arbeitskreis Auskunfteien an einer Thematik, die vor allem Verbraucher interessieren dürfte, die häufig ihren Energieversorger wechseln, um jederzeit den optimalen Tarif für sich zu beanspruchen.

Derzeit können Kunden bei der Wahl des Strom- und Gasanbieters durch einen regelmäßigen Preisvergleich und den Wechsel des Anbieters von günstigeren Preisen oder besonderen Angeboten für Neukunden profitieren.

Anlass dafür, dass sich nun der Arbeitskreis Auskunfteien des Themas angenommen hat, liegt in Berichten des NDR sowie der Süddeutschen Zeitung begründet, wonach zwei große deutsche Auskunfteien eine Datenbank planen, in denen Vertragsdaten von Strom- und Gaskunden branchenweit gespeichert werden sollen.

Häufig wechselnde Kunden sind für die Unternehmen jedoch weniger interessant als langfristige Kunden. Aus diesem Grund haben die Anbieter ein Interesse daran, möglichst schon vor Vertragsabschluss in Erfahrung zu bringen, wie häufig potenzielle Kunden ihren Energieanbieter wechseln.

Pläne von Wirtschaftsauskunfteien für Datenbanken über Strom- und Gasverbraucher haben Befürchtungen ausgelöst, dass Energieversorger Kunden ausbremsen könnten, die häufig ihren Vertrag kündigen, um zu einem günstigeren Anbieter zu wechseln.

"Aus Sicht des Arbeitskreises bestehen erhebliche Zweifel an der Verarbeitung von Positivdaten wie Angaben zur Vertragsdauer durch Wirtschaftsauskunfteien im Bereich der Energieversorgungsbranche auf der Grundlage des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO. Positivdaten sind Informationen, die keine negativen Zahlungserfahrungen oder anderes nicht vertragsgemäßes Verhalten zum Inhalt haben. Dieses Ergebnis des Arbeitskreises soll der Datenschutzkonferenz als Entscheidungsvorlage zugeleitet werden, so Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz."

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

ENISA veröffentlicht Leitlinien zur Cybersicherheit des Internets der Dinge

ENISA, die Agentur der Europäischen Union für Cybersicherheit, ist ein Fachzentrum für Cybersicherheit in Europa. Die Agentur unterstützt die EU und ihre Mitgliedsländer bei der Vorbeugung, Ermittlung und Bekämpfung von Problemen der Informationssicherheit.

ENISA hat eine neue Studie veröffentlicht, die den Beteiligten helfen soll, bessere Sicherheitsentscheidungen zu treffen, wenn Sie IoT-Technologien bauen, einsetzen oder bewerten.

Diese ENISA-Studie definiert Leitlinien zur Cybersicherheit der Lieferkette für das IoT (Internet of Things). Die ENISA hat unter Mitwirkung von IoT-Experten Sicherheitsleitlinien für die gesamte Lebensdauer erstellt: von den Anforderungen und dem Design über die Lieferung und Wartung bis hin zur Entsorgung. Die Studie soll IoT-Herstellern, Entwicklern und allen an der Lieferkette des IoT beteiligten Akteuren helfen, bessere Sicherheitsentscheidungen zu treffen, wenn IoT-Technologien gebaut, eingesetzt oder bewertet werden.

ENISA setzt sich seit langem dafür ein, dass "security by design and default" in digitalen Produkten standardmäßig berücksichtigt wird. Der Festlegung spezifischer Leitlinien für die Sicherheit der IoT-Lieferkette wird von den Autoren eine große Bedeutung für die Frage der Sicherheit des IoT beigemessen. IoT-Sicherheit müsse in allen Phasen der Lieferkette berücksichtigt werden, vom frühen Konzeptentwurf bis zur Lieferung an den Endverbraucher und der Wartung.

Quelle: ENISA

Infos und Prüfschema des BfDI zu Schrems II

Bereits mit Schreiben vom 08.10.2020 adressierte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ein Informationsschreiben zur Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 "Schrems II") an die öffentlichen Stellen des Bundes und Unternehmen unter der Aufsicht des BfDI.
Unter Ziffer 3. seines Informationsschreibens fasste der BfDI die Verpflichtung der Verantwortlichen zur Prüfung der Datentransfers in Drittländer wie folgt zusammen:
"Unternehmen und Behörden müssen als Reaktion auf die Vorgaben aus dem Urteil des EuGH in der Rechtssache C-311/18 "Schrems II" als Verantwortliche ihre Datentransfers in Drittländer prüfen. Je nach bisher gewählter Grundlage für die Datenübermittlung muss diese – z. B. im Falle des EU-US Datenschutzschildes – durch eine neue Grundlage ersetzt werden. Zudem müssen alle Verantwortlichen bei der Verwendung von geeigneten Garantien nach Art. 46 DSGVO prüfen, ob und ggf. welche zusätzlichen Maßnahmen ergriffen werden müssen, um die übermittelten Daten im Drittland angemessen zu schützen. Das Ergebnis dieser Prüfung und die getroffenen Maßnahmen sind nachvollziehbar zu dokumentieren."

Mittlerweile hat der BfDI die empfohlene Vorgehensweise verfeinert und in einem Prüfschema veröffentlicht. Das vorgestellte Prüfschema dürfte auch für Unternehmen interessant sein, die nicht unter der Aufsicht des BfDI stehen. Die Schritte der Prüfung des Drittlandtransfers strukturiert der BfDI folgendermaßen:

1. Datentransfers prüfen
2. Vorliegen Angemessenheitsbeschluss
3. Schutzniveau im Drittland: Einzelfallanalyse
4. Prüfung Schutzmechanismus
5. Definierung zusätzlicher Maßnahmen
6. Implementierung zusätzlicher Maßnahmen
7. Ausnahmen nach Art. 49 DS-GVO
8. Dokumentation
9. Meldung an die Aufsichtsbehörde

Anzeige

GDD Winter-Workshop
für Datenschutzbeauftragte und -berater
sowie Datenschutzdienstleister

25.–26. Januar 2021 in Garmisch-Partenkirchen

Weitere Informationen erhalten Sie hier.

GDD DATAKONTEXT

Deutsche Ratspräsidentschaft legt neuen Entwurf zur ePrivacy-Verordnung vor und scheitert

Im Januar 2017 wurde der erste Vorschlag der Europäischen Kommission für die ePrivacy-Verordnung vorgelegt. Seitdem wird vor allem im Rat intensiv um eine gemeinsame Positionierung gerungen. Verschiedene Meinungsverschiedenheiten behinderten eine Einigung im Gremium der Regierungen der 27 Mitgliedstaaten immer wieder. Nun kommt durch die deutsche EU-Ratspräsidentschaft – inzwischen die achte Ratspräsidentschaft, die sich mit dieser Verordnung auseinandersetzt – neuer Schwung in die Debatte.

Veränderte Bestimmungen zur Zulässigkeit der Datenverarbeitung

Natürlich verfolgt auch die deutsche Ratspräsidentschaft die Verarbeitung von Verbindungs- und Standortdaten sowie Zugriffe auf Endgeräte der Nutzer und das Sammeln von Informationen, etwa mithilfe von Cookies, weiter zulässig zu gestalten. Gleichzeitig sieht die jüngste Fassung der Ratspräsidentschaft das "berechtigte Interesse" als Rechtmäßigkeitstatbestand für die Speicherung personenbezogener Daten nicht mehr vor. Gestrichen wurde der im letzten entsprechenden Dokument noch vorhandene Rechtmäßigkeitstatbestand:
"*…it is necessary for the purpose of the legitimate interests pursued by a service provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user. The end-user's interests shall be deemed to override the interests of the service provider where the end-user is a child or where the service provider processes, stores or collects the information to determine the nature and characteristics of the end-user or to build an individual profile of the end-user or the processing, storage or collection of the information by the service provider contains special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679*"
Danach müssen Unternehmen, die im Rahmen ihrer Geschäftstätigkeit personenbezogene Daten ihrer Kunden verarbeiten wollen, dies wohl über rechtliche Verpflichtungen oder die Vertragsdurchführung legitimieren.

Alternative Erlaubnistatbestände:

1. Metadatenverarbeitung zum Schutz lebenswichtiger Interessen erlaubt

Mittels Metadaten sind Zeit, Ort und an der Kommunikation beteiligte Personen erkennbar. In bestimmten Notfallsituationen soll es Kommunikationsanbietern zwar ermöglicht werden, diese Daten ohne Zustimmung zu verarbeiten. Beispiele für solche Notfallszenarien sind die Überwachung der Ausbreitung von Epidemien, Naturkatastrophen sowie von Menschen verursachte Katastrophen. Abgestellt wird hierbei auf den "Schutz lebenswichtiger Interessen", der sich auch in der DS-GVO wiederfindet. Dadurch ist dieser Tatbestand bereits weitestgehend in der Praxis bekannt und es insoweit eindeutig, welche Fälle von einer Metadatenverarbeitung aufgrund "lebenswichtiger Umstände" erfasst sind.

2. Datenverarbeitung zur Verbrechensbekämpfung

Außerdem wurde von der deutschen Ratspräsidentschaft eine Klarstellung vorgelegt. Diese regelt die Möglichkeit einer nationalen Behörde, auf bestimmte Daten der elektronischen Kommunikation zum Zwecke der Verbrechensbekämpfung zuzugreifen.
Der Zuwachs an Sicherheitsprotokollen führte zu einer Diskussion über die Möglichkeiten zum rechtmäßigen Abhören von Telekommunikationsnetzen der nächsten Generation. Diskutiert wird, wie es Strafverfolgungsbehörden ermöglicht werden kann, Kommunikation abzuhören. Die Mitgliedsstaaten arbeiten, wie sich im Januar herausstellte, gemeinsam mit Europol und der Europäischen Kommission an geeigneten Wegen, um Möglichkeiten zum rechtmäßigen Abhören in 5G-Netzen zu erhalten. Ursache dessen ist, dass die 5G-Technologie eine 256-Bit-Verschlüsselung verwendet, die ein neues Niveau an Privatsphäre und Anonymisierung in Kommunikationsnetzen ermöglicht. Dadurch entstehen mit dem vermehrten Einsatz von 5G im europäischen Raum neue Herausforderungen für Strafverfolgungsbehörden.

Kritik von Lobbyverbänden und Beobachtern

Protest dagegen kommt von der Telekommunikationsindustrie. Dort wird eine Verringerung des Potenzials für "Dateninnovation" befürchtet. Die Lobbyverbände ETNO (European Telecommunications Network Operators' Association) und GSMA (Global System for Mobile Communications) forderten die EU-Mitgliedstaaten zur Ablehnung des neuen Kompromisses auf.
Ferner bestehe die Sorge, die ePrivacy-Verordnung würde den Plänen der EU entgegenlaufen, ihre Datenwirtschaft als Teil ihrer bahnbrechenden Datenstrategie der Kommission weiter zu stärken. Diese Strategie soll bezwecken, dass das ungenutzte Potenzial riesiger Schätze an Industriedaten bestmöglich zu nutzen und sowohl öffentlichen als auch privaten Akteuren einen erleichterten Zugang zu großen Informationsreserven zu ermöglichen.

Neuer Vorschlag fällt durch

Der neue Vorschlag der deutschen Ratspräsidentschaft wurde am 11.11. in einer Ratsarbeitsgruppe abgelehnt. So hat die jüngste Vorlage bei den Mitgliedstaaten keine Mehrheit finden können.

Microsoft Office 365 und Datenschutz-Folgenabschätzung

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI Baden-Württemberg) unterstützt das Ministerium für Kultus, Jugend und Sport Baden-Württemberg bei einem Pilotprojekt zum Einsatz von Microsoft 365-Werkzeugen. Dabei stellt Office 365 lediglich eines der geplanten Anwendungen auf der sog. Digitalen Bildungsplattform dar.

Die Digitale Bildungsplattform soll den Schulen wesentliche Anwendungen und Dienste für einen digital unterstützten Unterricht bereitstellen. Die Plattform ist modular aufgebaut und hat zum Ziel, Lehrkräfte, Schulen und Schulträger von technischen, administrativen und datenschutzrechtlichen Fragen zu entlasten.

Zum Anwendungs-Portfolio gehören unter anderem auch Moodle, das Videokonferenzsystem Big Blue Button, der Messenger-Dienst Threema für Lehrkräfte sowie ein weiteres Lernmanagementsystem, das kurz vor dem Abschluss einer EU-weiten Ausschreibung steht. Office 365 soll dabei die dienstliche E-Mail-Adresse für Lehrkräfte, klassische Büro-Werkzeuge wie Word, PowerPoint, Excel sowie einen Datenspeicher und Teams als Videokonferenz- und Kollaborationssystem abdecken.

Für die Bausteine, bei denen Lösungen von Microsoft 365 zum Einsatz kommen sollen, hat das Kultusministerium mit externen Partnern eine Datenschutz-Folgenabschätzung (DSFA) erarbeitet. Die DSFA wurde in Absprache und enger Kooperation mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDi) Dr. Stefan Brink beraten und weiterentwickelt.

Im Pilotprojekt prüft der LfDI, ob die in der Datenschutz-Folgenabschätzung beschriebenen Datenflüsse auch den tatsächlich messbaren entsprechen und ob ein hinreichendes Datenschutzniveau auch in der Praxis besteht. Auch ist geplant, dass der LfDI Schulen auf Wunsch seine Beratungsleistungen und Unterstützung auch bei der Erstellung von Datenschutz-Folgenabschätzungen für alternative Produkte anbietet. In diesem Rahmen können Fachleute des Bildungszentrums für Datenschutz und Informationsfreiheit des LfDI (BIDIB) die Schulen – SchülerInnen, LehrerInnen und auch auf Wunsch Eltern z. B. bei Elternbeiratssitzungen – beraten.

Quelle: LfDI Baden-Württemberg

Anzeige

DSK veröffentlicht Orientierungshilfe Videokonferenzsysteme

Aufgrund der Maßnahmen zur Bekämpfung der Corona-Pandemie richten viele Unternehmen kurzfristig Telearbeitsplätze ein, sodass ihre Beschäftigten ihren arbeitsvertraglichen Pflichten auch von Zuhause nachkommen können. Um trotzdem die betriebsinterne Kommunikation sicherzustellen, setzen Unternehmen häufig sog. Software as a Service Dienstleister (kurz: SaaS) für Video- und Onlinekonferenzen, Meetings oder Webinare ein. Hierbei die Vorgaben der DS-GVO einzuhalten, erhöht nicht nur das Datensicherheitsniveau in Organisationen, sondern hilft den ungeregelten Abfluss von solchen Unternehmensinformationen zu verhindern, die im internationalen Wettbewerb die eigene Wertschöpfung sichern sollen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat nun eine "Orientierungshilfe Videokonferenzsysteme" veröffentlicht, in dem sie die datenschutzrechtlichen Anforderungen an die Durchführung von Videokonferenzen durch Unternehmen, Behörden und anderen Organisationen erläutert. Diese Handreichung soll den Verantwortlichen eine Hilfestellung bieten, wie diese Anforderungen erfüllt werden können.

Eine besondere Herausforderung bei der Sicherstellung der Datenschutzkonformität dürfte der Aspekt "Besonderheiten bei Übermittlungen an Drittländer" darstellen.

Wie unter Ziffer 3.5.6 der Orientierungshilfe dargestellt, dürfte mit der Tatsache, dass nach dem Schrems II-Urteil des EuGH das sog. EU-US-Privacy Shield nicht mehr als Mittel zur Sicherstellung eines angemessenen Schutzniveaus in den USA taugt und ein Zurückgreifen auf die EU-Standardvertragsklauseln ebenfalls versperrt sein wird, die Auswahl geeigneter Anbieter/Auftragsverarbeiter für Videokonferenzsysteme stark eingeengt sein.
Diese Vermutung wird durch einen Blick in das Papier "Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten" bestätigt.

Hilfreich, sowohl bei der Bewertung der Datenschutzkonformität als auch für den Vergleich der einzelnen Anbieter, ist auch die Praxishilfe "Videokonferenzen und Datenschutz" der Gesellschaft für Datenschutz und Datensicherheit (GDD e. V.).
Die Praxishilfe der GDD soll einen Beitrag zur Beseitigung bestehender Unsicherheit im Hinblick auf aktuelle datenschutzrechtliche Fragen rund um das Thema Videokonferenzen leisten.

Mit einer Auswahl und Gegenüberstellung verschiedener Anbieter von Videokonferenzlösungen und der dazugehörigen Veranschaulichung datenschutzrechtlicher Aspekte soll eine Hilfestellung für Datenschutzverantwortliche bei der Auswahl eines geeigneten Videokonferenzdienstleisters gegeben werden. Die Checkliste soll zudem die grundsätzlichen Anforderungen an Datenschutz und -sicherheit in diesem Zusammenhang veranschaulichen und einfaches "Abarbeiten" der Kriterien ermöglichen.

Datenschutz-Gutachten: Tesla in der Kritik

Bereits in der Laudatio zum BigBrotherAward 2020 in der Kategorie "Mobilität" musste die Firma Tesla Inc. für ihre Elektro-Autos einiges an Kritik einstecken. Der damalige Laudator, Dr. Thilo Weichert, kam damals zu dem Fazit, dass die (datenschutzrechtliche Funktionsweise) der Tesla-Autos unzulässig sei. Wer einen Tesla kaufe – es gab 2019 alleine 10.000 Neuzulassungen in Deutschland – müsse zunächst viele Dienste deaktivieren, um die DS-GVO einzuhalten.
Tesla erwähne die seit Mai 2018 in Europa geltende DS-GVO mit keinem Wort und berufe sich, was Übermittlungen in die USA angehe, auf das Privacy Shield, das kürzlich vom Europäischen Gerichtshof für ungültig erklärt worden sei. Die Tesla-Autos verstoßen schon im Normalbetrieb gegen die DS-GVO, so der Redner der Laudatio.

Nun hat Herr Dr. Weichert diese in der Laudation angerissenen Kritikpunkte in einem Rechtsgutachten (Datenverarbeitung und Datenschutz bei Tesla-Fahrzeugen Kfz-Automation und informationelle Selbstbestimmung), weiter ausgeführt. Darin untersucht Thilo Weichert die personenbezogene Datenverarbeitung im Modell 3 von Tesla und die von dem Unternehmen hierbei eingesetzten Allgemeinen Geschäftsbedingungen. Das Gutachten kommt zu dem Ergebnis, dass dabei in vieler Hinsicht gegen europäische Datenschutzregeln sowie gegen Verbraucherschutzrecht verstoßen wird.
So, wie diese derzeit in Deutschland ausgeliefert werden, dürften sie weder auf den Markt kommen, noch zugelassen werden, so Dr. Weichert im Ergebnis seiner Untersuchungen.

Quelle: Netzwerk Datenschutzexpertise

Interessenkollision bei Personalunion: DSB und IT-Sicherheitsbeauftragter

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) geht in seinem 2. Tätigkeitsbericht zum Datenschutz nach der DS-GVO (Berichtsjahr 2019, veröffentlicht am 22.10.2020) auf die Fragen von möglichen Interessenkollisionen für die Tätigkeit des Datenschutzbeauftragten ein (vgl. S. 135, Ziffer 4.1.).

In diesem Zusammenhang sei zu beachten, dass auch nach Wirksamkeit der DS-GVO die Tätigkeit eines IT-Sicherheitsbeauftragten und Datenschutzbeauftragten in Personalunion nicht miteinander vereinbar sein, da diese zu Interessenkonflikten führten.

Es sei zwar nachvollziehbar, dass für die Entscheidung, eine Person beide Aufgaben übernehmen zu lassen, die hohe Arbeitsbelastung, das knappe Personal und die Tatsache, dass in beiden Funktionen sehr gute IT-Kenntnisse notwendig seien, als Argumente vorgetragen werden könnten. Jedoch habe der TLfDI bereits in seinem 3. Tätigkeitsbericht zum nicht-öffentlichen Bereich (Beitrag 2.3) zur alten Rechtslage die Auffassung vertreten, dass in dieser Konstellation Interessenkonflikte drohen und daher die Bestellung zum betrieblichen Datenschutzbeauftragten (bDSB) unzulässig sei. Einen Grund, diese Bedenken auszuräumen, könne sich nicht aus der Neuausrichtung der Funktion des DSB, welche in der DS-GVO zu erkennen sei, ergeben.

Nach Art. 38 Abs. 6 DS-GVO sei es grundsätzlich möglich, dass der Datenschutzbeauftragte auch andere Aufgaben übernehmen könne. Dabei müsse allerdings zwingend sichergestellt werden, dass es nicht zu Interessenkonflikten komme. Interessenkonflikte seien immer dann anzunehmen, wenn der Datenschutzbeauftragte sich selbst (im Rahmen seiner anderweitigen Tätigkeit) kontrollieren müsse, oder die Unabhängigkeit des Datenschutzbeauftragten gefährdet wäre.

Eine mögliche Interessenkollision sieht der TLfDI u. a. in dem Umstand, dass der IT-Sicherheitsbeauftragte im Rahmen der Gefahrenabwehr von Angriffen Dritter auf IT-Systeme des Unternehmens oftmals an einer umfangreichen Sammlung personenbezogener Daten interessiert sei, um Missbrauch zu entdecken, während der DSB, unter Berücksichtigung der Schutzziele der DS-GVO, eine Begrenzung der Sammlung personenbezogener Daten anstrebe. Auch in puncto die Speicherdauer personenbezogener Daten sei zu erwarten, dass IT-Sicherheitsbeauftragte und Datenschutzbeauftragte häufig unterschiedliche Positionen vertreten müssten.

Quelle: Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI)

Anzeige

Die Überwachungsaufgabe des Datenschutzbeauftragten nach DS-GVO

Organisieren Sie mit dem Leitfaden interne Kontrollen, Datenschutz-Audits und Überwachung effektiv, nachweisbar, risikoorientiert!

Bestellen Sie direkt unter: **datakontext.com/ueberwachungsaufgabe**

DATAKONTEXT

Corona: Datenschutz bei Befreiung von der Maskenpflicht

In Zusammenhang mit der Coronakrise ist die Kontaktdatenerfassung von großem Interesse, um Infektionsketten aufzudecken und zu unterbrechen. Mit der zunehmenden Öffnung des Alltagslebens wird dies immer wichtiger. Inwieweit die Kontaktdatenerfassung im Bereich der Wirtschaft datenschutzrechtlich erlaubt ist, richtet sich nach den verschiedenen Wirtschaftsbranchen.

In allen Bundesländern existieren Ausnahmen von der Maskenpflicht, wenn das Tragen einer Mund-Nasen-Bedeckung aufgrund gesundheitlicher oder psychischer Einschränkungen nicht zumutbar bzw. nicht möglich ist. Das kann etwa Asthma oder anderen schweren Lungen- aber auch Herzerkrankungen gelten, bei denen die Sauerstoffversorgung bereits eingeschränkt ist. In aller Regel sollte die Erkrankung durch ein ärztliches Attest belegt sein, um einen entsprechenden Nachweis hierüber zu haben. Das BayLDA gibt in aktuellen Hinweisen eine Hilfestellung, was bzgl. der Verarbeitung von personenbezogenen Daten in solchen Fällen zu beachten ist.

Nach Auffassung des BayLDA muss und darf der Prüfende keine weiteren Daten erheben, soweit dem Prüfenden bereits Umstände bekannt sind, welche ihm einen Befreiungstatbestand als hinreichend wahrscheinlich erscheinen lassen.
Ansonsten kann eine Befreiung vom Tragen einer Mund-Nasen-Bedeckung insbesondere durch das Vorzeigen einer ärztlichen Bestätigung glaubhaft gemacht werden, so das BayLDA. Darüber hinaus empfiehlt die Behörde den Betroffenen, sich bei einem Arzt eine Bestätigung über die Befreiung vom Tragen einer Mund-Nasen-Bedeckung ausstellen zu lassen, die wie etwa bei einer Arbeitsunfähigkeitsbescheinigung keine Diagnose nennt. Die Bestätigung werde jedoch aus arztrechtlichen Gründen in der Regel die Facharztbezeichnung enthalten müssen. Sei zweifelhaft, dass das Attest für die vorzeigende Person ausgestellt wurde, könne der Verantwortliche verlangen, dass ein Ausweis vorgelegt wird.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

IT-Sicherheitslage in Deutschland weiter angespannt

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes. Ihre Aufgabe ist es, Deutschland digital sicherzumachen.

Wie jedes Jahr legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland einen umfassenden und fundierten Überblick über die Bedrohungen Deutschlands, seiner Bürger:innen und seiner Wirtschaft im Cyber-Raum vor.

Im Ergebnis sieht das BSI im aktuellen Bericht die IT-Sicherheitslage in Deutschland als angespannt an. Nach der Beobachtung des BSI reagieren Cyber-Kriminelle schnell auf gesellschaftlich relevante Themen und Trends. So verzeichnete das BSI unterschiedliche Angriffe unter Ausnutzung der COVID-19-Pandemie. Hier wurden beispielsweise Phishing-Kampagnen, CEO-Fraud und Betrugsversuche mit IT-Mitteln registriert.

Außerdem traten im Berichtszeitraum erneut mehrere, teils kritische Schwachstellen in Software-Produkten auf, die Angreifer für Schadprogramm-Angriffe oder Datendiebstahl ausnutzen konnten. Dabei nutzten die Angreifer auch verstärkt den Faktor "Mensch" als Einfallstor für Angriffe, die mit Social-Engineering-Methoden arbeiten und gleichsam als Türöffner für weitere Angriffe dienen.
Die geschickte Kombination eines digitalen Werkzeugkastens mit Social Engineering verhalf den professionell agierenden Cyberkriminellen, Infektionen auch bei professionellen Anwendern zu verursachen.

Zugleich stellt das BSI in seinem Bericht fest, dass die Bedrohung durch Daten-Leaks mit der Offenlegung von Millionen von Patientendatensätzen im Internet eine neue Qualität erreicht hat. Im Berichtszeitraum entdeckte das BSI unter anderem Datenbanken mit hochsensiblen medizinischen Daten frei zugänglich im Internet. Anders als bei Datendiebstählen war hier also kein technisch aufwändiger Angriff notwendig, sondern unzureichend gesicherte oder falsch konfigurierte Datenbanken waren Ursache für den Datenabfluss.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

DS-GVO-Bußgeld des BfDI hält Urteil des LG Bonn nicht stand

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hatte im November 2019 den Telekommunikationsdienstleister 1&1 Telecom GmbH wegen eines grob fahrlässigen Verstoßes gegen Art. 32 Abs. 1 DS-GVO mit einer Geldbuße in Höhe von 9.550.000 Euro belegt.
Das Unternehmen hatte nach Auffassung des BfDI keine hinreichenden technisch-organisatorischen Maßnahmen ergriffen, um zu verhindern, dass Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können.

Im Fall von 1&1 Telecom GmbH hatte der BfDI Kenntnis erlangt, dass Anrufer bei der Kundenbetreuung des Unternehmens allein schon durch Angabe des Namens und Geburtsdatums eines Kunden weitreichende Informationen zu weiteren personenbezogenen Kundendaten erhalten konnten. In diesem Authentifizierungsverfahren sah der BfDI einen Verstoß gegen Artikel 32 DS-GVO, nach dem das Unternehmen verpflichtet ist, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Verarbeitung von personenbezogenen Daten systematisch zu schützen.

Nach der damaligen Einschätzung des BfDI bewegte er sich bei der Festsetzung der Höhe der Geldbuße aufgrund des während des gesamten Verfahrens kooperativen Verhaltens von 1&1 Telecom GmbH im unteren Bereich des möglichen Bußgeldrahmens.

Der Telekommunikationsdienstleister legte gegen den Bußgeldbescheid Einspruch ein, sodass die Sache an fünf Verhandlungstagen vor der 9. Kammer für Bußgeldsachen verhandelt wurde. Am heutigen Tag (11.11.2020) erging am Landgericht Bonn das Urteil im Verfahren.

Die Höhe des Bußgeldes hat die Kammer in ihrer Entscheidung auf 900.000 EUR herabgesetzt. Dabei sei berücksichtigt worden, dass das Verschulden des TK-Anbieters gering gewesen sei. Die Geringfügigkeit des Datenschutzverstoßes sei auch vom BfDI nicht bestritten worden. Für die Geringfügigkeit spreche, dass die fehlenden technisch-organisatorischen Maßnahmen im Sinne des Art. 32 DS-GVO nicht geeignet gewesen seien, zu einer massenhaften Herausgabe von Daten an Nichtberechtigte zu führen. In der Sache habe die Kammer aber einen Datenschutzverstoß festgestellt, da der TK-Anbieter die Daten seiner Kunden im Rahmen der Kommunikation über die Callcenter nicht durch ein hinreichend sicheres Authentifizierungsverfahren geschützt habe.

Eine Stellungnahme des BfDI zum Ausgang des Verfahrens folgte bereits am Tag der Urteilsverkündung. Der BfDI sieht sich durch die Entscheidung des Landgerichts Bonn bestätigt. Das LG Bonn habe geurteilt, dass 1&1 für seinen Verstoß hafte. Das zeige, dass Datenschutzverstöße nicht ohne Folgen blieben.

Auch wenn der BfDI in seiner Stellungnahme nicht auf die beträchtliche Reduzierung der Höhe der Geldbuße eingeht, dürfte diese ggf. verkürzte Feststellung durchaus den Kern des Urteils richtig beschreiben. Vor dem Hintergrund, dass sowohl der BfDI als auch das LG Bonn von einem eher geringfügigen Datenschutzverstoß ausgehen, kann die Höhe des Bußgeldes trotz der Reduzierung als wirksam, verhältnismäßig und abschreckend im Sinne des Art. 83 Abs. 1 DS-GVO bezeichnet werden. Eine interessante Frage wäre, wie das LG Bonn wohl in einem Fall eines Kalibers wie H & M geurteilt hätte.

Ob der Ausgang des Urteils ggf. dazu führt, dass das Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen neu angefasst wird, bleibt abzuwarten.

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen?
Dann tragen Sie sich unverbindlich und kostenlos ein unter www.datakontext.com/newsletter