Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

Bilder sagen mehr als 1.000 Worte. Werden Menschen identifizierbar auf der Webseite, in Broschüren oder sonstigen Firmenunterlagen abgebildet, ist der Datenschutz zu beachten. In der Regel wird man wenigstens die Einwilligung der abgebildeten Person einholen müssen. Wird das unterlassen, kann das Schadensersatzzahlungen zur Folge haben. Wir informieren Sie über eine entsprechende Entscheidung des Arbeitsgerichts Münster.

Umgekehrt kann Beschäftigten durchaus fristlos gekündigt werden, wenn diese gegen den Datenschutz verstoßen. Einen solchen Fall hatte das Landesarbeitsgericht Köln zu entscheiden. Und auch ein Geschäftsführer wird in Mithaftung genommen, wenn er nicht datenschutzkonforme Maßnahmen veranlasst, so ein Urteil des Oberlandesgerichts Dresden. Das Oberlandesgericht Düsseldorf musst sich Ende des letzten Jahres mit einem Fall des Versandes einer unverschlüsselten E-Mail an einen falschen Adressaten befassen. Da dies ein latentes Risiko in jeder Organisation in der heutigen Zeit ist, greifen wir auch dieses Thema für Sie noch einmal auf. Sie finden die Informationen über die drei Entscheidungen in dieser Ausgabe.

Seit der Schrems-II-Entscheidung des Europäischen Gerichtshofs stehen Unternehmen und Organisationen vor der Herausforderung, den datenschutzkonformen Einsatz von Software und Diensten von US-amerikanischen Anbietern zu gewährleisten. Das Landgericht München I sowie die französische Aufsichtsbehörde (CNIL) haben sich zum Jahresbeginn hinsichtlich der Dienste „Google-Fonts“ und „Google Analytics“ eindeutig positioniert: Ihr Einsatz ist nicht DSGVO-konform.

Wir schließen diese Ausgabe mit dem Hinweis auf die 2. Auflage des Leitfadens „Datenschutz ist Chefsache“ des Landesbeauftragte für den Datenschutz Sachsen-Anhalt.

Ich wünsche eine anregende Lektüre

Ihr

Asmus Eggert

Inhalt

ArbG Münster: Foto ohne Einwilligung – Beschäftigte erhält 5.000 Euro Schadensersatz 2
LAG Köln: Fristlose Kündigung wegen Datenschutzverstoß 2
OLG Dresden: Geschäftsführer haften persönlich für Datenschutzverstöße der GmbH 3
OLG Düsseldorf: Schadensersatz wegen der unverschlüsselten Übersendung einer Gesundheitsakte an eine falsche E-Mailadresse 3
Nutzung von Google Diensten in Europa nach Schems-II 4
Literaturhinweis: „Datenschutz ist Chefsache“ 5

ArbG Münster: Foto ohne Einwilligung – Beschäftigte erhält 5.000 Euro Schadensersatz

In Rahmen einer Kündigungsschutzklage hatte sich das Arbeitsgericht Münster, Urt. v. 25.03.2021 – 3 Ca 391/20, auch mit einem datenschutzrechtlichen Anspruch auf Schadensersatz wegen der Verwendung eines Fotos ohne Einwilligung zu beschäftigen. Das Gereicht stellte fest, dass der Arbeitgeber unter Verstoß gegen die DSGVO und das Kunst-Urhebergesetz (KUG) ein Bild der Arbeitnehmerin ohne deren schriftliche Einverständniserklärung verwendet.

Nach Ansicht des Gerichts hätte sich der Arbeitgeber von der Arbeitnehmerin nach § 26 Abs. 2 S. 3 BDSG eine schriftliche Einwilligung einholen und zuvor in Textform über den Zweck der Datenverarbeitung und ihr Widerrufsrecht aufklären müssen. Im Arbeitsverhältnis ist § 22 KUG verfassungskonform dahingehend auszulegen, dass die Einwilligung der Schriftform bedarf, vgl. BAG 8 AZR 1010/13. Die Arbeitnehmerin sei auch nicht derartig untergeordnet auf dem Bild zu sehen, so dass hier keine Ausnahme für die Entbehrlichkeit einer schriftlichen Einwilligung nach § 23 KUG vorläge.

Praxishinweis: Fotos transportieren Emotionen. Es ist daher verständlich, dass sich Organisationen in ihren Publikationen nicht auf Texte beschränken, sondern auch Bilder und Videos einsetzen wollen.

Datenschutzkonform ist das nur möglich, wenn es hierfür eine Rechtsgrundlage gibt. Das kann ein Vertrag sein (Modellvertrag), in dem die abgebildete Person dem Verwender des Bildes die Nutzung erlaubt bzw. das Nutzungsrecht gegen Bezahlung oder gegen Einräumung von Nutzungsrechten an den Bildern für persönliche Zwecke der abgebildeten Personen abtritt. Gibt es keine vertragliche Grundlage, kommt die Einwilligung in Betracht, auf die im vorliegenden Fall auch das Gericht abstellt. Fehlt diese, stellt diese unberechtigte Verwendung von Bildern eine rechtswidrige Datenverarbeitung dar. Alle Verantwortlichen, die Bildnisse ohne Zustimmung der betroffenen Person nutzen, setzen sich folglich dem Risiko eines nicht unerheblichen Entschädigungsanspruchs nach Art. 82 DSGVO aus.

LAG Köln: Fristlose Kündigung wegen Datenschutzverstoß

Das Landesarbeitsgericht Köln hatte sich im Rahmen einer Kündigungsschutzklage mit der Frage zu beschäftigen, ob eine mit der Buchhaltung betraute Mitarbeiterin fristlos, also ohne vorherige Abmahnung, gekündigt werden kann, wenn Sie einen Datenschutzverstoß begangen hat. Dies hat das Gericht in dem konkreten Fall bejaht (Urteil vom 02.11.2021 - 4 Sa 290/21).

Folgendes war vorgefallen: Die Mitarbeiterin war in einer Kirchengemeinde als Buchhalterin angestellt. Sie war im Rahmen ihrer Tätigkeit berechtigt, auf das E-Mailkonto der Gemeinde zuzugreifen und E-Mails mit Bezug zu ihren buchhalterischen Aufgaben zu öffnen, zu lesen und zu bearbeiten. Sie hat E-Mails, die offensichtlich an einen anderen Beschäftigten der Gemeinde gerichtet waren und auch keinen Bezug zu ihrer Tätigkeit hatten, gelesen, kopiert und an Dritte weitergeitet.

Aus Sicht des Gerichts kann die rechtswidrige Datenverarbeitung des Arbeitnehmers im Arbeitsverhältnis, die mit Verletzungen des allgemeinen Persönlichkeitsrechts etwa von Arbeitskollegen einhergeht, dazu geeignet sein, bei entsprechender Schwere des Verstoßes "an sich" einen wichtigen Grund für den Ausspruch einer Kündigung darstellen, auch wenn die in Rede stehenden Daten nicht dem Schutzbereich des Gesetzes zum Schutz von Geschäftsgeheimnissen unterliegen.

Im verhandelten Fall konnte nach Ansicht des Gerichts für die rechtliche Bewertung dahinstehen, ob die Mitarbeiterin das E-Mailkonto der Gemeinde oder den Dienstcomputer durchsucht hat oder zufällig auf die E-Mails im Postfach gestoßen ist. Bereits das Öffnen und Lesen der E-Mails sei als Pflichtverstoß zu werten, völlig unabhängig davon, ob diese gezielt gesucht oder zufällig entdeckt

wurden. Sie sei hierzu nicht berechtigt gewesen. Zudem habe Sie bestimmte E-Mails, die zwischen dem anderen Beschäftigten und dessen Vorgesetzten ausgetauscht wurden, ausgedruckt und den Anhang einer E-Mail kopiert, was weitere Pflichtenverstöße darstelle.

Durch die Weitergabe der rechtswidrig erlangten Daten an eine dritte Person habe die Mitarbeiterin, so das Gericht, den vorherigen Verstoß gegen die arbeitsvertragliche Schutz- und Rücksichtnahmepflicht vertieft, das allgemeine Persönlichkeitsrecht des anderen Beschäftigten und dessen Kontaktpersonen verletzt und einen weiteren Verstoß durch eine rechtswidrige Datenverarbeitung - nämlich durch das Verbreiten - begangen.

Praxishinweis: In Organisationen sind regelmäßig Sammelpostfächer (info@, kontakt@, Bewerbung@, Job@ etc.) im Einsatz. Freilich müssen die E-Mails aus diesen Postfächern bearbeitet werden. Zum einen ist über ein Berechtigungskonzept sicher zu stellen, wer hier was soll und darf. Bewerbungen sollten z.B. in ein gesondertes Postfach gehen und nicht auf eine info@-Adresse. Zum anderen muss nach außen für alle Sender klar sein, dass ein Sammelpostfach nicht der Platz ist, Privates auszutauschen. Bearbeiter:innen dieser Konten sollten Sender:innen, denen das nicht klar ist, auf diese Situation hinweisen. An dieser Stelle empfehlen wir dem Management dringend, die private Nutzung des dienstlichen E-Mail-Postfachs, auch des individuellen, zu untersagen. Nur so kann nachhaltig die notwendige Trennung von dienstlichen und privaten Angelegenheiten datenschutzkonform sichergestellt werden.

Es gibt diverse Möglichkeiten, diese Vorgabe umzusetzen (z.B. Zusatzvereinbarung zum Arbeitsvertrag, Betriebsvereinbarung, Richtlinie). Sollten Sie hierbei Unterstützung benötigen, sprechen Sie Ihren Berater gerne an.

OLG Dresden: Geschäftsführer haften persönlich für Datenschutzverstöße der GmbH

Das Oberlandesgericht Dresden (Urt. v. 30.11.2021 – 4 U 1158/21) hat eine Gesellschaft und ihren Geschäftsführer als Gesamtschuldner zur Zahlung von 5.000 Euro DSGVO-Schadensersatz verurteilt. Das Gericht ging dabei davon aus, dass neben der Gesellschaft auch der Geschäftsführer selbst als datenschutzrechtlich Verantwortlicher einzustufen sei und daher für den Datenschutzverstoß persönlich hafte.

Sollten weitere Gerichte dieser Auffassung folgen, müssten Geschäftsführer:innen zukünftig damit rechnen, wegen Datenschutzverstößen auch persönlich in Anspruch genommen zu werden. Dieses Haftungsrisiko besteht, folgt man der Ansicht des Gerichts, insbesondere dann, wenn Geschäftsführer:innen die Datenverarbeitung, die dem Datenschutzverstoß zugrundeliegen, selbst initiiert oder an entsprechenden Entscheidungen oder Beauftragungen mitgewirkt haben.

Praxishinweis: Geschäftsführer vertreten die Gesellschaft. Sie haben die Umsetzungsverantwortung für den Datenschutz im Unternehmen und müssen daher eine entsprechende Datenschutzorganisation implementieren. In Rahmen des Datenschutzmanagements haben sie für die Einhaltung des Datenschutzes zu sorgen. Tun sie das nicht, setzen Sie ihr Unternehmen und auch sich selbst Haftungsrisiken bei Datenschutzverstößen aus.

OLG Düsseldorf: Schadensersatz wegen der unverschlüsselten Übersendung einer Gesundheitsakte an eine falsche E-Mailadresse

Das Oberlandesgericht Düsseldorf hat einer Versicherungsnehmerin einen Schadensersatz iHv. 2.000 EUR gegen ihre Versicherung zugesprochen, weil ein Mitarbeiter der Versicherung die E-Mail

mit der Akte versehentlich nicht an sie, sondern aufgrund einer falschen Eingabe an einen fremden Adressaten geschickt hatte (Urteil vom 28.10.2021 - 16 U 275/20).

Das Gericht kommt interessanterweise in dem konkreten Fall zu dem Ergebnis, dass die Versicherungsnehmerin in den unverschlüsselten Versand per E-Mail an sich wirksam nach Art. 6 Abs.1 Satz1 a) DSGVO eingewilligt habe (die Aufsichtsbehörden halten einen Verzicht durch Einwilligung für unzulässig). Nicht als erforderlich sah das Gericht an, dass hier eine sog. informierte Einwilligung eingeholt hätte werden müssen. Das Merkmal der Erklärung der Einwilligung in informierter Weise verlangt, dass die betroffene Person abschätzen können muss, welche Auswirkungen die Erteilung der Einwilligung für sie hat (Buchner/Kühling, in: dies., DS-GVO/BDSG, 3. Aufl., Art. 7 Rn. 59). Nach ihrer informatorischen Anhörung habe der Senat nicht die geringsten Zweifel gehabt, dass der Versicherungsnehmerin die Problematik und die Gefahren einer unverschlüsselten Versendung ihrer nicht pseudonymisierten Gesundheitsakte erkannt habe.

Auch stellt der Senat keinen Verstoß gegen Art. 32 DSGVO fest. Er geht davon aus, dass die Versicherung die technischen und organisatorischen Maßnahmen grundsätzlich eingehalten hat, auch wenn ein Beschäftigter auf Grund des Wunsches einer Versicherungsnehmerin auf den Schutz des verschlüsselten Versands verzichtet.

Als Datenschutzverstoß sah das Gericht aber schließlich die Tatsache des Falschversands an. Da die Versicherte hierdurch die Kontrolle über die Daten verlor und es sich auch um einen bedeutenden Umfang sowie vor allem um Gesundheitsdaten handelte, bejahte das Gericht einen Schmerzensgeldanspruch in Höhe von 2.000 EUR.

Praxishinweis: Verschlüsselung schützt! Verantwortliche setzen sich dem Risiko einer Datenpanne durch unberechtigte Zugriffe aus, wenn sie personenbezogene Daten per E-Mail verschicken. Der Fall, dass versehentlich eine unverschlüsselte Datei an einen falschen Adressatengeschickt wird, kommt immer wieder vor und stellt kein abstraktes Risiko dar. Die falsch adressierte E-Mail ist eine Datenpanne mit den Folgen der Art. 33 und 34 DSGVO. Das Prozedere zum Umgang mit Datenpannen, das allen Beschäftigten bekannt sein muss, ist fristgerecht (72 Stunden-Frist!) zu durchlaufen und zu dokumentieren.

Ob diese Pannen gemeldet werden muss oder dem Betroffenen anzuzeigen sind, hängt davon ab, ob der Verstoß voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Es ist offensichtlich, dass die verschlüsselte Datei mit personenbezogenen Daten, die bei einem unberechtigten Empfänger landet, ein deutlich niedrigeres Risiko darstellt als eine unverschlüsselte.

Auf den Beschluss der Datenschutzkonferenz (DSK), dass Verantwortliche nur im Einzelfall auf die Verschlüsselung verzichten dürfen, haben wir in der Januar Ausgabe der Beratungsinformation hingewiesen.

Nutzung von Google Diensten in Europa nach Schems-II

In den vorgegangenen Beratungsinformationen hatten wir in unterschiedlichen Zusammenhängen über die Auswirkungen der Schems-II-Entscheidung des Europäischen Gerichtshofs (EuGH) in der Zusammenarbeit Europäischer Unternehmen mit US-Amerikanischen Softwareanbietern informiert. In dieser Ausgabe wollen wir auf ein Urteil des Landgerichts München vom Januar in Sachen „Google Fonts“ und der Entscheidung der Französischen Datenschutzaufsicht (CNIL) zur Datenschutzkonformität von „Google Analytics“ hinweisen.

Google stellt über den Dienst „Google Fonts“ externe Schriftarten (Fonts) der Google Ireland Limited (Registernummer: 368047), Gordon House, Barrow Street, Dublin 4, Irland, https://www.google.com/fonts zur Verfügung. Die Einbindung von Google Fonts erfolgt durch Abruf der Fonts bei einem Google-Server (in der Regel in den USA). Google erhält hierdurch die

Information, dass von der IP-Adresse des Besuchers der Webseite und damit dessen Gerät die jeweilige Webseite aufgerufen wurde.

IP-Adressen sind für den Betreiber einer Webseite ein personenbezogenes Datum, da sich darüber die Identität des Nutzers ermitteln lässt.

Das Landgericht München I hat sich mit der Rechtmäßigkeit des Einsatzes von Google Fonts befassen müssen (Urteil v. 20.01.2022 – 3 O 17493/20). Der Nutzer einer Internetseite hatte den Betreiber der Seite verklagt, es zu unterlassen, seine dynamische IP-Adresse an Google weiterzuleiten. Das Gericht hat den Unterlassungsanspruch anerkannt: Für die erneute Zuwiderhandlung wurde ein Ordnungsgeld iHv. 250.000 EUR festgesetzt. Außerdem wurde dem Nutzer für die unzulässige Weiterleitung der IP-Adresse noch ein Schadensersatz iHv. 100 EUR auf Basis von Art. 82 Abs. 1 DSGVO zugesprochen.

Auch die CNIL kommt in Ihrem Verfahren zu einem nicht datenschutzkonformen Einsatz eines Google-Produkts, hier von Google Analytics. Nach Ansicht der CNIL sei der Einsatz von Google Analytics auf Webseiten mit europäischen Besuchern nicht mit der Datenschutz-Grundverordnung (DSGVO) vereinbar. Wer das Statistikprogramm nutze, verstoße gegen die Vorgaben des Gesetzes zur Datenübermittlung. Google habe für den Transfer in die USA zwar zusätzliche Schutzmaßnahmen ergriffen. Diese reichten aber nicht aus, "um den Zugriff auf diese Daten durch US-Geheimdienste auszuschließen". Damit schlägt die CNIL in die gleiche Kerbe wie schon die österreichische Datenschutzbehörde.

Praxishinweis: Solange es keine Anerkennung des Datenschutzniveaus der USA durch die EU gibt, setzen sich europäische Unternehmen, die Produkte US-amerikanischer Unternehmen im Einsatze haben, die personenbezogene Daten ihrer Nutzer/Kunden in die USA transferieren bzw. einen Zugriff durch US-Behörden nicht verhindern (können), dem Risiko der gerichtlichen und aufsichtsbehördlichen Ahndung durch Schadensersatz- und Bußgeldforderungen aus.

Die beiden Fälle zeigen, dass die Risiken von Sanktionen immer konkreter werden.

Laut Pressebereichten fordert Google nun, dass endlich eine Nachfolgeregelung für das EU-US Privacy Shield in Kraft tritt. Bis eine solche Nachfolgeregelung in Kraft tritt, empfehlen wir in Bezug auf die obigen Tools folgendes:

1. Google Fonts lassen sich auch in einer Variante einsetzen, in der die Fonts selbst gehostet werden und damit IP-Adresse nicht in die USA weitergeleitet werden.
2. Anstelle von Google Analytics sollte auf andere Tools (z.B. Matomo in einer selbst in der EU gehosteten Variante) umgestellt werden.

Literaturhinweis: „Datenschutz ist Chefsache“

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat seinen Datenschutz-Leitfaden für kleine und mittlere Unternehmen (KMU) unter dem Titel „Datenschutz ist Chefsache“ in einer 2. Auflage vorgelegt. Die Auflage ist online kostenlos unter folgendem Link abrufbar:

https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Materialien/KMU/Datenschutz_ist_Chefsache.pdf

Die Broschüre ist als Orientierungshilfe gedacht. Auf 95 Seiten finden Sie hier in 18 Kapiteln grundlegende Informationen zu Fragestellungen, die in kleinen und mittleren Unternehmen relevant sein können. In den jeweiligen Kapiteln gibt es Hinweise zu vertiefenden, mitunter sehr ausführlichen Quellen, hilfreichen Formularen, Vorlagen usw., die ebenfalls auf der Homepage des Landesbeauftragten Sachsen-Anhalt eingesehen werden können.

Praxishinweis: Die Ressourcen für den Datenschutz sind begrenzt. Für die Umsetzung einer Datenschutzorganisation in einem Unternehmen, auch unter Einsatz externe Berater, bedarf der Unterstützung durch die Unternehmensleitung: Datenschutz ist Chefsache! Aus unserer Sicht ist der neu aufgelegte Leitfaden eine gute Handreichung für Geschäftsleitungen, sich einen Überblick zu relevanten Themen zu machen bzw. auftretende Themen einordnen zu können. Schauen Sie sich es an.

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