Datenschutz News 2020 – 05

datenschutz-link.de
SABINE LINK
DATENSCHUTZBEAUFTRAGTE

Herzlich willkommen bei meinen Datenschutz-News, Ausgabe Oktober 2020

Datenübermittlung in die USA: EuGH-Urteil „Schrems II“

Der EuGH (Europäische Gerichtshof) hat durch sein Urteil vom 16.07.2020 (C-311/18, Volltext) die Regeln für die Übermittlung personenbezogener Daten in die USA grundlegend verändert. Das „Privacy Shield“-Abkommen zwischen EU und USA, das bisher die übliche Grundlage für Datenübermittlungen aus der EU in die USA war, wurde wegen grundsätzlicher Datenschutzmängel in den USA für unwirksam erklärt, mit sofortiger Wirkung. Für Datenübermittlungen in die USA ist „Privacy Shield“ keine zulässige Rechtsgrundlage mehr. Das „Privacy Shield“ enthielt die Festlegung der EU-Kommission, dass -unter bestimmten darin genannten Auflagen- bei Datenübermittlungen an Privacy-Shield-zertifizierte US-Unternehmen ein gemäß DSGVO angemessenes Datenschutzniveau gewährleistet würde.

„Privacy Shield“ ungültig

Das „Privacy Shield“ ist aber laut EuGH insbesondere deshalb nicht DSGVO-konform, weil alle Informationen, die in Cloud-Umgebungen amerikanischer Anbieter gespeichert werden, dem Zugriff von US-Regierungsbehörden unterliegen, um Überwachungsprogramme zum Zweck der Auslandsaufklärung durchzuführen. US-Regierungsbehörden können prinzipiell Zugriff auf diese Daten erhalten, auch wenn sie außerhalb der USA gespeichert werden. Alleine die Tatsache, dass eine amerikanische Firma die Daten speichert, reicht als Zugriffsberechtigung aus. US-amerikanische Unternehmen sind sogar dann zur Herausgabe der gespeicherten Informationen verpflichtet, wenn lokale Gesetze am Ort des Datenspeichers dies verbieten. Für diese nach amerikanischem Recht zulässigen Eingriffe gibt es nicht die aus Sicht der EU erforderlichen Einschränkungen und Garantien, und keinen im Sinne der EU effektiven gerichtlichen Rechtsschutz. Daher beurteilte der EuGH das „Privacy Shield“, das ein angemessenes Datenschutzniveau der Datenübermittlung an US-Unternehmen feststellt, für ungültig.

Rechtsgrundlage für Datenübertragungen in die USA mit sofortiger Wirkung entfallen

Kein angemessenes Datenschutzniveau in den USA

US-Überwachungsbehörden haben auf Anforderung Datenzugriffsrecht, kein ausreichender gerichtlicher Rechtsschutz

Sogenannte „Standardvertragsklauseln“ (Standard Contract Clauses SCC) stehen laut EuGH weiterhin als mögliche Rechtsgrundlage für Datenübertragungen aus der EU in die USA zur Verfügung, aber der EuGH verlangt, dass der Verantwortliche in diesem Rahmen eine Prüfung durchführt, ob tatsächlich ein angemessenes Datenschutzniveau eingehalten wird.

„Standard-vertragsklauseln“ bleiben eine mögliche Rechtsgrundlage für Datenübertragungen

Wegen dieser Einschränkung bewerten Datenschutzexperten die SCC für Datenübertragungen in die USA derzeit als Sackgasse: Wegen grundsätzlicher Datenschutzmängel in den USA gibt es dort kein angemessenes Datenschutzniveau, also seien SCC keine belastbare allgemeintaugliche Lösung. *****

Sabine Link – Datenschutzbeauftragte • Schulte-Marxloh-Str. 19 • 47169 Duisburg • info@datenschutz-link.de
Telefon 0176-8488 5082 oder 0203-3498 3045 • USt-Id DE298 214 620 • Nationalbank • DE20 3602 0030 0000 2490 68

Fast alle Unternehmen sind betroffen

Das EuGH-Urteil hat gravierende praktische Auswirkungen, denn fast alle Unternehmen und öffentliche Stellen nutzen Datenverarbeitungs-Dienstleistungen von US-Unternehmen, die bisher auf „Privacy Shield“ gestützt waren, hier nur einige Beispiele:

- Google Analytics, Google Fonts, Google-Ads etc.
- Office 365 oder Teams und OneDrive von Microsoft,
- Social Media wie Facebook, Twitter und Instagram,
- Videokonferenzsystem wie Zoom oder Teams,
- Amazon Web Service AWS,
- Hosting in US-amerikanischer Infrastruktur, z.B. MS Azur, Cloudflare

*****

Handlungsoptionen für Datenübermittlungen in die USA

Durch das EuGH-Urteil ist allen Datenübermittlungen, die auf das „Privacy Shield“ gestützt waren, die Rechtsgrundlage entzogen worden.

Verantwortliche sind also in der Misere, dass die weitere Datenübermittlung eine Verletzung der DSGVO darstellt und insbesondere ein Bußgeld auslösen kann, sofern die zuständige Aufsichtsbehörde tätig wird. Was also tun?

- An erster Stelle steht die Analyse, welche Datenübermittlungen in die USA überhaupt stattfinden.
- Zweiter Schritt: Sofern solche Dienste verzichtbar sind, können sie beendet werden, das ist die rechtssichere Lösung.
- Dritter Schritt: Falls eine Dienstleistung weiter genutzt werden soll, ist es erforderlich, alle Möglichkeiten auszuschöpfen, um Datenübermittlungen in die USA zu vermeiden, man muss also alle Möglichkeiten zur „datenschutzfreundlichen Gestaltung“ nutzen.

Alle zusätzlichen Aktionen sind Versuche der Risikominimierung, aber nicht rechtssicher. Das Dilemma in der Praxis ist: Wenn ein Dienst wie beispielsweise Microsoft 365 in einem Unternehmen genutzt wird, kann man das nicht abschalten, denn das wäre das Ende der Arbeitsfähigkeit.

- Man kann versuchen, ob für die verbleibenden Datenübermittlungen die Einwilligung der betroffenen Personen erfolgt. Die Einwilligung muss informiert erfolgen, d.h. die geplanten Datenübermittlungen und mögliche entstehende Risiken müssen detailliert und verständlich beschrieben werden, die Einwilligung muss ausdrücklich und nachweislich erfolgen, und sie kann jederzeit widerrufen werden. Die Formulierung eines Einwilligungstext ist in der Praxis immer ein Risiko, Rechtssicherheit gibt es nicht. Bei kremer-rechtsanwaelte.de gibt es ohne Gewähr einen Formulierungsvorschlag für die Einwilligung in Drittlandübermittlungen beim Webseiten-Besuch.
- Man kann ggf. argumentieren, die Daten würden durch den US-amerikanischen Dienstleister ausschließlich auf Servern in der EU verarbeitet und gespeichert, sodass keine Datenübermittlung in die USA stattfindet – allerdings ignoriert man damit, dass US-Unternehmen dem amerikanischen Recht unterworfen sind, also Daten auf Anforderung an die US-Regierungsbehörden herausgeben müssen, auch bei einer Datenspeicherung in der EU.

Enorme Praxis-Auswirkungen

Fast alle Unternehmen übertragen Daten in die USA im Rahmen von Dienstleistungen der großen amerikanischen Softwareanbieter

Unternehmen und öffentliche Stellen sind „Verantwortliche“ der Datenübermittlungen, sie müssen dafür eine gültige Rechtsgrundlage nachweisen.

Datenübermittlung ohne Rechtsgrundlage ist Bußgeldtatbestand

Bestandsaufnahme

Verzichtbare Dienste beenden

Bei weiter benötigten Diensten alle vermeidbaren Datenübermittlungen ausschalten: „Datenschutzfreundliche Gestaltung“

Umstellen auf eine neue Rechtsgrundlage:

Evtl. (selten) ist eine Einwilligung möglich

Evtl. kann der Dienst ausschließlich in der EU erbracht werden (aber dennoch ist Datenzugriff der US-Überwachungs-behörden möglich)

- Von einigen großen US-Unternehmen gibt es die Kundeninformation, beispielsweise von Microsoft für „Enterprise“- und „Education“-Kunden, dass mit Abschluss der jeweiligen Nutzungsverträge automatisch auch Standardvertragsklauseln abgeschlossen worden sind, die ja laut EuGH-Urteil prinzipiell als Rechtsgrundlage für die Datenübermittlungen geeignet seien, damit bestehe für die Kunden kein Problem. Aber leider ignoriert dies, dass in den USA nicht allgemein ein angemessenes Datenschutzniveau vorhanden ist, insbesondere wegen des möglichen Datenzugriffs der Überwachungsbehörden, sodass die Standardvertragsklauseln nicht generell rechtssicher geschlossen werden können.
- Man kann versuchen, eine IT-technische Gestaltung zu finden, bei der Daten zwar in die USA übertragen werden, um sie dort zu verarbeiten, aber jegliche Datenspeicherung nur auf eigenen Servern in der EU stattfindet. Ebenso wäre eine Gestaltung möglich, bei der durch den US-Dienstleister lediglich verschlüsselte Daten gespeichert werden, ohne Schlüssel-Zugriff des amerikanischen Unternehmens.

Umstellung auf Standardvertrags-klauseln als Rechtsgrundlage – aber fraglich ist das angemessene Datenschutzniveau

Speicherung von Daten druch amerikanische Unternehmen möglichst vermeiden, oder verschlüsselt speichern, nur alle anderen Verarbeitungen nutzen

Die Datenschutzaufsichtsbehörden bemühen sich um ein EU-weit einheitliches Vorgehen. Von den deutschen Aufsichtsbehörden der Bundesländer gibt es einige Veröffentlichungen, Datenübermittlungen in die USA werden sehr kritisch gesehen, auch bezüglich Microsoft 365. Dazu gibt‘s einen Beitrag der Datenschutzexpertin RA Nina Diercks: „Datenschutzbehörden stimmen Bewertung ‚Microsoft Office 365 sei nicht datenschutzgerecht einsetzbar‘ mehrheitlich zu. Ist damit der Einsatz von Office 365 in jedem Fall klar rechtswidrig? Spoiler: Nein“.

Datenschutzaufsichts-behörden der EU bemühen sich um ein einheitliches Vorgehen. Deutsche Aufsichtsbehörden sehen Datenübertragungen in die USA ohne Rechtsgrundlage sehr kritisch, keine offizielle „Bußgeld-Schonzeit“

Die Regierungsbehörden in den USA bemühen sich, zu einer Lösung beizutragen. HoganLovells berichtet vom „White Paper“, Stand September 2020, das gemeinsam von U.S. Department of Commerce, U.S. Department of Justice und Office of the Director of National Intelligence herausgegeben wurde. Darin werden Punkte aufgelistet, die aus amerikanischer Sicht in die Einzelfall-Abwägung über das „angemessene Datenschutzniveau“ seitens der Verantwortlichen (EU-Unternehmen und Behörden) einfließen sollten, sodass Standardvertragsklauseln eben doch eine valide Rechtsgrundlage der Datenübermittlung sein können. Insbesondere habe (frei übersetzt) „die überwältigende Mehrzahl von Unternehmen niemals eine Anordnung erhalten, Daten an die US-Behörden herauszugeben“, und „Unternehmen, die normale betriebliche Informationen wie Daten über Beschäftigte, Kunden oder Verkaufszahlen handhaben, hätten keinen Grund zu glauben, dass US-Sicherheitsbehörden beabsichtigen würden, diese Daten zu sammeln.“

White-Paper der US-Regierung mit Abwägungspunkten, wonach Standard-vertragsklauseln ein angemessenes Datenschutzniveau sichern: „Normale betriebliche Informationen“ seien kein Ziel der Überwachungsbehörden

Auch die EU-Kommission ist aktiv, in „wenigen Wochen“ sei ein Entwurf zu erwarten, der die Standardvertragsklauseln zu einer verlässlichen Basis der Datenübermittlung machen soll (EU-Justizkommissar Reynders, Privacy-Konferenz des IT-Verbands Bitkom am 28.9.2020, laut heise.de).

EU-Kommission bereitet Dokument vor, Standardvertrags-klauseln sollen verlässliche Rechts-grundlage für Daten-übermittlungen werden

Die rechtliche Auswertung und Reaktion auf das EuGH-Urteil läuft gerade erst richtig an. Verantwortliche müssen dennoch soweit wie möglich schnell handeln. *****

Cyber-Security-Monat Oktober

Passend zum Cyber-Security-Monat Oktober macht Microsoft in seinem „Digital Defense Report 2020“ auf die weitere Professionalisierung der Cyberkriminellen aufmerksam. Laut Microsoft hat sich der sogenannte CEO-Fraud als beliebte Angriffsmethode weiter etabliert. Dabei gelingt es Betrügern, Beschäftigte zu überzeugen, es gebe eine durch Vorgesetzte legitimierte Aufforderung zum Überweisen von Geldbeträgen. Unternehmen und deren Chefetage werden teils über Monate beobachtet, um letztlich mit überzeugend vorgespiegelten Formulierungen im Namen der Chef*in gezielt einzelne Beschäftigte per E-Mail aufzufordern, Geld zu überweisen. Durch raffinierte Methoden werden auch versierte und vorsichtige Nutzer hereingelegt.

Betrüger spionieren Unternehmen aus, um dann als vorgetäuschte Chefetage Beschäftigte aufzufordern, Geld zu überweisen. Immer raffiniertere Methoden, selbst misstrauische Nutzer werden hereingelegt

Auch Trojaner-Software zur Einschleusung von Schadsoftware, z.B. zwecks Verschlüsselung und Erpressung, wurde weiter „verbessert“. Der berüchtigte Trojaner „Emotet“ kann jetzt nicht nur bei einem befallenen Unternehmen das Outlook-Adressbuch auslesen, sondern gleich auch noch E-Mail-Inhalte und Anhänge. Alle diese Daten werden automatisiert verwendet, um an weitere potentielle Opfer möglichst authentisch wirkende Schadware-Mails zu versenden. Die Mail-Absenderangabe, die passende „korrekte“ Signatur und auch noch übliche Betreff- und Textformulierungen täuschen vertrauenswürdige bekannte Kommunikationspartner vor. Wer dann auf einen beigefügten Mailanhang klickt oder einen Hyperlink ohne weitere Überprüfung öffnet, erhält prompt Schadsoftware und jede Menge Ärger.

Schadware „Emotet“ kopiert von befallenen Systemen Mailadressen, sendet dorthin Mails mit Schadanhang mit „korrekter“ Absender-Signatur, und verwendet Text aus früheren echten Mails: Tückisch!

*****

35 Millionen Euro Bußgeldbescheid für H & M

Bei H&M wurden sensible Daten von Beschäftigten systematisch ausspioniert. Vorgesetzte führten nach Fehltagen (Krankheit, Urlaub) Gespräche mit den zurückkehrenden Beschäftigten und trugen die Informationen über Urlaub, Gesundheit, Familie etc. heimlich in eine Datei ein. Diese war Führungskräften frei zugänglich und wurde auch bei Personalentscheidungen genutzt. Selbstverständlich ein krasser Datenschutzverstoß. Die Konzernleitung sei laut Pressetext der Aufsichtsbehörde bemüht, Betroffene zu entschädigen und Vertrauen wiederherzustellen. Die Hamburger Datenschutzaufsichtsbehörde hat dennoch die deutsche Rekordsumme von 35,3 Millionen Euro Bußgeld verhängt. Ob H&M zahlt oder Einspruch einlegt, ist derzeit unklar.

Krasser Datenschutzverstoß mit Beschäftigtendaten

Konzernleitung arbeitet mit Aufsichtsbehörde zusammen, beendet den Verstoß

Rekord-Bußgeld – Rechtsweg noch möglich

*****

Impressum: Sabine Link
Datenschutzbeauftragte und Unternehmensberatung
Schulte-Marxloh-Str. 19, 47169 Duisburg
Telefon: 0176-8488 5082 oder 0203-3498 3045
Internet: www.datenschutz-link.de
E-Mail: info@datenschutz-link.de
Umsatzsteueridentifikationsnummer: DE 298 214 620

Verantwortlich für den Inhalt: Sabine Link, Anschrift siehe oben.

Plattform der EU-Kommission zur Online-Streitbeilegung: www.ec.europa.eu/consumers/odr .

Die Berufshaftpflichtversicherung (Vermögens-schaden-Haftpflichtversicherung) besteht bei der ERGO Versicherung AG, Victoriaplatz 1, 40477 Düsseldorf. Räumlicher Geltungsbereich: Europa.