Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

die Corona-Beschränkungen werden schrittweise gelockert und endlich können wieder mit einer gewissen Zuversicht Urlaube geplant werden. Bevor nun die ersten Bundesländer in die Sommerferien starten, wollen wir Sie mit unserer Juni-Ausgabe der mip Beratungsinformation über aktuelle Datenschutz-Themen unterrichten.

Insbesondere für das Thema Datentransfers in Drittländer möchten wir Sie noch vor der Sommerpause sensibilisieren. Die deutschen Aufsichtsbehörden haben nämlich angekündigt, in einer koordinierten Aktion die Umsetzung der im Schrems-II-Urteil vom EuGH definierten Anforderungen an den Datentransfer in Drittländer (insbesondere in die USA) bei ausgewählten Unternehmen zu prüfen. Wir zeigen Ihnen, was Sie hier beachten müssen.

Die EU-Kommission hat Anfang Juni darüber informiert, dass sie neue Standardvertragsklauseln beschlossen hat. Was dies bedeutet, erfahren Sie ebenfalls in dieser Ausgabe.

Außerdem weisen wir auf eine Beschwerdekampagne der Datenschutzorganisation noyb gegen fehlerhafte Cookie-Banner hin sowie auf die geänderte rechtliche Bewertung der Datenübermittlung per Fax. Das ist ein Thema, das in vielen Unternehmen trotz der voranschreitenden Digitalisierung insbesondere beim Datenaustausch mit Behörden oder auch mit einzelnen Kunden noch Relevanz hat.

Wir halten Sie auf dem Laufenden!

Ihr

Asmus Eggert

Inhalt

Koordinierte Prüfung internationaler Datentransfers durch neun deutsche Aufsichtsbehörden

In seiner Entscheidung „Schrems II“ vom 16.07.2020 hatte der Europäische Gerichtshof (EuGH) festgestellt, dass die Übermittlung von personenbezogenen Daten in die USA nicht länger auf Basis des sogenannten Privacy Shields erfolgen kann. Wir hatten in diversen Ausgaben unserer mip

Beratungsinformation über die Auswirkungen dieser Entscheidung auf den Datentransfer in Staaten außerhalb der EU (Drittstaatentransfer) informiert.

Der EuGH hat in der genannten Entscheidung deutlich gemacht, dass die Aufsichtsbehörden unzulässige Transfers „aussetzen oder verbieten“ müssen. Ziel der Aktion von neun Aufsichtsbehörden (Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Niedersachsen, Rheinland-Pfalz und Saarland) ist es daher nun, diese definierte Anforderung um- und durchzusetzen, indem sie Unternehmen aus ihrem Zuständigkeitsbereich anschreiben und diese auffordern, einen von den Behörden abgestimmten Fragenkatalog schriftlich zu beantworten. Die Kompetenz für eine derartige Aktion der Aufsichtsbehörden ergibt sich aus Art. 58 Abs 1 lit. a DSGVO.

Es sollen insgesamt folgende 5 Bereiche befragt werden:

- Bewerberportale
- Konzerninterner Datenverkehr
- Mailhoster
- Tracking
- Webhoster

Eine Veröffentlichung der Fragenkataloge finden Sie z.B. hier. Laut Information aus den Aufsichtsbehörden entscheidet jede Aufsichtsbehörde individuell, in welchen dieser Themenfelder sie tätig wird. Die Rückmeldefrist soll laut der Aufsichtsbehörden der 09.07.2021 sein.

Dass die Entscheidung des EuGHs die Unternehmen als Verantwortliche und/oder Auftragsverarbeiter im Sinn der DSGVO vor große Herausforderungen stellt, ist auch den Aufsichtsbehörden klar. Dennoch haben die Behörden eine eindeutige Erwartungshaltung: Die Verantwortlichen müssen sich mit den neuen Anforderungen ernsthaft auseinandersetzen und eigenständig nach Lösungen suchen.

Sollte ein Unternehmen in den Antworten diese Anforderungen nicht plausibel belegen, wird die Aufsichtsbehörde die Prüfung ausweiten und ggfs. ein aufsichtsbehördliches Verfahren mit dem Ergebnis von Untersagungsverfügungen oder sogar Bußgeldern eröffnen.

Praxishinweis: Angeschriebene Unternehmen sollten die Beantwortung der Fragebögen in jedem Fall ernst nehmen und den Datenschutzbeauftragten unverzüglich einbinden. Die Beantwortung sollte mit Bedacht erfolgen (auch wenn die Fragebögen an sich erst eine Vorstufe zu einem aufsichtsbehördlichen Verfahren darstellen dürften und insbesondere, sofern ohne Rechtsbehelfsbelehrung versandt, zunächst auch keine Sanktionen für die Nichtbeantwortung verhängt werden dürfen). In jedem Fall sollten Sie – falls noch nicht geschehen - umgehend alle Drittlandübermittlungen überprüfen.

EU-Kommission: Neue Standardvertragsklauseln für den Austausch personenbezogener Daten beschlossen

Am 04.06.2021 gab die Europäische Kommission bekannt, dass sie zwei neue Sätze von Standardvertragsklauseln ("SVK") beschlossen habe, einen für die Verwendung zwischen Verantwortlichen und Auftragsverarbeitern und einen für die Übermittlung personenbezogener Daten in Drittländer. Die Kommission hob insbesondere hervor, dass die SVK die Anforderungen der DSGVO widerspiegelten und das Urteil des Gerichtshofs der Europäischen Union in der Rechtssache Datenschutzbeauftragter gegen Facebook Ireland Limited, Schrems II (C-311/18) berücksichtige, um ein hohes Datenschutzniveau für die EU-Bürger zu gewährleisten. Darüber hinaus wies die Kommission darauf hin, dass die neuen SVK auch die gemeinsame Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten, Rückmeldungen von Interessengruppen und die Stellungnahme der Mitgliedstaaten berücksichtigen.

Die überarbeiteten SVK schreiben erstmals Garantien vor, "um etwaige Auswirkungen der Gesetze des Bestimmungsdrittlands" auf die Einhaltbarkeit der Klauseln durch den Datenimporteur zu regeln. Dabei gilt es vor allem vorab zu klären, "wie mit verbindlichen Ersuchen von Behörden im Drittland nach einer Weitergabe der übermittelten personenbezogenen Daten umzugehen ist".

Die neuen SVK für die Übermittlung personenbezogener Daten in Drittländer folgen anders als bisher einem "modularen Ansatz". Das bedeutet, dass für jede der folgenden Situationen entsprechende Klauseln aus der Vorlage auszuwählen sind:

- EU-Verantwortlicher und Drittland-Verantwortlicher (Modul 1)
- EU-Verantwortlicher und Drittland-Auftragsverarbeiter (Modul 2)
- EU-Auftragsverarbeiter und Drittland-Unterauftragsverarbeiter (Modul 3 - Neu)
- EU-Auftragsverarbeiter und Drittland-Verantwortlicher (Modul 4 - Neu)

Die Modularität erhöht die Flexibilität, erschwert aber gleichzeitig die Anwendung.

Kennzeichnend für die neuen SVK ist, dass die von der Datenverarbeitung betroffenen Personen aus den Klauseln eigene Rechte gegen die Vertragsparteien ableiten und diese ggf. vor EU-Gerichten durchsetzen können. Eine pragmatische Neuerung ist zudem eine Klausel, die den Beitritt weiterer Parteien zu den SVK ermöglicht. Neu ist auch, dass die SVK eine Haftung der Parteien für Pflichtverletzungen nicht nur gegenüber den betroffenen Personen vorsehen, sondern auch im Verhältnis zueinander. Ob die Parteien diese Haftung im Innenverhältnis ausschließen oder zumindest begrenzen können, z.B. um sie an das ansonsten zwischen ihnen geltende Haftungsregime anzupassen, ist unklar.

Praxishinweis: Verantwortliche und Auftragsverarbeiter stehen nun vor folgenden zwei Herausforderungen:

1. Spätestens drei Monate nach Veröffentlichung der neuen SVK im EU-Amtsblatt dürfen Unternehmen bei neuen Verträgen die alten SVK nicht mehr verwenden.
2. Spätestens nach 18 Monaten ab Veröffentlichung der neuen SVK im EU-Amtsblatt müssen alle alten Verträge auf die neuen SVK umgestellt werden.

Allerdings gilt: Der simple Abschluss der SVK allein wird nicht ausreichen. Es ist weiterhin im Einzelfall zu prüfen, welchen Gesetzen der jeweilige Datenimporteur im Drittland und etwaige weitere Empfänger unterliegen und ob diese Gesetze, die von diesen mit Unterzeichnung der SVK gegebenen Garantien beeinträchtigen. Laut EuGH sind dann ggfs. zusätzliche Schutzmaßnahmen zu implementieren. Welche das sind, bleibt den Unternehmen überlassen. Gerade das ist aber eine große Herausforderung für die Unternehmen.

Um es deutlich hervorzuheben: Die neuen SVK sehen eine obligatorische Transfer-Folgenabschätzung vor, die von den Parteien durchgeführt werden muss. Beide Parteien müssen garantieren, dass sie keine Zweifel daran haben, dass das Land des Datenimporteurs den europäischen Standards genügt (was für US-Importeure schwer zu garantieren sein dürfte); diese Transfer-Folgenabschätzung muss dokumentiert und den Datenschutzaufsichtsbehörden auf deren Anfrage vorgelegt werden können.

Es ist daher weiterhin wünschenswert, dass es insbesondere der EU und den USA gelingt, eine Lösung über einen Angemessenheitsbeschluss zu finden. Erste politische Ansätze gibt es, siehe hier. Warten kann man darauf als Verantwortlicher und Auftragsverarbeiter jedoch nicht. Das Risiko der Prüfung durch eine Aufsichtsbehörde zeigen wir in unserem ersten Artikel dieser Ausgabe auf.

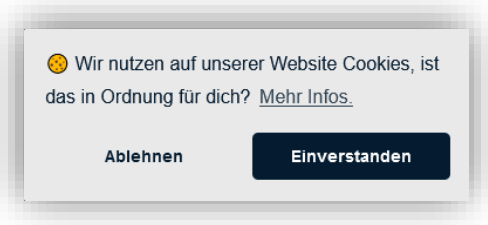
Beschwerdekampagne gegen Cookie-Banner

Die Datenschützer beschäftigen sich seit geraumer Zeit mit dem Thema Cookies. Die Kernfrage war und ist die Frage nach den Anforderungen an einen rechtskonformen Einsatz von Cookies und

insbesondere an die Einwilligung des Betroffenen. Diverse Anbieter haben sich am Markt mit Lösungen für Cookie-Banner und das dahinterliegende Management von Cookies bzw. Cookie setzenden Applikationen etabliert. Die Vielfalt der eingesetzten Cookie-Banner ist groß.

Nutzer:innen haben bei vielen Versionen ein Störgefühl, weil das „Abwählen“ von Cookies oder Trackern bewusst erschwert wird. Aktuell ist es fast schon Standard, dass das Abwählen von Cookies nicht durch einen einfachen Klick erfolgen kann. Stattdessen müssen Nutzer:innen erst in die Cookie-Einstellungen abtauchen und können dort dann Cookies abwählen.

Dem ist nun Max Schems mit seiner Datenschutzorganisation noyb nachgegangen. Er hat laut eigener Auskunft zahlreiche Unternehmen mit einer selbst entwickelten Software auf rechtswidrige Cookie-Banner untersucht. Die Software erkennt nach Bekundung von noyb die verschiedenen Arten von rechtswidrigen Cookie-Bannern und generiert automatisch Beschwerden. Die festgestellten Mängel werden zunächst den Unternehmen angezeigt und diese unter Fristsetzung von einem Monat zur Anpassung der Banner aufgefordert. Sollten die Unternehmen innerhalb der Frist nicht aktiv werden, will noyb Beschwerde bei den zuständigen Datenschutzbehörden erheben. In Deutschland sind aktuell unter anderem das Kaffee- und Versandhaus Tchibo und der Paketdienst DHL, aber auch Mittelständler wie Grohe oder Hunkemöller sowie der Europa-Park in Rust betroffen.



Ausnahme: Cookie-Banner von ComX.io mit direkter Ablehnen-Option, allerdings ist die Ablehnen-Option farblich nicht gleichwertig zur Einverstanden-Option realisiert

Für die Unternehmen kann sich durch den Einsatz automatisierter und damit kostengünstiger Prüfverfahren ein Sanktionsrisiko und in Deutschland auch ein zivilrechtliches Abmahnrisiko durch Verbraucherschutzorganisationen oder Verbraucherschutzanwält:innen realisieren. Die Beschwerdekampagne von noyb könnte also der Auslöser eine Beschwerdelawine werden. noyb selbst plant bis zu 10.000 Beschwerden zu produzieren.

Praxishinweis:

- Informieren Sie Ihre Nutzer:innen klar über die Zwecke, die hinter der Verwendung von Cookies stehen (z.B. Ausspielung personalisierter Werbung oder der Austausch von Informationen mit Social-Networking-Plattformen) sowie über die Identität der Betreiber:innen, die Cookies verwenden.
- Es sollten keine Voreinstellungen für die Nutzer:innen getroffen werden. Damit ist sichergestellt, dass Nutzer:innen eine aktive Entscheidung treffen können.
- Die Verweigerung der Verwendung von Cookies muss genauso einfach sein, wie deren Akzeptanz, d.h. die Nutzer:innen dürfen keinen komplexen Verfahren zur Ablehnung von Cookies unterworfen werden (simple Ja/Nein-Option).
- Vermeiden Sie bei der Gestaltung des Zustimmungsbuttons Gewichtungen, die manipulierenden Charakter haben (z.B. farblich hervorgehobener Button für die Zustimmung, hellgrauer Button für die Ablehnung).
- Es muss Nutzer:innen einfach möglich sein, die Zustimmung zur Verwendung von Cookies jederzeit zu widerrufen.
- Prüfen Sie beim Einsatz von Google Analytics, ob die Datenschutzinformation die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO abbildet und insbesondere auch, ob der Einsatz von

Google Analytics nach dem Schrems II Urteil des EuGH auf Ihrer Webseite weiter zulässig ist (siehe auch oben unser erster Beitrag). Ggf. bauen Sie in das Cookie-Banner eine Einwilligung für die Datenverarbeitung durch Google Analytics in den USA ein.

- Eine gute Checkliste zu den Anforderungen an Cookie-Banner hat die niedersächsische Aufsichtsbehörde veröffentlicht.

Datentransfer per Fax - nicht mehr Datenschutzkonform

Bis vor einiger Zeit wurde der Versand von Unterlagen mit personenbezogenen Daten per Telefax noch als relativ sichere Methode angesehen. Das hat sich mittlerweile geändert. In der Rechtsprechung hat sich u.a. das OVG Lüneburg im Beschluss vom 22.7.2020 – 11 LA 104/19 hierzu geäußert und die Übertragung per Fax als unsicher klassifiziert. Aber auch die Aufsichtsbehörden positionieren sich gegen die Übermittlung von personenbezogenen Daten per Fax. Eine entsprechende Einschätzung der Bremer Aufsichtsbehörde findet sich in einer Orientierungshilfe mit Stand Mai 2021.

Kern des Problems sei, so Gerichte und Aufsichtsbehörden, die Unkenntnis des Versendenden über die eingesetzte Technik auf der Empfangsseite. Vielfach sei das reale Faxgerät inzwischen durch digitale Lösungen abgelöst, die das Fax im Grunde zu einer E-Mail umwandeln. Ob und wie diese E-Mail verschlüsselt werde, könne die versendende Stelle nicht beeinflussen. Daher ist das Fax mit dem Schutzniveau einer unverschlüsselten E-Mail zu vergleichen.

Praxishinweis: 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 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.

Falls Sie Unterstützung benötigen, sprechen Sie Ihren Berater 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