Verbandssanktionen – EuGH erklärt EU-US Privacy Shield für unwirksam: Verträge zum Transfer personenbezogener Daten in die Vereinigten Staaten müssen angepasst werden.

Der EuGH hat mit seiner Entscheidung zum EU-US Privacy Shield wie bereits zum vorherigen Safe-Harbor Abkommen festgestellt, dass dieser kein angemessenes Datenschutzniveau gewährleisten kann. Das Gericht entzieht damit einem Großteil des transatlantischen Datentransfers die rechtliche Grundlage. Europäische Unternehmen sind nun gezwungen, sämtliche ihrer Vereinbarungen zum Datentransfer in die Vereinigten Staaten zu überprüfen und ggf. auf eine andere rechtliche Grundlage zu stellen.

Hintergrund der Entscheidung

Der Transfer personenbezogener Daten an Unternehmen in den Vereinigten Staaten von Amerika ist nicht zuletzt auch aufgrund der omnipräsenten Nutzung von Cloud-Diensten alltäglich geworden. Auch aus den betrieblichen Abläufen vieler europäischer Unternehmen ist die Nutzung der Leistungen großer amerikanischer Cloudanbieter nicht mehr wegzudenken. Doch die Europäische Datenschutzgrundverordnung stellt strenge Anforderungen an solche Datenübertragungen an Unternehmen in Ländern außerhalb der EU bzw. des EWR. So bedarf es der Sicherstellung, dass das Datenschutzniveau in dem Land des Empfängerunternehmens im Wesentlichen dem Datenschutzniveau in Europa entspricht. Diese Angemessenheit des Datenschutzniveaus kann durch verschiedene Mechanismen sichergestellt werden. Einer dieser Mechanismen – wohl einer der am häufigsten verwendeten – ist der Angemessenheitsbeschluss, der 2016 zwischen Europa und den Vereinigten Staaten als sog. EU-US Privacy Shield (“EU-US Privacy Shield“) verhandelt und abgeschlossen wurde. Daneben stehen weitere Mechanismen, wie die sog. EU-Standardvertragsklauseln (“Standardvertragsklauseln”) oder verbindliche unternehmensinterne Datenschutzvorschriften („Binding Corporate Rules“), zur Verfügung.

Gegen das EU-US Privacy Shield hat der österreichische Datenschutzaktivist Max Schrems mit der Begründung geklagt, dass der Privacy Shield insbesondere aufgrund der weitreichenden Befugnisse amerikanischer Geheimdienste keinen ausreichenden Schutz für Europäische betroffene Personen biete und dementsprechend kein angemessenes Datenschutzniveau im Sinne der Anforderungen des europäischen Datenschutzes gewährleisten könne. Zum EU-US Privacy Shield sowie zu den EU-Standardvertragsklauseln hat nun der Europäische Gerichtshof (“EuGH”) entschieden.

Die Entscheidung des EuGH und die sie tragenden Gründe

Der EuGH befand in seiner Entscheidung „Schrems II“ vom 16. Juli 2020, dass die Entscheidung der EU-Kommission 2016/1250 vom 12. Juli 2016, die den „EU-US Privacy Shield“ als Nachfolger des Safe-Harbor Abkommens etabliert hatte, ebenfalls unwirksam ist. Diese Entscheidung des EuGH hat sehr weitrechende Konsequenzen, da ab sofort die Übermittlung personenbezogener Daten von europäischen Unternehmen an US-amerikanische Unternehmen nicht länger auf die häufig verwendete Rechtsgrundlage gestützt werden kann. Darüber hinaus hat der EuGH auch geurteilt, dass die EU-Standardvertragsklauseln jedenfalls aufgrund der in

diesem Verfahren vorgetragenen Sachlage und Argumente nicht unwirksam seien und grundsätzlich weiterhin als Rechtsgrundlage verwendet werden können.

Der EuGH stützt seine Entscheidung zur Unwirksamkeit des EU-US Privacy Shields im Wesentlichen auf die folgenden Gründe:

- Die Entscheidung der EU-Kommission zur Angemessenheit des Schutzniveaus ist nach Auffassung des EuGH aus mehreren Gründen fehlerhaft und daher aufzuheben. Der EuGH schätzt insbesondere nunmehr die Fragen der Verhältnismäßigkeit und Bestimmtheit der Möglichkeiten staatlicher Zugriffe auf Daten europäischer Bürger als auch die Möglichkeiten eines wirksamen Rechtsbehelfs europäischer Bürger gegen Zugriffe US-amerikanischer staatlicher Stellen entgegen der Auffassung der Kommission als unzureichend ein.
- Der EuGH führt zunächst aus, dass das EU-US Privacy Shield selbst bereits Beschränkungen des Schutzes der Rechte und Freiheiten der betroffenen Personen enthalte, soweit eine Beschränkung erforderlich sei für die nationale Sicherheit, das öffentliche Interesse oder Strafverfolgungsinteressen der Vereinigten Staaten.
- Weiter führt der EuGH aus, dass es dabei jedoch tatsächlich an einer Eingrenzung auf ein notwendiges Maß fehle, da einerseits weder eindeutige Voraussetzungen für den Zugriff auf die Daten europäischer Betroffener noch Mindeststandards zum Schutz der Rechte und Freiheiten für den Fall eines Zugriffs in den US-amerikanischen Sicherheitsgesetzen verankert seien. Anderseits sei insbesondere für Überwachungsmaßnahmen der Geheimdienste, wie den durch Edward Snowden bekanntgewordenen Programmen PRISM oder UP-STREAM, der Schutz individueller Personen nicht adäquat geregelt, sondern diese Programme würden vielmehr nur pauschal aufgrund einer jährlichen Prüfung des Gesamtprogramms genehmigt. Dies sei, so der EuGH, jedoch keine wirksame Beschränkung von Ein-griffen in die Rechte und Freiheiten auf ein notwendiges und verhältnismäßiges Maß.
- Als weiteren tragenden Grund seiner Entscheidung führt der EuGH an, dass europäischen Personen, die von solchen Maßnahmen betroffen sind, keine ausreichenden Rechtsbehelfe zur Verfügung stehen. Insbesondere der durch den EU-US Privacy Shield vorgesehene Ombudsmann biete keinen ausreichenden Rechtsschutz im Sinne europäischer Grundrechte.
- Der EuGH stellt zunächst fest, dass bereits im EU-US Privacy Shield selbst dem Ombudsmann die Überprüfung einiger Maßnahmen entzogen sei, in denen elektronische Überwachung für die nationale Sicherheit durch US-Geheimdienste durchgeführt werden. Bereits diese Unzuständigkeit mache es unmöglich, von einem Rechtsschutzniveau auszugehen, das den Anforderungen der Europäischen Charta genüge.
- Schließlich stellt der EuGH fest, dass der nach dem EU-US Privacy Shield vorgesehene Ombudsmann weder unabhängig sei noch Entscheidungen treffen könne, die für die zugreifende staatliche Stelle verbindlich wären. So werde der Ombudsmann zwar im EU-US Privacy Shield als unabhängig von den Geheimdiensten beschrieben, er werde jedoch vom US Secretary of State ernannt, gehöre dem US State Department an und könne ohne besonderen Schutz wieder aus seiner Position entlassen werden. Und letztlich, so der EuGH, fehle es an jeglicher erkennbarer rechtlicher Absicherung, dass Entscheidungen des Ombudsmanns gegen andere staatliche Stellen verbindlich und auch vollstreckbar wären. Auch politische Zusagen, auf die sich Europäische betroffene Personen stützen könnten, seien nicht erkennbar.

Folgen der Entscheidung und Handlungsempfehlungen

Die aus den vorstehenden wesentlichen Gründen ergangene Entscheidung erklärt den EU-US Privacy Shield ab sofort für unwirksam. Der EuGH stellt abschließend fest, dass diese sofortige Wirkung der Entscheidung kein unzumutbares rechtliches Vakuum erzeuge, da die Datenschutzgrundverordnung weiterhin andere Möglichkeiten („Garantien“) vorsehe, um den Datentransfer in die Vereinigten Staaten zu ermöglichen.

Die Folgen der Entscheidung sind weitreichend und für viele Unternehmen ein bitteres Ergebnis eines Prozesses, das jedoch von viele Experten erwartet wurde: Personenbezogene Daten von EU-Bürgern können nun ab sofort

nicht mehr rechtmäßig auf der Grundlage des EU-US Privacy Shields in die USA übermittelt werden. Auch eine offizielle Übergangsfrist gibt es nicht. Es ist daher Eile geboten. Zunächst gilt es, in betroffenen Unternehmen zu überprüfen, welche Garantien zur Datenübermittlung aktuell genutzt werden.

Sofern Datenübermittlungen aktuell auf Basis des EU-US Privacy Shields erfolgen, sollte die Datenverarbeitung zunächst sofort eingestellt werden, um Bußgelder zu vermeiden. Es ist zu erwarten, dass auch die Aufsichtsbehörden in Kürze beginnen werden, die Rechtmäßigkeit der Datentransfers zu überprüfen.

In einem zweiten Schritt wären die Datenverarbeitungen durch eine andere geeignete Garantie entsprechend abzusichern. Kurzfristig sind hier sicherlich die Standardvertragsklauseln das Mittel der Wahl – wenn auch mit den in der Entscheidung des EuGH ebenfalls beleuchteten Risiken. Denn zwar sind die Standardvertragsklauseln nach dem Urteil des EuGH nach wie vor gültig, jedoch besteht auch hier das Risiko für die Betroffenen, dass öffentliche Stellen in Rechte und Freiheiten der Betroffenen durch einen Zugriff auf die personenbezogenen Daten eingreifen. Im Einzelfall, so führt der EuGH aus, sei das für die Datenverarbeitung verantwortliche EU-Unternehmen, welches die personenbezogenen Daten in einen Staat außerhalb der EU oder des EWR (Drittland) übermittelt, sowie das die Daten empfangende Unternehmen im Drittland in der Pflicht zu prüfen (z.B. anhand Regelungen zur öffentlichen Sicherheit, Verteidigung und Staatssicherheit – insbesondere bezüglich ausreichender Schutzmaßnahmen für EU-Bürgern) und sicherzustellen, dass das erforderliche Schutzniveau eingehalten wird. Ist dies nicht der Fall, darf der Datentransfer nicht erfolgen.

Allerdings, und dies ist der Unterschied zum EU-US Privacy Shield, enthielten die Standardvertragsklauseln nicht sämtliche Garantien für ein angemessenes Schutzniveau in ein Drittland – die Schutzmechanismen der Standardvertragsklauseln seien grundsätzlich erweiterbar. Daher sei im Falle der Anwendung der Standardvertragsklauseln im Einzelfall eine Prüfung erforderlich, ob die so getroffenen Vereinbarungen tatsächlich auch eingehalten werden können, ggf. sind – so-weit dies möglich ist – zusätzliche Garantien über eine Erweiterung der Standardvertragsklauseln zu schaffen.

Wie diese Entscheidung des EuGH zukünftig in der Praxis umgesetzt wird, bleibt derzeit noch weitgehend offen. Denn der Verantwortliche wird regelmäßig nur unter erheblichen Schwierigkeiten dazu in der Lage sein, die Risiken für die Rechte und Freiheiten, die sich in der spezifischen fremden Rechtordnung stellen, selbst zu bewerten – auch und gerade rechtsvergleichend zum europäischen Recht. Fraglich bleibt daher, ob zur Beantwortung dieser Frage der Auftragsverarbeiter (dem seine eigene Rechtsordnung bekannt sein dürfte) verstärkt in die Pflicht genommen wird oder ob die Europäischen Aufsichtsbehörden länderspezifische Empfehlungen zur Ergänzung der Standardvertragsklauseln veröffentlichen werden.
Mittel bis langfristig wären Binding Corporate Rules – neben den sonst in Betracht kommenden Rechtsgrundlagen, wie z.B. einer Einwilligung oder zum Zwecke der Vertragserfüllung – eine geeignete und sichere Möglichkeit, um die Datenverarbeitung wieder auf eine sichere Grundlage zu stellen. Deren Implementierung ist jedoch aufwändig und der Prozess braucht erfahrungsgemäß Zeit. Schließlich werden auch Überlegungen dahingehend anzustellen sein, wo auf die Datenverarbeitung gänzlich verzichtet, auf die Datenverarbeitung in Drittländer verzichtet und ob die Datenverarbeitung ggf. in die EU/den EWR verlagert werden kann.

Im Übrigen soll nicht unerwähnt bleiben, dass die aktuelle Entscheidung des EuGH sicherlich auch Indizwirkung für andere Angemessenheitsbeschlüsse hat. Es bleibt abzuwarten, ob und wie sich die Aufsichtsbehörden kurzfristig zum Thema insgesamt positionieren werden.

Zusammenfassung

- EuGH: Angemessenheitsbeschluss der Kommission zum EU-US Privacy Shield ist unwirksam.
- Allein auf diesen Beschluss gestützte transatlantischen Datentransfers haben keine rechtliche Grundlage mehr.
- Europäische Unternehmen müssen alle auf den Angemessenheitsbeschluss zum EU-US Privacy Shield beruhende Vereinbarungen zum Datentransfer in die Vereinigten Staaten umstellen.
- Standardvertragsklauseln als Rettungsanker sind – neben sog. Binding Corporate Rules für konzerninterne Datentransfers – die einzig verbleibende Möglichkeit, die aber nach der EuGH-Entscheidung nicht nur mit Blick auf die USA auch mit Risiken verbunden ist.

Ansprechpartner: