Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

nach wie vor gibt es keine abschließende Bewertung der datenschutzkonformen Alternativen zum Datenaustausch mit US-amerikanischen Unternehmen nach dem Wegfall des EU-US Privacy Shields. Es dürfte kaum ein Unternehmen in Europa geben, das keine IT-Produkte im Einsatz hat, die direkt oder indirekt Daten zu US-Unternehmen transferieren. Daher ist guter Rat gefragt. Wir geben Ihnen aktuelle Hinweise zu möglichen Lösungsansätzen.

In unserer Beratungspraxis stellen wir fest, dass der Beschäftigtendatenschutz an Bedeutung gewinnt. Neben dem Einsichtsrecht in die Personalakte nutzen Beschäftigte nun auch das Auskunftsrecht nach Art. 15 DSGVO. Wir haben einen Praxishinweis in diese Beratungsinformation aufgenommen.

Ferner finden Sie in dieser Ausgabe zwei Beiträge zur Datensicherheit mittels technischer und organisatorischer Maßnahmen (sog. TOM): Zum einen wollen wir Sie auf Handlungsbedarfe bei adhoc eingerichteten mobilen Arbeitsplätzen aufmerksam machen. Zum anderen zeigt ein aktueller Fall der Aufsichtsbehörde Baden-Württemberg, dass die TOM ein Aufgabenfeld darstellen, das kontinuierliche Verbesserungen in dem präventiven Schutz verlangt. Vernachlässigt man dies als Verantwortlicher oder als Auftragsverarbeiter, kann es teuer werden.

Ich wünsche Ihnen eine anregende Lektüre!

Ihr

Asmus Eggert

Inhalt

Wegfall des EU-US Privacy Shields - Update

Die Diskussion zu den Folgen und den notwendigen Maßnahmen aufgrund des Wegfalls des EU-US Privacy Shields sind weiter in vollem Gang. Max Schrems, der mit seiner Klage vor dem EuGH erneut die Schwächen des US-amerikanischen Datenschutzes aufzeigen konnte, hat nachgelegt. Mit seiner Organisation „noyb“ hat er inzwischen gegen 101 Unternehmen Beschwerde erhoben, die sich einen Monat nach dem Urteil weiterhin auf das Abkommen berufen. Ob dieser Aufruf Nachahmer findet und es zu einer Beschwerdeflut kommt, wird sich zeigen. Die Aufsichtsbehörden werden mit oder ohne Beschwerden nicht untätig bleiben können.

Praxishinweis: Prüfen Sie, ob Sie direkt oder indirekt im Datenaustausch mit US-amerikanischen Unternehmen stehen. Hierzu können Sie an diese Dienstleister Fragebögen schicken. Wir haben entsprechende Muster, die Sie bei Ihrem Berater abfragen können. Klären Sie, ob sich die Unternehmen hinsichtlich der Einhaltung eines angemessenen Datenschutzniveaus weiterhin auf das EU-US Privacy Shield berufen. Dies wäre anzupassen. Es kann dabei nicht ungeprüft auf die Standardvertragsklauseln umgestellt werden. Im Zweifel ist der Datenaustausch einzustellen. Schauen Sie für weitere Details möglicher Maßnahmen in unseren Blog oder sprechen Sie Ihren Berater der mip an.

Auskunftsersuchen (Art. 15 DSGVO) von Beschäftigten beim Arbeitgeber

In § 83 Abs. 1 BetrVG ist im deutschen Recht das Einsichtsrecht in die Personalakte verankert. Für leitende Angestellte ergibt es sich aus § 26 Abs. 2 SprAuG. Mit der DSGVO ist nun das Auskunftsrecht nach Art. 15 DSGVO dazu gekommen. Dass es dieses Recht auf eine allgemeine Datenauskunft gibt, ist inzwischen weitgehend bekannt. Das zeigt der Anstieg der Auskunftsersuchen, denen sich Unternehmen, Vereine und Einrichtungen stellen müssen. Wenn Beschäftigte dieses Auskunftsrecht für sich nutzen, stehen Arbeitgeber vor der Herausforderung, wie die parallel bestehenden Transparenzregelungen zu behandeln sind. Der Art. 15 DSGVO Auskunftsanspruch lässt offen, ob und in welchem Umfang das Beauskunftete auf Verlangen des Betroffenen/Beschäftigten auch „verkörpert“ als Kopie bzw. Ausdruck „auszuhändigen“ ist. Die Auskunftsbehörden vertreten hier keine einheitliche Auffassung. Eine höchstrichterliche Entscheidung zu dieser Frage steht noch aus.

Praxishinweis: Werden Sie als Arbeitgeber mit einem Art. 15 DSGVO-Auskunftsersuchen konfrontiert, binden Sie den Datenschutzbeauftragten ein. Bereiten Sie sich über die Datenschutzorganisation auf solche Anfragen vor. Schaffen Sie sich über das Verzeichnis der Verarbeitungstätigkeiten eine Übersicht, welche personenbezogenen Daten Sie von Mitarbeitern an welcher Stelle in welchen Systemen verarbeiten. In diesem Zusammenhang stellen Sie auch sicher, dass die Löschregeln umgesetzt werden und ihr Unternehmen den Löschpflichten nachkommt. Legen sich Muster an und halten Sie diese aktuell. Wenn Sie Unterstützung benötigen, sprechen Sie Ihren Berater an.

Überprüfung der adhoc eingerichteten Homeoffice-Lösungen

Der Lockdown zur Eindämmung der Covid-19 Pandemie im März dieses Jahres hat zu einer massiven Verlagerung von Arbeitsplätzen in den privaten Bereich von Arbeitnehmer geführt. Wir hatten hierzu bereits in der Beratungsinformation April informiert.

Die kurzfristig ergriffenen adhoc Lösungen sind vielfach unverändert im Einsatz. Auch wenn nach der Beendigung des Lockdowns die Rückkehr ins Büro nun grundsätzlich wieder möglich ist, bestehen Schutzmaßnahem wie das Abstandhalten und Hygienevorgaben weiter fort. Auch kann es sein, dass

die Maßnahmen wieder verschärft werden, falls die Infektionen im Herbst und Winter wieder ansteigen.

Das Arbeiten im Homeoffice bzw. mobiles Arbeiten werden die Unternehmen also weiterhin begleiten. Für den Datenschutz bedeutet das, dass sich die anfängliche adhoc Situation manifestiert hat. Als Folge sind die unter der Sondersituation erst einmal akzeptierten Risiken für die Verarbeitung personenbezogener Daten abzubauen. Die Unternehmen müssen also ihre technischen und organisatorischen Maßnahmen der neuen Situation anpassen. Dazu zählt das Erstellen von entsprechenden Verhaltensrichtlinien aber auch der datenschutzkonforme Einsatz der verwendeten Hard- und Software. Prominent diskutiert wird in diesem Zusammenhang die Auswahl von Videokonferenzsystemen und von Messengerdiensten für die Mitarbeiter sowie der Einsatz von Cloud-Diensten etc.

Praxishinweis: Prüfen Sie in Abstimmung mit Ihrem Datenschutzbeauftragten, welche adhoc-Maßnahmen noch gelebt werden. Passen Sie die Maßnahmen an, um die Kriterien für ein angemessenes Datenschutzniveau zu erfüllen, und schaffen Sie datenschutzkonforme Bedingungen. Ist das tatsächlich oder wirtschaftlich nicht möglich, suchen Sie nach Alternativen, die das Risiko minimieren. Denken Sie an die Dokumentation dieser Überprüfung.

Datensicherheit ist eine Daueraufgabe: Bußgeld in Höhe von 1,2 Mio. EUR verhängt

Die AOK Baden-Württemberg hatte in den Jahren 2015-2019 im Rahmen von Gewinnspielaktionen Einwilligungen für die Verwendung der personenbezogenen Daten für Werbezwecke eingeholt. In 500 Fällen kam es trotz getroffener technischer und organisatorischer Maßnahmen zur werblichen Ansprache von Betroffenen, die die Einwilligung nicht erteilt hatten. Nach Bekanntwerden hatte die AOK reagiert, in dem sie u.a. alle vertrieblichen Aktivitäten eingestellt hatte. Außerdem wurden in Abstimmung mit der Aufsichtsbehörde diverse weitere Maßnahmen ergriffen, um das Datenschutzniveau zu erhöhen. Dies hatte sich zwar positiv auf die Bemessung des Bußgeldes ausgewirkt, führte dennoch zu einem Bußgeld in Höhe von 1,24 Mio. EUR.

Praxishinweis: Die technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO sind regelmäßig Grund für Beanstandungen und Bußgelder durch die Aufsichtsbehörden. Die TOM sind daher in einen kontinuierlichen Verbesserungsprozess zu überführen. Oft wird auch von einem sog. PDCA-Zyklus gesprochen: planen, umsetzen, überprüfen, Folgemaßnahmen ergreifen (Plan, Do, Check, Act).

Der Fall zeigt, dass die TOM einen präventiven Charakter haben müssen. Maßnahmen, die erst nach einer Panne ergriffen werden und dann erst den Schutz für die Zukunft erhöhen, können trotzdem zu Bußgeldern führen. **Prüfen Sie regelmäßig,** ob in Ihren aktuellen Maßnahmen Risiken schlummern. Schließen Sie Lücken, verbessern Sie Maßnahmen und sorgen Sie für den aktuellen Stand der Technik.

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, Yanick Röhricht, 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 § 55 Abs. 2 RStV: Asmus Eggert