„Schrems II“ und die Auswirkungen

DataSeCon
Data Security Consulting
Daten - Schutz - Sicherheit - Verfügbarkeit

Liebe Geschäftspartnerin,
lieber Geschäftspartner,

am 16.07.2020 hat der Europäische Gerichtshof mit einer aufsehenerregenden Entscheidung den Beschluss der Europäischen Kommission 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig erklärt.

Die Aufhebung dieses Angemessenheitsbeschlusses erfolgte auf Basis einer Beschwerde des österreichischen Datenschutzaktivisten Max Schrems gegen Facebook vor der irischen Datenschutzbehörde DPC.

Die Aufhebung des Angemessenheitsbeschlusses bedeutet in einem kurzen Satz, dass Datenübermittlungen in die USA, die sich auf die Rechtsgrundlage des EU-US-Privacy Shield gestützt haben, seit 16.07.2020 nicht mehr erlaubt sind und somit einen Verstoß gegen die DSGVO darstellen.

Ausführlicher geht’s jetzt weiter …

Was ist der EU-US-Privacy Shield ?

Der EU-US-Privacy Shield ist eine (informelle) Absprache, die zwischen der Europäischen Union und den USA im Jahr 2016 – als Nachfolger des sog. Safe-Harbour-Abkommens – ausgehandelt wurde. Diese Absprache besteht aus einer Reihe von Zusicherungen der amerikanischen Regierung und dem (jetzt für ungültig erklärten) Angemessenheitsbeschluss der EU-Kommission.

US-Unternehmen konnten sich freiwillig dem EU-US-Privacy Shield unterwerfen bzw. sich zertifizieren und sich in einer entsprechenden Liste eintragen lassen. Diese Liste umfasst derzeit über 5.000 US-Unternehmen und kann unter https://www.privacyshield.gov/list eingesehen werden.

Die Absprache regelt den Schutz personenbezogener Daten, die aus der EU in die USA übermittelt und dort (weiter)verarbeitet werden, indem es den Unternehmen, die sich dem EU-US-Privacy Shield unterworfen haben, ein Datenschutzniveau zuspricht, das demjenigen der EU gleichkommt und somit eine Datenübermittlung ohne weitere zusätzliche Genehmigungen möglich machte.

Warum wurde der Angemessenheitsbeschluss für ungültig erklärt und welche Alternativen gibt es ?

Im Kern stellte der EuGH fest, dass es die aktuelle Gesetzeslage in den USA den Unternehmen faktisch unmöglich macht, ein der EU entsprechendes Datenschutzniveau garantieren zu können. Amerikanischen Behörden muss – auch anlasslos – Zugriff auf die Daten eingeräumt werden und Nicht-US-Bürger stehen keine Rechtsmittel zur Verfügung, um sich gegen diese Zugriffe einfach und erfolgreich zur Wehr setzen zu können.

Hier schützt die amerikanische Gesetzgebung nur US-Bürger. Nicht-US-Bürger können sich nicht auf diesen gesetzlichen Schutz berufen.

Gleichzeitig stellt der EuGH in dem Urteil aber auch fest, dass als Alternative sog. Standard-vertragsklauseln (Standard Contractual Clauses = SCC) als Basis für die Datenübermittlung in sog.

„unsichere Drittländer“ weiterhin verwendet werden können, sofern über diese bilateralen Verträge zwischen dem Verantwortlichen („Daten-Exporteur“) und dem Datenempfänger oder Verarbeiter („Daten-Importeur“) sichergestellt werden kann, dass beim Daten-Importeur ein der EU entsprechendes Datenschutzniveau eingehalten werden kann und die Rechte der EU-Bürger auch tatsächlich durchsetzbar sind.

Angesichts der ausführlichen Begründung für die Ungültigkeit des Angemessenheitsbeschlusses im EuGH Urteil erscheint es derzeit zumindest äußerst fraglich, ob für Datenübermittlungen in die USA über Standardvertragsklauseln das nach der DSGVO geforderte Schutzniveau für EU-Bürger garantiert werden kann.

Ebenso dürfte es aus heutiger Sicht in absehbarer Zeit auch kein „Nachfolge-Abkommen“ für den EU-US-Privacy Shield geben, das einen ungehinderten Datentransfer zwischen EU und den USA – wie er bisher unter dem EU-US-Privacy Shield realisiert werden konnte – weiterhin ermöglichen würde.

Diese Problematik betrifft im Übrigen auch Datenübermittlungen nach Großbritannien nach dem Ende der Brexit-Übergangsfrist am 31.12.2020. Nach dem Ende dieser Übergangsfrist ist Großbritannien endgültig kein EU-Mitglied mehr und damit aus Sicht der DSGVO ein „unsicheres Drittland“, gleich wie z.B. China, Indien, Russland, … und eben seit kurzem auch die USA.

Es ist zum gegenwärtigen Zeitpunkt ebenfalls nicht davon auszugehen, dass die Europäische Kommission einen entsprechenden Angemessenheitsbeschluss für Datenübermittlungen nach Großbritannien bis zum Ende der Brexit-Übergangsfrist fassen wird.

Die DSGVO sieht aber glücklicherweise auch noch weitere Möglichkeiten vor, um Datenübermittlungen in ein Drittland zu legitimieren. Dies ist aber für jede Übermittlung im Einzelfall zu überprüfen.

Bin ich von dieser Entscheidung betroffen ?

Es kommt – wie immer – darauf an …

Nicht von der Entscheidung betroffen sind Datenübermittlungen, die auf Basis einer Vertragserfüllung unbedingt erforderlich sind (z.B. eine Hotelreservierung für einen Mitarbeiter im Zuge einer Dienstreise in die USA oder die geschäftsübliche Korrespondenz mit einem amerikanischen Kunden oder Lieferanten)

Sehr wohl betroffen sind aber regelmäßige Datenübermittlungen an amerikanische Dienstleister in Verbindung mit der Nutzung von (Cloud)Services wie z.B. Microsoft 365, Microsoft Azure, Amazon AWS, Google Analytics, Salesforce, Shopify und dergleichen.

Es ist dabei (leider) auch unerheblich, ob die Daten, die über diese Services verarbeitet werden in der EU oder in den USA gespeichert werden. Amerikanische Behörden dürfen u.a. auf Basis des CLOUD Act auch auf die Daten amerikanischer Unternehmen zugreifen, wenn diese außerhalb der USA (z.B. in der EU) gespeichert sind.

Auch wenn du selbst keinen direkten Vertrag mit einem amerikanischen Dienstleister hast, kann es durchaus denkbar sein, dass sich dein IT-Dienstleister in der EU eines amerikanischen Sub-Dienstleisters bedient.

Gibt es Übergangsfristen ?

Leider NEIN !

Das EuGH Urteil entfaltete mit dem Zeitpunkt seiner Verkündung Rechtswirksamkeit. Eine Datenübermittlung in die USA auf Basis des EU-US-Privacy Shield ist damit seit 16.07.2020 nicht mehr DSGVO konform möglich.

Das bedeutet, dass derartige Datenübermittlungen in die USA einen Verstoß gegen die DSGVO darstellen, der durch die Datenschutzbehörde mit der Verhängung einer Verwaltungsstrafe (gem. Art. 83 Abs. 5 DSGVO „bis zu € 20 Mio oder 4% des weltweit erzielten Jahresumsatzes, je nachdem welcher der Beträge höher ist“) geahndet werden kann. Zusätzlich kann die Datenschutzbehörde die Einstellung der Datenübermittlung anordnen.

Was muss ich jetzt tun ?

Um Douglas Adams zu zitieren: **Don’t panic !**

Wie so oft, sind auch hier Panikreaktionen nicht angebracht und nicht zielführend. Dennoch besteht Handlungsbedarf. Nachdem es – wie oben erwähnt – keinerlei Übergangsfristen gibt, sollte das Thema nicht unnötig lange aufgeschoben werden.

Gerade die Erwähnung des EU-US-Privacy Shield in den Hinweisen zur Verarbeitung personenbezogener Daten (Datenschutzerklärung) gibt Außenstehenden die Möglichkeit, vergleichsweise einfach festzustellen, ob man auf die neue Rechtslage bereits reagiert hat. Es besteht dadurch auch ein erhöhtes Risiko, sich eine Beschwerde bei der Datenschutzbehörde „einzufangen“.

Folgende Schritte solltest du daher möglichst bald einleiten:

- Prüfung, ob Verarbeitungen mit Datenübermittlungen in die USA verbunden sind und ob dies auf Basis des EU-US-Privacy Shields erfolgt.
- Prüfung, ob es indirekte Datenübermittlungen in die USA gibt (Sub-Dienstleister des IT-Dienstleisters).
- Prüfung, ob der US-Dienstleister Standardvertragsklauseln (SCC) für die Legitimierung der Datenübermittlung bereitstellt. Diese müssen dann dahingehend überprüft werden, ob der Dienstleister auch WIRKLICH entsprechende Garantien abgeben kann.
- Hinweise zur Datenverarbeitung (Datenschutzerklärung) anpassen
- Prüfen, ob Alternativen bei Europäischen Dienstleistern existieren (besonders bei neuen Verarbeitungstätigkeiten).

Gerne stehe ich bei Fragen zum Thema zur Verfügung und unterstütze selbstverständlich auch gerne bei der Umsetzung.

Mit den besten Wünschen für einen „beschwerdefreien“ Sommer !

Matthias Haidekker

DataSeCon e.U.
Unternehmensberatung
Lacknerweg 38
6380 St. Johann in Tirol

T: +43 677 62 83 86 08
E: matthias.haidekker@datasecon.eu
W: www.datasecon.eu

Impressum

DataSeCon e.U.
Unternehmensberatung

Lacknerweg 38
6380 St. Johann in Tirol

T: +43 (677) 62 83 86 08
E: office@datasecon.eu
W:www.datasecon.eu

Allgemeine Hinweise

Meine Absicht ist es, die Themen in klarer und verständlicher Sprache zu vermitteln. Die Inhalte stellen meine Sichtweise dar und sind daher keine verbindliche Rechtsberatung.

Aus Gründen der Lesbarkeit verzichte ich darauf, geschlechtsspezifische Formulierungen zu verwenden. Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Männer, Frauen und Divers in gleicher Weise.