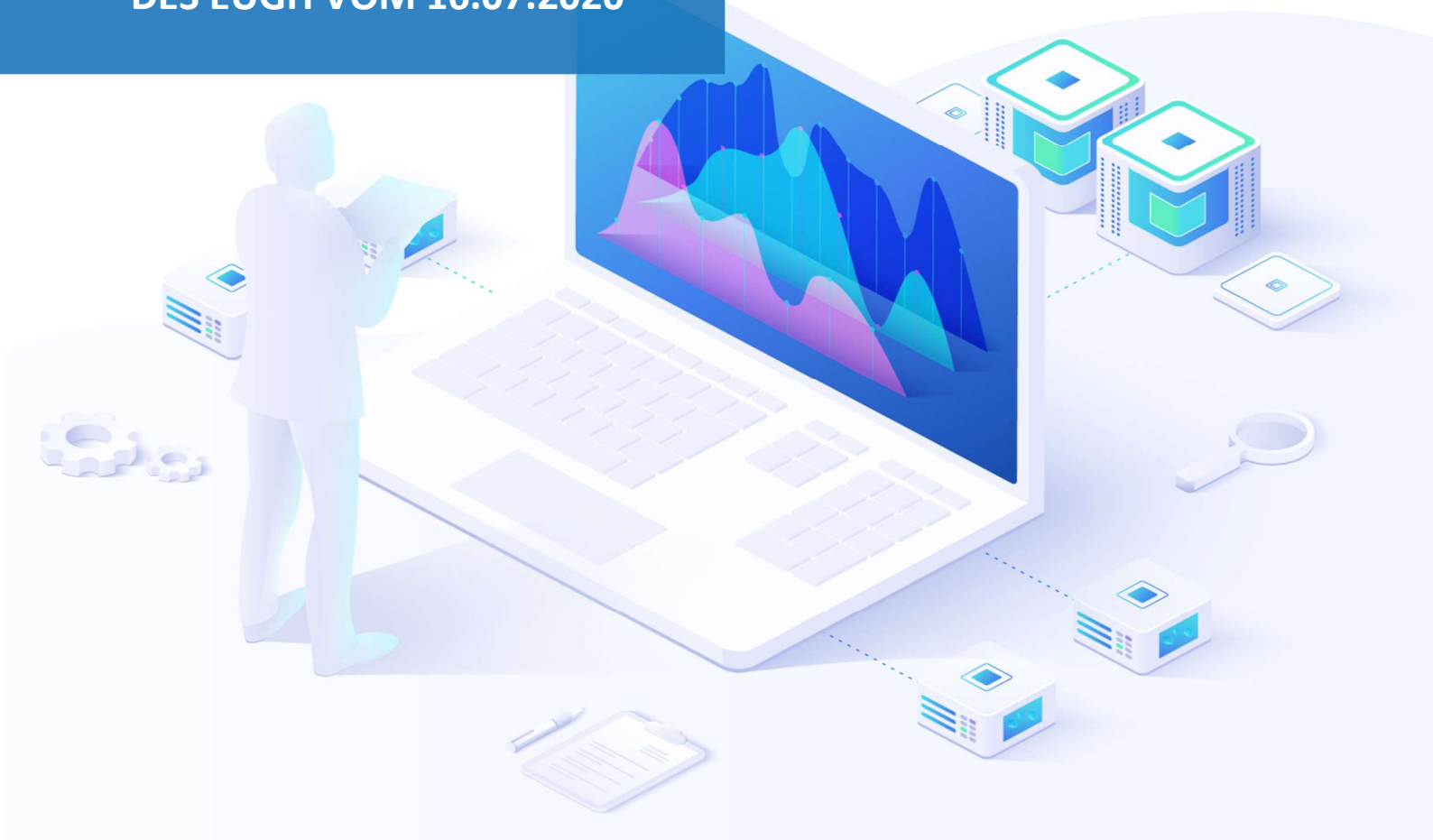


MANDANTENINFORMATION

**DAS PRIVACY SHIELD-URTEIL
DES EUGH VOM 16.07.2020**



DIE NEUE RECHTSLAGE BEI DATENÜBERMITTLUNGEN IN DIE USA

Ausgangslage

Personenbezogene Daten können an einen Empfänger in den USA übermittelt werden, wenn besondere Garantien für ein ausreichendes Datenschutzniveau vorgesehen werden. Solche Garantien können vor allem in einem Abschluss sog. **EU-Standardvertragsklauseln**, dem Vorhandensein von verbindlichen internen Datenschutzvorschriften (**Binding Corporate Rules**) beim Empfängerunternehmen oder in einem **Beschluss der Europäischen Kommission**, in welchem die Beachtung eines angemessenen Datenschutzniveaus durch den Empfänger bestätigt wird, gesehen werden.

Daneben können personenbezogene Daten an Empfänger in den USA u.a. dann übermittelt werden, wenn die betroffene Person ausdrücklich hierin einwilligt oder die Übermittlung zur Durchführung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Diese Ausnahmetatbestände sind jedoch regelmäßig nicht erfüllt, sodass Übermittlungen in die USA **in der Praxis** auf Rechtsgrundlagen beruhen, deren Wirksamkeit die betroffene Person nicht direkt beeinflussen kann.

Der EU-US-Privacy Shield

Der EU-US-Privacy Shield stellte – als Nachfolger des sog. Safe-Harbor-Abkommens zwischen der EU und den USA, welches im Jahr 2015 vom EuGH für unwirksam erklärt wurde – einen **Angemessenheitsbeschluss** im oben genannten Sinne dar. US-amerikanische Unternehmen, welche sich zur Beachtung der Grundsätze des Privacy Shield verpflichtet hatten und in die Liste der zertifizierten Teilnehmer aufgenommen worden waren, wurden von der EU-Kommission als sichere Empfänger in den USA anerkannt. An diese Unternehmen konnten personenbezogene Daten aus der EU heraus übermittelt werden, ohne dass weitere vertragliche oder organisatorische Vorkehrungen erforderlich gewesen waren.

Kernaussagen des Urteils des EuGH vom 16.07.2020

Nachdem der österreichische Jurist und Datenschutzaktivist Maximilian Schrems sich bei der irischen Datenschutzbehörde darüber beschwert hatte, dass die irische Facebook Ireland Ltd ohne hinreichende Garantien personenbezogene Daten mit der US-amerikanischen Facebook Inc. teile, setzte das irische Gericht das darauf folgende Verfahren aus und legte dem **Europäischen Gerichtshof (EuGH) mehrere Fragen zur Vorabentscheidung** vor, welche auch die Zulässigkeit einer Datenübermittlung aufgrund des Privacy Shield betrafen.

In seinem Urteil vom 16.07.2020 (Rechtssache C-311/18) stellte der EuGH nun fest, dass der dem Privacy Shield zugrunde liegende **Angemessenheitsbeschluss der EU-Kommission unwirksam** ist und begründete dies vor allem damit, dass aufgrund der weitreichenden Überwachungsbefugnisse der US-amerikanischen Strafverfolgungs- und Sicherheitsbehörden und der fehlenden Möglichkeit von betroffenen Personen, effektiven Rechtsschutz gegen eine sie betreffende Datenverarbeitung durch US-Behörden zu erlangen, ein mit dem EU-Standard vergleichbares, angemessenes Datenschutzniveau nicht angenommen werden kann.

Gleichzeitig entschied der EuGH, dass **EU-Standardvertragsklauseln weiterhin eine effektive Datenschutzgarantie** bei einer Datenübermittlung an Empfänger in die USA darstellen können. Gleichzeitig soll die zuständige Datenschutzaufsichtsbehörde laut EuGH jedoch verpflichtet sein, die Aussetzung von Datenübermittlungen an Drittländer – also auch in die USA – anzuordnen, wenn sie feststellt, dass Empfänger in den betreffenden Drittstaaten die Regelungen der **Standardvertragsklauseln nicht einhalten können und keine sonstige Garantien** für ein angemessenes Datenschutzniveau vorgesehen sind.

Zwei Stufen der Datenübermittlung

Zunächst ist an dieser Stelle festzuhalten, dass das EuGH-Urteil zum Privacy Shield erst die **zweite Stufe der Datenübermittlung** betrifft, auf welcher geeignete Garantien für eine Übertragung aus der EU bzw. dem Europäischen Wirtschaftsraum (EWR) heraus vorzusehen sind. Daneben ist jedoch immer eine Rechtsgrundlage dafür erforderlich, dass personenbezogene Daten überhaupt vom Empfänger verarbeitet werden dürfen. Sofern es sich beim Empfänger um einen weisungsgebundenen Dienstleister handelt, stellt der zwischen Auftraggeber und Auftragnehmer abzuschließende Vertrag zur Auftragsverarbeitung eine solche **Rechtsgrundlage auf der ersten Stufe** dar. Daneben können auch eine Einwilligung, die Erforderlichkeit zur Erfüllung eines Vertrags mit der betroffenen Person sowie berechnete Interessen des Verantwortlichen oder eines Dritten die Zulässigkeit der Verarbeitung auf der ersten Stufe begründen. Erst nachdem eine hinreichende Rechtsgrundlage für eine Übermittlung auf der ersten Stufe vorliegt, d.h. wenn es um die Frage geht, ob die an sich zulässige Verarbeitung auch gerade außerhalb von EU / EWR erfolgen kann, werden die auf der zweiten Stufe vorzusehenden Garantien relevant.

Folgen des Urteils für Datenübermittlungen in die USA

Welche direkten Folgen hat die Entscheidung des EuGH für Verantwortliche, welche personenbezogene Daten an Empfänger in den USA übermitteln?

Die wichtigste Konsequenz ist, dass Datenübermittlungen in die USA, welche bislang alleine aufgrund einer Privacy Shield-Zertifizierung des Empfängers erfolgten, nun die Rechtsgrundlage entzogen ist. Sind keine zusätzlichen effektiven Datenschutzgarantien vorgesehen, ist die **Übermittlung nunmehr rechtswidrig** und kann theoretisch mit einem Bußgeld belegt werden. Dass die Aufsichtsbehörden hier sofort tätig werden und Bußgeldverfahren gegen Verantwortliche einleiten, ist jedoch eher unwahrscheinlich. Eine **gewisse Karenzzeit** wird bereits aus Rechtsstaatsgründen angezeigt sein, damit Verantwortliche Übermittlungen an US-amerikanische Empfänger entweder auf eine neue Rechtsgrundlage stützen, oder diese geordnet einstellen können. Ob und ggf. wann zwischen der EU und den USA ein Nachfolger für das Privacy Shield-Abkommen ausgehandelt und in Kraft gesetzt wird, ist zum jetzigen Zeitpunkt nicht abzusehen. In der Zwischenzeit **muss der Verantwortliche tätig werden** und nunmehr unzulässige Datenübermittlungen an US-

amerikanische Empfänger entweder auf eine neue taugliche Rechtsgrundlage umstellen, oder solche Übermittlungen fürs erste aussetzen.

Viele größere US-amerikanische Unternehmen haben interne verbindliche Datenschutzvorschriften, sog. **Binding Corporate Rules (BCR)**, implementiert. Diese wurden zuvor von der zuständigen Datenschutz-Aufsichtsbehörde in der EU geprüft und von dieser als angemessene Datenschutzgarantien freigegeben. Sofern mit einem größeren Konzern in den USA eine Geschäftsbeziehung besteht, stehen die Chancen also nicht schlecht, dass die Datenübermittlung weiterhin zulässig ist, da das Unternehmen aufgrund seiner BCR zur Gewährleistung eines ausreichenden Datenschutzstandards verpflichtet ist. Solange die zuständige Aufsichtsbehörde die BCR nicht für unzureichend erklärt, können Verantwortliche auf deren Wirksamkeit vertrauen.

Liegen keine BCR vor, bleibt faktisch nur noch der Abschluss von sog. **EU-Standardvertragsklauseln**. Darin verpflichtet sich der US-amerikanische Empfänger gegenüber dem Verantwortlichen, freiwillig ein Datenschutzniveau zu gewährleisten, welches mit dem europäischen vergleichbar und damit angemessen ist. Der Inhalt der Standardvertragsklauseln wird von der EU-Kommission vorgegeben. Solange die zuständige Datenschutz-Aufsichtsbehörde nicht feststellt, dass US-amerikanische Empfänger aufgrund der dortigen Gesetzeslage nicht in der Lage sind, die Standardvertragsklauseln einzuhalten, kann auf deren Wirksamkeit vertraut werden. Dies setzt jedoch voraus, dass der US-amerikanische Empfänger überhaupt bereit ist, Standardvertragsklauseln zu unterzeichnen.

In allen anderen Fällen wird Verantwortlichen in der Regel nichts anderes übrig bleiben, als entweder die **ausdrückliche Einwilligung** der betroffenen Personen in die Übermittlung ihrer personenbezogenen Daten an US-amerikanische Empfänger einzuholen, oder Übermittlungen in die USA **zunächst auszusetzen**, wenn der Empfänger nicht die Möglichkeit anbietet, Verarbeitungen ausschließlich in der EU / dem EWR durchzuführen.

KONTAKT



legal data
Schröder Rechtsanwaltsgesellschaft mbH
Prannerstr. 10
80333 München



Tel:
+49 89 954 597 520
Fax:
+49 89 954 597 522



E-mail: datenschutz@legaldata.law
www.legaldata.law