Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

in dieser Ausgabe unserer Beratungsinformation haben wir Ihnen vier Stellungnahmen von Aufsichtsbehörden zu den aktuellen Themen Facebook-Fanpages, Nutzung von Zoom, Verwendung von Fax sowie dem Fragerecht des Arbeitgebers zum Corona-Impf-/Genesenenstatus oder Testergebnis seiner Beschäftigten zusammengestellt. Die Position der Aufsichtsbehörden ist in diesen Themen eine wichtige Orientierung. Allerdings darf nicht vergessen werden, dass nicht die Aufsichtsbehörden, sondern die Gerichte bei der Klärung von Rechtsfragen die letzte Instanz sind.

Zum Abschluss informieren wir über die Entscheidung des Landgerichts Essen zu einer Schadenersatzklage wegen eines auf dem Postweg verlorengegangenen unverschlüsselten USB-Sticks.

Ich wünsche Ihnen eine interessante Lektüre.

Ihr

Asmus Eggert

Inhalt

Bundesbeauftragter für den Datenschutz kündigt Vorgehen gegen Facebook-Fanseiten bei Bundesbehörden an

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber, hat am 16.06.2021 seine E-Mail an alle Bundesministerien und -behörden veröffentlicht, in der er insbesondere auf sein Rundschreiben vom 20.05.2021 verweist, in dem dargelegt wurde, dass der Betrieb einer datenschutzkonformen Fanpage der Facebook Inc. derzeit nicht möglich sei. Es wäre

erforderlich, dass öffentliche Stellen, die eine Fanpage betreiben, eine Vereinbarung mit Facebook zur gemeinsamen Verantwortlichkeit schließen müssten, die den Anforderungen von Art. 26 Datenschutz-Grundverordnung (DSGVO) entspräche. Diese gebe es derzeit nicht. Das von Facebook bereitgestellte „Addendum“ sei aus Sicht der Datenschutzbehörden von Bund und Ländern weiterhin unzureichend.

Aus Sicht von Herrn Kelber ist es auch nicht ausreichend, die Nutzer in Bezug auf Informationen zur Verarbeitung der personenbezogenen Daten im Rahmen einer Facebook-Fanpage allein pauschal auf Facebook zu verweisen. Für diese Fälle geht er von der fortdauernden Verletzung des Schutzes personenbezogener Daten der Nutzerinnen und Nutzer aus. Sofern die Behörden eine Fanpage betrieben, empfehle er diesen daher nachdrücklich, diese bis Ende 2021 abzuschalten. Ab Januar 2022 beabsichtige er – im Interesse der betroffenen Bürgerinnen und Bürger – schrittweise von den ihm nach Art. 58 DSGVO zur Verfügung stehenden Abhilfemaßnahmen Gebrauch zu machen.

Der BfDI weist ferner darauf hin, dass auch die Nutzung von Instagram, TikTok und Clubhouse datenschutzrechtlich bedenklich sein könnte, und riet daher bis auf Weiteres von der Nutzung dieser Apps auf Geschäftsgeräten ab.

Praxishinweis: Herr Kelber legt für seinen Zuständigkeitsbereich der Bundesbehörden den Finger in die Wunde. Für die datenschutzrechtliche Bewertung macht es dabei keinen Unterschied, ob es sich um öffentliche oder nicht öffentliche Organisation handelt. Soweit Sie in Ihrer Organisation Facebook-Fanpages unterhalten, sollten Sie sich bewusst sein, dass die Aufsichtsbehörden dies als nicht datenschutz-konform einstufen. Zwar sind die Aufsichtsbehörden nicht die letzte Instanz für derartige Entscheidungen, sondern die Gerichte, aber Sie sollten die Aktion des BfDI zum Anlass nehmen, eine Risikobewertung vorzunehmen (Deaktivierung vs. Weiterbetrieb - und im Falle eines Weiterbetriebs, welche risikominimierenden Datenschutzmaßnahmen lassen sich ggf. implementieren).

Hamburger Datenschutzaufsicht mahnt Senatskanzlei wegen der Nutzung von Zoom ab

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat im August darüber informiert, dass er die Senatskanzlei der Freien und Hansestadt Hamburg wegen der Nutzung von Zoom Inc. abgemahnt hat. Der HmbBfDI wies insbesondere darauf hin, dass die Praktiken von Zoom in Bezug auf Datenübermittlungen nicht mit der Datenschutzgrundverordnung und dem EuGH-Urteil in der Rechtssache „Schrems II" (Az. C-311/18) vereinbar seien. Ein Datentransfer sei nur unter sehr engen Voraussetzungen möglich, die bei dem geplanten Einsatz von Zoom durch die Senatskanzlei nicht vorlägen. Die Daten von Behördenbeschäftigten und externen Gesprächsbeteiligten würden auf diese Weise der Gefahr einer anlasslosen staatlichen Massenüberwachung in den USA ausgesetzt, gegen die keine ausreichenden Rechtsschutzmöglichkeiten bestünden. Der HmbBfDI, Ulrich Kühn, kommentierte: *„Öffentliche Stellen sind in besonderem Maße zur Einhaltung des Rechts verpflichtet. Es ist daher mehr als bedauerlich, dass ein solcher formaler Schritt unternommen werden musste.“*

Praxishinweis: Der Einsatz und die Auswahl von Videokonferenzsystemen stellt für Organisationen insbesondere aufgrund der Schrems II Rechtsprechung des EuGHs eine Herausforderung dar. Wir hatten bereits eine Checkliste zur Auswahl von Videokonferenzsystemen zur Verfügung gestellt. Achten Sie bei der Auswahl und dem Einsatz auf datenschutzkonforme Einstellungen und Nutzung der Tools. Dies gilt umso mehr, wenn Sie Videokonferenzsysteme von Nicht-EU/EWR-Anbietern einsetzen.

HBDI gibt Stellungnahme zu datenschutzrechtlichen Risiken der Faxnutzung ab

Der Hessische Datenschutzbeauftragte (HBDI) hat am 14.09.2021 eine Stellungnahme zur Nutzung von Fax als Kommunikationsmittel durch Unternehmen veröffentlicht. Der HBDI stellte in dieser Stellungnahme insbesondere fest, dass das Faxen im Interesse der Datensicherheit und vor dem Hintergrund der fortschreitenden Digitalisierung als unsicheres Kommunikationsmittel einzustufen sei. In diesem Zusammenhang wies der HBDI auf die folgenden Risiken bei der Übermittlung personenbezogener Daten per Fax hin:

- Personenbezogene Daten können unbefugt an Dritte gelangen, wenn die Faxnummer des Empfängers falsch eingegeben wird;
- Der Absender des Faxes verfügt möglicherweise nicht über ausreichend Informationen über den möglichen Kreis an Empfängern, z. B. wo sich das Empfangsgerät befindet und wer Zugang zu ihm hat;
- Bei der heute üblicherweise verwendeten Faxübertragungsmethode (keine dezidierten Leitungen mehr, sondern über Internet) werden die Daten bei der Übertragung grundsätzlich nicht verschlüsselt.

Darüber hinaus forderte der HBDI auf, so schnell wie möglich alternative datenschutzkonforme Kommunikationsmittel zum Fax zu prüfen und einzusetzen.

Praxishinweis: Bereits in der Juni-Ausgabe unserer Beratungsinformation hatten wir über eine Entscheidung des OVG Lüneburg im Beschluss vom 22.07.2020 – 11 LA 104/19 sowie eine Orientierungshilfe der Bremer Aufsichtsbehörde vom Mai 2021 hingewiesen. Die Problematik des Einsatzes des Fax zur Übermittlung personenbezogener Daten festigt sich also. Unser Praxishinweis in der Juni-Ausgabe ist weiterhin aktuell:

Prüfen Sie den Einsatz des Telefax für den Austausch personenbezogener Daten. Stellen Sie auf Alternativen um (Versand per Ende-zu-Ende verschlüsselte E-Mails, Download-Lösungen oder – im Zweifel – Nutzung des herkömmlichen Postwegs). Zur Übertragung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der DSGVO (z.B. Gesundheitsdaten) ist die Nutzung von Fax-Diensten nach Bewertung der Aufsichtsbehörde in jedem Falle unzulässig. Besteht ein/eine Empfänger:in auf den Faxversand, sollten Sie sich als Versandstelle dazu von dieser/diesem eine Einwilligung einholen, in der Sie auf die Risiken dieses Kommunikationsweges hinweisen.

Sächsischen Datenschutztaufsicht: Stellungnahmen zum Fragerecht des Arbeitgebers nach dem Impf-/Genesenenstatus oder Testergebnis seiner Beschäftigten

Die Sächsische Datenschutzaufsichtsbehörde (SächsDSB) hat am 29.09.2021 eine Stellungnahme zur Frage abgegeben, ob der Arbeitgeber von seinen Arbeitnehmern die Bekanntgabe des Impf- und Genesenenstatus‘ oder eines negativen COVID-19-Tests verlangen kann.

Die Einführung des 2G-Optionsmodells in einem Unternehmen berechtige den Arbeitgeber nach Ansicht der Aufsichtsbehörde nicht dazu, den Impf- oder Genesungsstatus der Arbeitnehmer zu verarbeiten. Der Impf- oder Genesungsstatus seien grundsätzlich Gesundheitsdaten im Sinne von Artikel 4 Nr. 15 DSGVO und stellen somit besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Abs. 1 DSGVO dar. Für deren Verarbeitung sei eine klare Rechtsgrundlage erforderlich. Eine solche verneint die Aufsichtsbehörde als Ergebnis einer ausführlichen datenschutzrechtlichen Prüfung.

Insbesondere geht die Aufsichtsbehörde davon aus, dass auch das Einholen einer Einwilligung als Rechtsgrundlage nur in wenigen Fällen in Anspruch genommen werden kann, um die Verarbeitung

dieser Gesundheitsdaten von Beschäftigten durch Arbeitgeber zu legitimieren. Dies wird damit begründet, dass die Anforderungen an eine wirksame Einwilligungserklärung im Beschäftigungsverhältnis wegen des zwischen Beschäftigten und Arbeitgeber bestehenden Abhängigkeitsverhältnisses hoch seien. Daher scheitere die Einwilligung in der Regel an der erforderlichen Freiwilligkeit.

Fazit: Folgt man der Ansicht der sächsischen Datenschutzaufsichtsbehörde ist ein Fragerecht des Arbeitgebers bezüglich des Impf- und Genesenenstatus‘ zu verneinen. Ein Fragerecht des Arbeitgebers bezüglich des Ergebnisses eines Tests auf das Nichtvorliegen einer Infektion mit SARS-CoV-2 bestehe ebenfalls regelmäßig nicht. Es obliege daher den zuständigen Gesundheitsbehörden, die Einhaltung der Voraussetzungen des § 6a SächsCoronaSchVO zu prüfen.

Praxishinweis: Gesundheitsdaten unterliegen als besondere Kategorien personenbezogener Daten einem hohen Schutz und fordern vom Arbeitgeber einen sensiblen Umgang. Der Umgang mit den gesetzlichen Anforderungen und Regelungen der Maßnahmen zur Bekämpfung der Corona-Pandemie stellt Arbeitgeber vor besondere Herausforderungen. Die strikte Haltung der Aufsichtsbehörden erschwert pragmatische Ansätze. Dennoch müssen datenschutzkonforme Lösungen gefunden werden, die die Interessen der Organisationen, Kunden und Beschäftigten rechtkonform abbilden. Wenn Sie hier Unterstützung benötigen, sprechen Sie Ihren Berater an.

LG Essen: Versand eines unverschlüsselten USB-Sticks mit personenbezogenen Daten per einfacher Post ist kein Verstoß gegen den Datenschutz

Das LG Essen (Urt. v. 23.09.2021 - Az. 6 O 190/21) hat geurteilt, dass das Zurückschicken eines unverschlüsselte USB-Sticks mit personenbezogenen Daten per Briefpost von einem Unternehmen an die Absender datenschutzkonform ist und dem aktuellen Stand der Datensicherheit nach Art. 32 DSGVO entspricht. Der Entscheidung lag folgender Sachverhalt zugrunde:

Der Kläger und seine Ehefrau stellten der Beklagten im Rahmen des Antrags einer Immobilienfinanzierung zahlreiche private Unterlagen (u.a. Ausweisdokumente, Steuerunterlagen und Einkommensverhältnisse) auf einem unverschlüsselten USB-Stick zur Verfügung, den Sie in den Briefkasten der Beklagten warfen. Der Immobilienfinanzierungsvertrag kam nicht zustande. Daraufhin schickte die Beklagte den USB-Stick mit einfacher Briefpost an den Kläger zurück. Dort kam er allerdings nicht an. Daraufhin hatte der Kläger einen DSGVO-Schadensersatz gegen die Beklagte i.H.v. mindestens 30.000 EUR geltend gemacht. Das LG Essen lehnt den Schadensersatzanspruch des Klägers ab.

Aus Sicht des Gerichts entspricht die Rücksendung des unverschlüsselten USB-Sticks dem aktuellen Stand der Datensicherheit nach Art. 32 DSGVO. Es sieht keinen Grund, weshalb die Beklagte den USB-Stick nicht per einfachem Brief an den Kläger und seine Ehefrau hätte versenden dürfen. Zwar waren auf dem USB-Stick Dokumente mit sensiblen persönlichen und wirtschaftlichen Informationen enthalten. Dies sei jedoch kein Grund, nicht den Service der Deutschen Post nutzen zu dürfen. Von verschiedensten Stellen würden ausgedruckte Dokumente mit sensiblen Informationen, z.B. Steuerbescheide, Schreiben von Anwälten und Steuerberatern o.Ä., mit einfacher Post versandt. Hiergegen sei ebenfalls nichts einzuwenden; eine irgendwie geartete Pflichtverletzung der handelnden Stellen ist nicht ersichtlich. Weshalb zwischen ausgedruckten Dokumenten, die naturgemäß unverschlüsselt übersandt werden, und digitalen Dokumenten auf einem unverschlüsselten USB-Stick im Zuge der postalischen Übermittlung unterschieden werden soll, erschließe sich dem Gericht nicht.

Auch hatte es in dem Fall an einem konkreten Schaden gefehlt. Aus Sicht des Landgerichts genüge ein bloßes "ungutes Gefühl" sowie die theoretisch mögliche Gefahr eines Datenmissbrauchs nicht, um den Anspruch zu begründen.

Praxishinweis: In der Beratungspraxis ist der Einsatz von USB-Sticks nach wie vor ein Thema. Soll der Stick für den Transfer von personenbezogenen Daten genutzt werden, stellt sich stets die Frage der Erforderlichkeit der Verschlüsselung. Diese ist immer dann zu bejahen, wenn es ein Risiko für einen unberechtigten Zugriff auf die dort gespeichert Daten gibt. Im Prinzip stellt der Einsatz der Post als „Datentransporteur“ einen verschlüsselten Versand dar. Verhindert werden können damit jedoch keine Datenverstöße beim Sender und beim Empfänger selbst. Hier sind die Daten nur zu schützen, wenn auch der Datenträger, also der USB-Stick selbst, einen unberechtigten Zugriff verhindert. Das kann nur die Verschlüsselung des Datenträgers selbst. Daher empfehlen wir die Verschlüsselung von USB-Sticks.

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Asmus Eggert

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 18 Abs. 2 MStV: Asmus Eggert