Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

ich hoffe, Sie sind alle gesund und wohlbehalten ins Neue Jahr gekommen.

Leider begleitet uns die Coronapandemie weiterhin und stellt Unternehmen und Organisationen vor die Herausforderung, die wechselnden Maßnahmen und Anforderungen datenschutzkonform umzusetzen. Daher haben wir auch in dieser Ausgabe wieder zwei Corona-Themen für Sie aufbereitet.

Da die EU mit den USA noch immer keine Lösung für einen datenschutzkonformen Datentransfer erzielt hat, gelten die Einschränkungen der Schrems-II-Entscheidung des Europäischen Gerichtshofs weiter. In der Praxis sind damit Datentransfers, insbesondere zu US-Cloud-Diensten, datenschutzrechtlich kritisch und gönnen als Folge allen Beteiligten keine Atempause. Sie finden zu dieser Thematik einen Artikel zu Cloudanbietern und einen zu Cookie-Diensten.

Technische und organisatorische Maßnahmen (TOM) gehören gem. Art. 32 DSGVO zum Pflichtprogramm im Datenschutz. Zum sicheren, verschlüsselten Datentransfer hat die Datenschutzkonferenz (DSK) Ende des letzten Jahres einen richtungsweisenden Beschluss gefasst, den wir Ihnen vorstellen möchten.

Außerdem weisen wir auf das Thema Offboarding von Mitarbeitern und Dienstleistern sowie auf eine Entscheidung des Bundesgerichtshofs (BGH) hin, die sich mit einem Bewertungsportal für Ärzte befasst hat.

Ich wünsche Ihnen eine interessante Lektüre!

Ihr

Asmus Eggert

Inhalt

Corona 1: Umsetzung der 3-G-Regelung – Hinweise und Orientierung

In der letzten Beratungsinformation hatten wir Ihnen erste Hinweise zur Umsetzung der 3-G-Regelung als Arbeitgeber:in an die Hand gegeben. Aus unseren Beratungsgesprächen wissen wir jedoch, dass sich in der Umsetzung weiter Unsicherheiten und Fragen ergeben, die nicht unmittelbar durch das Infektionsschutzgesetz, die Testverordnung, das BDSG oder die DSGVO beantwortet werden.

Es gibt zwar inzwischen von den Aufsichtsbehörden und seit Ende Dezember auch von der Datenschutzkonferenz (DSK) Orientierungshilfen und weiterführende Informationen. Leider bieten all diese offiziellen Informationsquellen nicht immer passende Umsetzungshinweise für Unternehmen und Organisationen.

Grundsätzlich müssen Arbeitgeber:innen 3-G-Nachweise der Beschäftigten täglich vor deren Zugang zum Arbeitsplatz kontrollieren und die Kontrollen dokumentieren. Nach dem Willen des Gesetzgebers soll es möglich sein, dass bei geimpften und genesenen Personen das Vorhandensein eines gültigen Nachweises nur einmal erfasst und dokumentiert werden muss. Wenn also der Arbeitgeber den Impf- oder Genesenenstatus einmal kontrolliert und diese Kontrolle dokumentiert hat, können Beschäftigte mit gültigem Impf- oder Genesenenstatus anschließend von den täglichen Zugangskontrollen ausgenommen werden. Das hatten wir Ihnen bereits in unserer Dezember Ausgabe mitgeteilt.

In der konkreten Umsetzung der Kontrollerleichterung stellt sich nun die Frage, ob insbesondere eine differenzierte Erfassung der Status beim Erfassen der 2-G-Nachweise möglich ist. Die Datenschutzkonferenz (DSK) kommt zum Schluss, dass eine Erfassung des 2-G-Nachweises (geimpft oder genesen) nur durch eine Einwilligung des Beschäftigten möglich ist. Auf Basis der Einwilligung empfiehlt die DSK weiter, den 2-G-Nachweis in einer gesonderten Liste zu erfassen, allerdings ohne dabei nach genesen und geimpft zu unterscheiden (Grundsatz der Datensparsamkeit). Das Gültigkeitsdatum dürfe jedoch erfasst werden.

Die nach der Veröffentlichung aufgekommene Diskussion über die Gültigkeit des Genesenenstatus und auch des Impfschutzes macht es aus unserer Sicht für das Aufrechterhalten der Kontrollvereinfachung erforderlich, dass statt des Gültigkeitsdatums das Ausstelldatum erfasst wird und auch die Art des Nachweises. Nur so können Arbeitgeber:innen nachvollziehen, ob die Zutrittsvoraussetzung (unter wechselnden Bedingungen, aktuell u.a. Verkürzung der Gültigkeit des Genesenenstatus von 6 auf 3 Monate) für den jeweiligen Beschäftigten noch vorliegt.

Weitere Informationen zu dem Komplex finden Sie über die nachfolgenden Links:

https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf

https://www.bmas.de/DE/Corona/Fragen-und-Antworten/Fragen-und-Antworten-ASVO/faq-corona-asvo.html

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/11/Orientierungshilfe-3G_Arbeitsplatz.pdf

https://www.lda.bayern.de/media/veroeffentlichungen/FAQ-Sammlung_zur_Verarbeitung_von3G-3G_plus-2G.pdf

https://www.datenschutz-bayern.de/datenschutzreform2018/aki38.html

https://www.datenschutz-bayern.de/datenschutzreform2018/AP_Impfstatus.pdf

Sollten Sie noch Fragen haben, helfen unsere Berater:innen Ihnen gerne weiter. Auch Muster für Einwilligungen und Erfassungsvorlagen, stellen unsere Berater:innen bei Bedarf gern zur Verfügung.

Corona 2: Datenschutzkonformes Auslesen und Prüfen digitaler Nachweise

Impfungen und Testergebnisse, die digital vorgelegt werden, können auch digital überprüft werden. Viele erleben das inzwischen bei Besuchen von Veranstaltungen, Restaurants, Frisören etc. Natürlich können auch Arbeitgeber:innen digital prüfen. Dazu kann zum Beispiel die kostenlose CovCheckPass-App des RKI genutzt werden (https://www.digitaler-impfnachweis-app.de/covpasscheck-app/). Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat dazu eine „Aktuellen Kurz-Information" (AKI) veröffentlicht und sich darin wie folgt positioniert:

- *Ein gesicherter digitaler Impfnachweis ist nur im QR-Code enthalten und kann zuverlässig mit technischen Hilfsmitteln geprüft werden.*
- *Zur Prüfung kann die CovPassCheck-App verwendet werden. Die CovPass-App oder die Corona-WarnApp darf dafür nicht verwendet werden.**
- *Bei der Prüfung muss der Grundsatz der Datenminimierung beachtet werden* [u.a. keine Speicherung des verwendeten Impfstoffs, Anm. mip].

*Anm. mip zum Hintergrund: Für eine Prüfung ist ausschließlich eine Prüf-App zu nutzen (CovPassCheck) und nicht eine App, die zum Speichern der Zertifikate verwendet wird (CovPass- oder CoronaWarn-App), da ansonsten die Zertifikate nicht geprüft, sondern auf dem Mobiltelefon der prüfenden Person dauerhaft gespeichert werden.

Praxishinweis: Für das Testen sollte nur dienstliche Hardware eingesetzt werden. Es muss in jedem Fall sichergestellt sein, dass mit der Prüfung keine Daten auf privaten Mobiltelefonen/Smartphones gespeichert werden.

DSK: Kein Verzicht des Betroffenen auf Verschlüsselung des Datenaustauschs

Im digitalen Austausch von personenbezogenen Daten zwischen Unternehmen (Steuerkanzleien, Lohnbuchhaltungsbüros, Abrechnungsstellen) und Betroffenen (Mandant:inn, Kund:innen) ist grundsätzlich ein datenschutz-konformer Datentransfer sicher zu stellen. In den vorangegangenen Ausgaben der mip Beratungsinformation hatten wir z.B. auf die Probleme des Faxens und auf die Möglichkeiten eines verschlüsselten Datenaustauschs per E-Mail hingewiesen. Dennoch sehen sich Verantwortliche mit „genervten" Betroffenen konfrontiert, die sich bewusst für den „komfortablen", unverschlüsselten Austausch und gegen die Datenschutzkonformität entscheiden.

Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen hat die Datenschutzkonferenz DSK am 24.11.2021 folgendes beschlossen:

1. *Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten,* ***die nicht zur Disposition der Beteiligten*** *stehen.*
2. *Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.*
3. *Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.*

4. *Kapitel V der DSGVO (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) bleibt hiervon unberührt.*

Praxishinweis: Alle Unternehmen und Organisationen, die in der Vergangenheit dem Wunsch der Betroffenen nachgekommen sind, eine Lösung (z.B. informierte Einwilligung) zum unverschlüsselten Datentransfer zu ermöglichen, sollten dieses Vorgehen in Anbetracht des DSK-Beschlusses erneut prüfen und idealerweise sichere Alternativen evaluieren (Download von Dokumenten über eine gesicherte Verbindung anstatt Dokumentenversand als E-Mail-Anlage).

Darf ein amerikanischer Cloud-Anbieter eingesetzt werden, wenn dieser die Daten in der EU hostet?

U.a. als Folge der Schrems-II-Entscheidung des Europäischen Gerichtshofes (EuGH) wurden die EU Standardvertragsklauseln überarbeitet und sind nunmehr ausschließlich in ihrer aktuellen Version zur Rechtfertigung einer Datenübermittlung in die USA oder anderer Drittstaaten ohne Angemessenheitsbeschluss einzusetzen. Die aktuelle Fassung der Standardvertragsklauseln berücksichtigt die Schrems-II-Rechtsprechung. Die Klauseln 14 und 15 der Standardvertragsklauseln legen dem Verantwortlichen eine sehr umfangreiche und zu dokumentierende Prüfung auf, ob der Vertragspartner die Klauseln auch tatsächlich einhalten kann oder ob die Rechtslage oder Rechtspraxis im Drittland dies „verhindert". Der EuGH hat für die USA in dem vorgenannten Urteil bereits entschieden, dass hier zusätzliche Maßnahmen erforderlich sind, um das Datenschutz-Niveau der DSGVO wieder herzustellen. Diese Maßnahmen müssen nach derzeitiger allgemeiner Ansicht technischer Natur sein, da vertragliche Vereinbarungen zwischen den Parteien gerade nicht gegenüber den amerikanischen Behörden wirken und daher deren Zugriff nicht verhindern können. Das kann auch nicht damit umgangen werden, dass die Daten durch US-amerikanische Unternehmen ausschließlich innerhalb der EU gespeichert werden. Aufgrund des sog. CLOUD-Acts können die amerikanischen Behörden unabhängig vom Speicherort auf die Daten zugreifen können, sobald ein amerikanisches Unternehmen beteiligt ist.

Praxishinweis: Um Daten in einer Cloud eines US-Dienstleister datenschutzkonform zu verarbeiten, sind die Daten so zu verschlüsseln, dass nur der Verantwortliche den Schlüssel kennt. Dabei dürfen die Daten beim US-Cloud-Anbieter zu keinem Zeitpunkt unverschlüsselt / entschlüsselt vorliegen.

BGH: Ärzte haben keinen Unterlassungsanspruch auf Veröffentlichung ihres Profils im Bewertungsportal Jameda

Der Bundesgerichtshof (BGH) hat mit Urteil vom 12.10.2021, Az.VI ZR 488/19 und VI ZR 489/19 entschieden, dass Ärzte keinen Anspruch auf Unterlassung der Veröffentlichung von Profilen auf dem Ärztebewertungsportal „Jameda" haben.

Das Online-Bewertungsportal „Jameda" erstellt mit Daten aus allgemein zugänglichen Quellen Basisprofile für Ärzte mit Namen, akademischem Grad, Fachrichtung, Praxisanschrift, weiteren Kontaktdaten und Sprechzeiten und veröffentlicht diese auf dem Portal. Die Nutzer können die Ärzte nach vorgegebenen Kriterien benoten und in Freitexten bewerten. Aus allen Benotungen wird eine Gesamtnote errechnet und auf dem jeweiligen Arzt-Profil angezeigt. Kostenpflichtig bietet „Jameda" den im Portal erfassten Ärzten die Möglichkeit an, ihre Profilseiten – etwa durch Hinzufügen eines Fotos, Setzen eines Links auf die eigene Internetseite oder die Veröffentlichung von Fachartikeln – zu gestalten. Zwei Ärzte, die nicht in das Portal aufgenommen werden wollten und daher auch keine kostenpflichtige Lösung in Anspruch nahmen, hatten gegen Jameda geklagt und die Unterlassung der Aufnahme in das Portal sowie die vollständige Löschung ihrer Profile und Daten gefordert.

Der BGH verneinte in seinem Urteil den Unterlassungsanspruch.

Eine Löschung komme in Betracht, wenn Art. 17 Abs. 1 DSGVO erfüllt sei. Die Voraussetzungen des Unterlassungsanspruchs aus Art. 17 Abs. 1 DSGVO seien vorliegend jedoch nicht erfüllt. Keiner der dort genannten Löschungs- beziehungsweise Unterlassungsgründe sei gegeben. Dies gelte insbesondere auch für die Löschungs- beziehungsweise Unterlassungsgründe des Art. 17 Abs. 1 Buchst. c DSGVO (berechtigter Widerspruch) und des Art. 17 Abs. 1 Buchst. d DSGVO (unrechtmäßige Verarbeitung).

Insbesondere scheitere der Anspruch daran, dass die streitige Datenverarbeitung rechtmäßig gem. Art. 6 Abs. 1 S. 1 lit. f. DSGVO sei. Denn mit dem Portalbetrieb und der damit verbundenen Verarbeitung der genannten personenbezogenen Daten der Ärzte verfolge Jameda berechtigte, von Art. 11 GRCh (Freiheit der Meinungsäußerung und Informationsfreiheit) und Art. 16 GRCh (unternehmerische Freiheit) geschützte Interessen. Zudem gehe die Datenverarbeitung über das dafür unbedingt Notwendige nicht hinaus und die durchzuführende Abwägung der nach den konkreten Umständen des Einzelfalls gegenüberstehenden Rechte und Interessen falle nicht zu Gunsten der Ärzte aus.

Praxishinweis: Bewertungsportsportale haben für Organisationen stets zwei Seiten: Sind die Bewertungen gut, sieht man dies als kostenloses Marketing. Gibt es hingegen schlechte Bewertungen oder wird man in einen Kontext gestellt, der nicht gewünscht ist, sollen die Daten vom Portal gelöscht werden. Es sollte daher der Umgang mit schlechten Bewertungen geprüft werden. Dazu zählt auch das Ausschöpfen der Möglichkeiten des Art. 17 Abs. 1 DSGVO.

VG Wiesbaden untersagt Hochschule RheinMain die Nutzung von Cookiebot auf deren Webseite

Für die Umsetzung der Anforderung an das Setzen von Cookies und Trackern sowie das damit verbundene sog. Consent-Management setzen Webseitenbetreiber oft Cookie-Dienste ein. Diese ermöglichen es, die erforderlichen Einwilligungen der Nutzer:innen einer Webseite in die Cookie-Verwendung einzuholen, überwachen die eingesetzten Cookies und blockieren die Cookies und Tracker, für die der Nutzer keine Zustimmung erteilt hat.

Das VG Wiesbaden hat der Hochschule RheinMain mit Beschluss vom 01.12.2021 im Wege der einstweiligen Anordnung untersagt, den Dienst *„Cookiebot“* zum Zweck des Einholens von Einwilligungen in der Weise einzubinden, dass personenbezogene oder -beziehbare Daten der Nutzer:innen (einschließlich deren/dessen IP-Adresse) an Server übermittelt werden, die von einem externen Unternehmen betrieben werden. Die Verarbeitung dieser Daten erfolge auf Servern eines Unternehmens, dessen Unternehmenszentrale sich in den USA befinde. Der hierdurch gegebene Drittlandsbezug (hier USA) sei im Hinblick auf die sog. Schrems-II-Entscheidung des Europäischen Gerichtshofs (EuGH) so unzulässig. Grund: Die Nutzer:innen der Webseite der Hochschule würden weder um ihre Einwilligung für eine Datenübermittlung in die USA gebeten, noch fände eine Unterrichtung über die mit der Übermittlung verbundenen möglichen Risiken durch den sog. CLOUD-Act statt. Die Datenübermittlung sei für die Hochschule zum Betrieb der Website auch nicht erforderlich.

Praxishinweis: Solange die EU mit den USA keine tragfähige Nachfolgelösung des EU-US-Privacy-Shields vereinbart hat, ist der Datentransfer zwischen EU und USA für Unternehmen und Organisationen herausfordernd. Die Entscheidung des VG Wiesbaden setzt die EuGH Entscheidung zu Schrems II um. Die Fortsetzung der Nutzung von US-Dienstleistern ist derzeit datenschutzkonform nur möglich, wenn Maßnahmen getroffen werden, die das europäische Datenschutzniveau auch in der Zusammenarbeit sicherstellen (z.B. durch Verschlüsselung siehe oben). Alle Verantwortlichen sollten sich daher im ersten Schritt Klarheit darüber verschaffen, ob und an welcher Stelle sie Cookiebot oder vergleichbare Dienste im Einsatz haben. Ist das der Fall, sind die Möglichkeiten von Datenschutz erhöhenden Maßnahmen zu prüfen. Fraglich ist jedoch, ob zusätzliche Maßnahmen bei

einem Cookie-Dienst überhaupt ergriffen werden können bzw. ob die damit verbundenen Aufwände im Verhältnis zum Nutzen des Dienstes stehen. Ggfs. ist zu einem anderen Dienst zu wechseln (Europa oder Land mit Angemessenheitsbeschluss).

LG München I: 2.500,- EUR DSGVO-Schadensersatz für Kunde von Broker Scalable Capital

Im Oktober 2020 teilte der Broker Scalable Capital seinen Kunden mit, dass es zu einem Datenschutzverstoß gekommen sei und unbekannte Dritte auf Daten der Kunden zugegriffen hätten (u.a. Ausweisdaten, Name und Adresse, Wertpapierabrechnungen, steuerliche Daten). Von der Panne waren geschätzt 30.000 Kunden betroffen. Ein Kunde hatte auf DSGVO-Schadensersatz geklagt und bekam vor dem LG München Recht: Das Gericht sprach dem Betroffenen einen Schadensersatz von 2.500,- EUR zu.

Grund für den Schadensersatz ist aus Sicht des Gerichtes die Verletzung von Sorgfaltspflichten nach Art. 32 DSGVO. Diese habe das Unternehmen verletzt, weil es die Passwörter, mit denen ein IT-Dienstleister Zugang auf die Systeme von Scalable Capital hatte, nach Vertragsbeendigung nicht geändert hatte und dieser daher weiterhin auf die personenbezogenen Daten in den Systemen zugreifen konnte.

Praxishinweis: Zum Datenschutzmanagement gehört es, nicht nur Onboarding-Prozesse, sondern auch Offboarding-Prozesse zu implementieren. Das gilt für Beschäftigte aber, das zeigt das Beispiel, auch für Dienstleister. Dazu gehört es, mit Beendigung der Zusammenarbeit die Zugangs- und Zugriffsberechtigungen zu löschen oder zu sperren. Rollen und Rechte auf Systeme müssen stets klar zugeordnet sein und der aktuellen Aufgabenzuordnung der jeweiligen Mitarbeiter entsprechen (Umsetzung des Need-To-Know-Prinzips). Dies gilt im Übrigen z.B. auch bei Stellenwechseln innerhalb einer Organisation.

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