Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

die technischen Vorteile der Digitalisierung und Vernetzung schaffen gerade in der Pandemie sinnvolle Lösungen, um die Geschäftstätigkeit auf alternativen Wegen fortzusetzen. Insbesondere im Bereich der Kollaborationstools hat in den letzten Monaten eine bemerkenswerte Entwicklung im Hinblick auf Anbieter und Funktionsumfang stattgefunden. Die dadurch verfügbaren Möglichkeiten der Zusammenarbeit per Chat, Videokonferenz usw. hat in vielen Unternehmen die Verlagerung der Arbeit vom Büro ins Homeoffice überhaupt erst möglich gemacht.

Die Datenpannen der vergangenen Monate und deren Folgen (Reputationsschäden, Sanktionen, Schadensersatzansprüche) machen uns jedoch deutlich, dass die Menschen im Umgang mit digitalen Daten noch nicht im erforderlichen Maß sensibilisiert sind. Es gibt nach unserer Beobachtung u.a. auch eine deutliche Diskrepanz was den Schutz von Daten auf Papier einerseits und elektronischen Daten andererseits angeht. Wie ist das bei Ihnen, legen Sie bei Bearbeitung von Unterlagen in beiden Welten die gleichen Maßstäbe an? Wie sieht es mit Bewerbungsunterlagen, Personalakten oder Krankmeldungen in elektronsicher Form aus, haben Sie hier auch deren Vertraulichkeit und Vernichtung nach Zweckerfüllung im Blick?

Wir jedenfalls sehen hier Nachschärfungsbedarf. Den Aktivitäten der Aufsichtsbehörden und Gerichte entnehmen wir, dass wir mit dieser Einschätzung nicht ganz falsch liegen. Wenn Aufsichtsbehörden und Gerichte aktiv werden, ist allerdings das Kind bereits in den Brunnen gefallen. Unsere Empfehlung: Beugen Sie vor! Wir unterstützen gern und laden Sie ein, die Themen dieser Ausgabe unter diesem Aspekt zu lesen. Wenn Sie also Fragen zu den Themen in dieser Ausgabe haben, melden Sie sich.

Ihr

Asmus Eggert

Inhalt

Homeoffice: Anforderungen an Arbeitgeber werden verschärft

Mit der Umsetzung der sog. Notbremse im Infektionsschutzgesetz werden Arbeitgeber unabhängig von der Inzidenz noch stärker in die Pflicht genommen. Aktuell sollen Arbeitgeber von Homeoffice-Angeboten nur noch dann absehen dürfen, wenn dem „zwingende betriebliche Gründe“ im Wege stehen. Arbeitnehmer wiederum müssen dieses Angebot annehmen, solange ihrerseits kein gravierender Grund dagegenspricht. Damit verschärft und manifestiert der Gesetzgeber die bisherige Regelung, die Arbeitgeber verpflichtet, den Beschäftigten im Fall von Büroarbeit oder vergleichbaren Tätigkeiten, das Arbeiten im Homeoffice anzubieten. Diese Regelung läuft bisher längstens bis zum Ablauf des 30.06.2021 (§ 28b Abs. 10 Infektionsschutzgesetz – IfSG)

Mit der Verschärfung werden also noch mehr Arbeitsplätze ins Homeoffice verlagert werden. Damit erhöht sich jedoch das Risiko für Arbeitgeber für Datenschutzverletzungen, wenn sie für das Homeoffice ihrer Mitarbeiter nicht die entsprechenden Rahmenbedingungen durch flankierende technische und organisatorische Maßnahmen schaffen. Kriminelle werden sich jedenfalls rasch auf die Schwächen der Auslagerung von Arbeitsplätzen ins Homeoffice einstellen und diese nutzen. Siehe zu dem Thema auch unseren Blog und die dort verlinkten Hinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Zu spät: Booking.com muss wegen deutlichem Überschreiten der 72 Stundenfrist Strafe zahlen

Die niederländische Datenschutzbehörde (Autoriteit Persoonsgegevens – AP) hat gegen Booking.com eine Strafe in Höhe von 475.000 Euro verhängt, weil das Portal erst 25 Tage nach einer Datenpanne die Aufsichtsbehörde informiert hatte.

Hintergrund der Datenpanne war, dass es 2019 Kriminellen gelungen war, sich über die Konten von Mitarbeitern von Hotels in den Vereinigten Arabischen Emiraten Zugriff auf Daten von 4109 Kunden zu verschaffen. Neben Namen, Adressen, Telefonnummern und Buchungsdetails konnten laut Pressemeldungen in 283 Fällen auch Kreditkarteninformationen eingesehen werden, in 97 Fällen sogar samt Sicherheitsnummer. Erst 25 Tage nachdem Booking.com von diesem Vorfall Kenntnis erlangte hatte, meldete das Portal den Vorfall. Die DSGVO hingegen schreibt vor, dass eine Datenpanne **binnen 72 Stunden** zu melden ist. Diesen Verstoß der verspäteten Meldung hat die Aufsichtsbehörde nun sanktioniert (Art. 83 Abs. 4a) i. V. m. Art 33 DSGVO).

Praxishinweis: Eine Datenpanne schwebt als abstrakte Gefahr beim täglichen Umgang mit personenbezogenen Daten stets über Verantwortlichen und Auftragsverarbeitern. Sie kann sich jederzeit realisieren. Wenn das der Fall ist, beginnt ab Kenntnis vom Vorfall die 72-Stunden-Frist zu laufen. Zögerliches Verhalten kostet hier stets kostbare Zeit. Melde- und Informationsprozesse müssen hier also unmittelbar in Gang gesetzt werden. Dies setzt voraus, dass die Prozesse vorher sauber definiert, implementiert und geschult wurden. Auch eine sofortige Einbindung des Datenschutzbeauftragten ist dringend zu empfehlen. Er kann mit einer qualifizierten Bewertung unterstützen und die Kommunikation mit Aufsichtsbehörden und ggfs. den Betroffenen organisieren.

Achtung: Die Frist läuft auch am Wochenende oder an Feiertagen. Wie die Frist berechnet wird, können Sie in unserem Blog nachlesen.

Verhältnis von Löschung und Anonymisierung nach DSGVO - Position des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

Bisher herrschte die Ansicht vor, dass die von der DSGVO gebotene Löschung personenbezogener Daten auch durch Anonymisierung dieser Daten erfolgen könne. Dazu hat sich nun der neue Hessische Beauftragte für Datenschutz und Informationsfreiheit jedoch wie folgt positioniert: In der

DSGVO gebe es keine Hinweise, dass Anonymisierung eine Datenlöschung ersetzen kann. Die Gleichsetzung wandele den Anspruch der betroffenen Person auf Datenbeseitigung in eine Erlaubnis des Verantwortlichen auf Veränderung und Weiterverarbeitung der Daten. Dogmatisch sei es daher nicht zu vertreten, dass die Anonymisierung ohne Einwilligung der betroffenen Person eine Löschung ersetzen kann.

Praxishinweis: Die DSGVO schützt personenbezogene Daten. Nach Art. 4 Nr. 1 DSGVO sind das alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Anonymisierung schließt eine Identifizierbarkeit per Definition aber gerade aus. Die Ansicht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit ist insofern durchaus diskutabel. So sieht die österreichische Aufsichtsbehörde es wiederum als angemessen an, eine Löschung durch Anonymisierung herbeizuführen. Im Kern ist aus unserer Sicht zu beachten, dass die voranschreitende Digitalisierung und immer stärkere Vernetzung immer neue Möglichkeiten schaffen, Daten zu re-anonymisieren. Das muss man als Verantwortlicher oder Auftragsverarbeiter im Blick behalten und bei der Anonymisierung beachten. Aus unserer Sicht besteht bei einer lege artis durchgeführten Anonymisierung kein Personenbezug mehr und die personenbezogenen Daten sind damit gleichzeitig als gelöscht zu betrachten. Gleichwohl werden wir die Entwicklung zum Thema Löschen und Anonymisieren für Sie weiter im Blick behalten.

BGH: Revisionsverfahren zum Schadensersatz wegen eines Datenlecks anhängig

Das Bundesverfassungsgericht hatte Anfang des Jahres klargestellt, dass deutsche Gerichte DSGVO-Schadenersatzansprüche nicht allein deshalb abweisen dürfen, weil sie nur Bagatellen betreffen (Beschluss vom 14.01.2021 – 1 BvR 2853/19).

Nach aktuellen Presseberichten muss der BGH nun über die Beweislastumkehr zugunsten der von Datenlecks Betroffenen entscheiden. Hintergrund war ein Datenleck bei Mastercard im Jahr 2019. Hier kursierten persönliche Daten wie Anschrift, Kontonummer, Telefonnummern und Mailadressen von Mastercard-Kunden im Internet. Tausende Betroffene hatten daraufhin Mastercard auf ein angemessenes Schmerzensgeld nach Art. 82 DSGVO verklagt. Ein Verfahren vor dem OLG Stuttgart liegt nun dem BGH zur Revision vor.

Praxishinweis: Grundsätzlich muss vor Gericht der Betroffene seinen Schaden beweisen. Falls der BGH nun allerdings zugunsten einer Beweislastumkehr entscheiden sollte, würde das entsprechende Schadensersatzklagen gegen Unternehmen erleichtern, weil nun wiederum die Unternehmen beweisen müssten, dass die Betroffenen durch den Datenschutzverstoß nicht geschädigt wurden. Als Folge dürfte die Zahl der DSGVO-Verfahren deutlich zunehmen und sich damit das Haftungsrisiko für Unternehmen erhöhen. Das Thema DSGVO-Schadensersatzanspruch bleibt somit spannend. Wir werden auch hier weiter berichten.

DSK: Praxistaugliche Lösungen zur Kontaktnachverfolgung in der Pandemie

In einer Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 26.03.2021 hat diese im Hinblick auf die Kontaktverfolgungs-App Luca auf die notwendige Verbindung von praxistauglichen Lösungen mit einem hohen Schutz personenbezogener Daten hingewiesen.

Hintergrund der Stellungnahme zur Verarbeitung der Kontaktdaten von Kunden, Gästen oder Veranstaltungsteilnehmern war ein entsprechendes Ersuchen der Culture4life GmbH als Betreiberin der Luca-App bei mehreren Aufsichtsbehörden. Ferner haben einige Länder und Landkreise die Absicht, diese App einzuführen und dann eine Verbindung zu den jeweiligen Gesundheitsämtern herzustellen.

Die DSK hat dabei noch einmal deutlich darauf hingewiesen, dass die digitalen Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten datenschutzkonform betrieben werden müssen. Um eine bundesweit einheitliche datensparsame digitale Infektionsnachverfolgung zu ermöglichen, fehle es bislang allerdings an gesetzlichen Regelungen. Hierfür sollten bundeseinheitliche normenklare Vorgaben zur digitalen Kontaktnachverfolgung geschaffen werden.

Die DSK hat angekündigt, eine eigenständige Orientierungshilfe für alle Betreiber von Kontaktverfolgungssystemen mit allgemeinen Anforderungen für die digitale Kontaktnachverfolgung zu erarbeiten und kurzfristig zu veröffentlichen.

Praxishinweis: Ein Baustein der Pandemiebekämpfung ist die Kontaktnachverfolgung. Oft ist die konkrete Umsetzung nicht datenschutzkonform. Wer kennt nicht die Listen, die allenthalben ausliegen und in denen man studieren kann, wer bereits Gast/Kunde gewesen ist? Auch die Luca-App sieht sich diverser Kritik, u.a. vom Chaos Computer Club, ausgesetzt.

Dass für die Unternehmen digitale Lösungen eine deutliche Arbeitserleichterung darstellen, ist offensichtlich. Es zeichnet sich zudem ab, dass Lockerungen zukünftig oft an Nachweise (Impfung, negativer Corona-Test etc.) gebunden werden. In der Umsetzung ergeben sich somit Dokumentations- und Nachweispflichten. Dann stellt sich konsequenterweise die Frage nach einem angemessenen Datenschutz. Datenschutz soll und darf hier kein Hemmschuh sein. Allerdings ist es in unser aller Interesse, das bestimmte Rahmenbedingungen eingehalten werden.

Aus unserer Sicht geht es im Kern darum, pragmatische Lösungen zu schaffen und gleichzeitig datenschutzrechtliche Aspekte ausgewogen zu berücksichtigen. Oft genug wird Datenschutz auch als Ausrede genutzt. Wir sind der festen Überzeugung, dass innovative Ansätze und Datenschutz sich durchaus vereinbaren lassen. Wenn Sie für Ihre Ideen Unterstützung benötigen, sprechen Sie Ihren Berater gerne an.

Vorangegangene Ausgaben der mip Beratungsinformation können Sie online auf unserer Seite abrufen: https://www.sofortdatenschutz.de/exklusiver-downloadbereich/

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