BRANDI
RECHTSANWÄLTE

Datenübermittlung in Drittstaaten

Einleitung

Um Datenübertragungen in Drittstaaten, also Staaten, die weder Mitglied der Europäischen Union (EU) noch des Europäischen Wirtschaftsraums (EWR) sind, zu rechtfertigen, wurde bisher in vielen Fällen auf das EU-US Privacy Shield und die EU-Standardvertragsklauseln zurückgegriffen. Der Europäische Gerichtshof hat nun mit einer Entscheidung vom 16.07.2020 das EU-US Privacy Shield für unwirksam erklärt und sich außerdem zu den EU-Standardvertragsklauseln geäußert (EuGH, Az. C-311/18). Das Urteil hat Auswirkungen für viele europäische Unternehmen, die Daten in die USA und andere Drittstaaten übermitteln.

Datenschutzrechtliche Anforderungen an die Datenübermittlung in Drittstaaten

Die Datenschutz-Grundverordnung (DSGVO) hat das Ziel, in allen Mitgliedstaaten der EU ein gleichwertiges Schutzniveau für personenbezogene Daten zu gewährleisten. Dieses gleichmäßig hohe Schutzniveau soll nach Erwägungsgrund 103 nicht dadurch untergraben werden, dass personenbezogene Daten aus der EU an Empfänger in Drittstaaten oder internationale Organisationen übermittelt werden. In Art. 44 DSGVO ist deshalb festgelegt, dass die Übermittlung personenbezogener Daten in einen Drittstaat oder eine internationale Organisation nur zulässig ist, wenn die Bestimmungen der DSGVO eingehalten werden.

Die Art. 44 ff. DSGVO enthalten spezielle Anforderungen an die Übermittlung personenbezogener Daten in Drittstaaten oder internationale Organisationen. Eine Übermittlung darf nur stattfinden, wenn vorab sichergestellt werden kann, dass in dem betroffenen Drittstaat ein Datenschutzniveau gewährleistet wird, das mit dem Datenschutzniveau in der EU vergleichbar ist. Für die Gewährleistung eines angemessenen Datenschutzniveaus sieht die DSGVO verschiedene Mechanismen vor.

Eine Übermittlung personenbezogener Daten in einen Drittstaat darf etwa vorgenommen werden, wenn die Europäische Kommission beschlossen hat, dass der betroffene Drittstaat, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittstaat ein angemessenes Schutzniveau bieten. Derartige Angemessenheitsbeschlüsse bestehen nur für sehr wenige Staaten, zum Beispiel für die Schweiz, Neuseeland und Argentinien. Eine vollständige Liste der Staaten findet sich auf der Internetseite der Europäischen Kommission. Hat die EU-Kommission in einem Angemessenheitsbeschluss ein vergleichbares Datenschutzniveau beschlossen, dürfen Ziel-Unternehmen in diesen Staaten datenschutzrechtlich so behandelt werden, als wären sie Unternehmen aus der EU.

Liegt ein solcher Beschluss nicht vor und bietet ein Drittstaat damit kein von der EU-Kommission bestätigtes angemessenes Schutzniveau, dürfen personenbezogene Daten an den Drittstaat nur übermittelt werden, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Der Datenexporteur aus der EU kann mit dem Datenimporteur in einem Drittstaat einen von der Europäischen Kommission vorgegebenen Vertrag, die sogenannten EU-Standardvertragsklauseln, abschließen, in welchem der Datenimporteur verpflichtet wird, ein dem Datenschutzniveau in der EU vergleichbares Schutzniveau zu garantieren. Durch den Abschluss der Standardvertragsklauseln unterwirft sich das außereuropäische Unternehmen den von der EU-Kommission festgelegten Regelungen zur Datenverarbeitung.

Darüber hinaus kann ein vergleichbares Datenschutzniveau für Unternehmen in Drittstaaten auch durch den Einsatz von verbindlichen unternehmensinternen Datenschutzvorschriften gemäß Art. 47 DSGVO („Binding Corporate Rules“) oder durch genehmigte Verhaltensregeln gemäß Art. 40, 46 Abs. 2 lit. e) DSGVO erreicht werden. Diese müssen allerdings zuvor von der zuständigen Aufsichtsbehörde genehmigt werden.

Für den Datenaustausch mit den USA haben Unternehmen aus der EU in der Vergangenheit häufig das EU-US Privacy Shield eingesetzt, um die Datenübermittlung in die USA zu rechtfertigen. Das EU-US Privacy Shield ist ein spezielles Abkommen zwischen der EU und den USA, durch das zertifizierten Unternehmen bisher ein angemessenes Datenschutzniveau zugesprochen wurde.

Falls weder ein Angemessenheitsbeschluss noch geeignete Garantien vorliegen, ist eine Übermittlung personenbezogener Daten in einen Drittstaat nur im Ausnahmefall möglich, etwa bei Vorliegen einer ausdrücklichen Einwilligung des Betroffenen, Art. 49 Abs. 1 S. 1 lit. a) DSGVO.

Das Urteil des EuGHs zum EU-US Privacy Shield und den EU-Standardvertragsklauseln

Der EuGH hat das EU-US Privacy Shield in seiner aktuellen Entscheidung nun für unwirksam erklärt (EuGH,Urt. v. 16.07.2020, Az. C-311/18). Nach seiner Auffassung gewährleiste das EU-US Privacy Shield nicht ausreichend den Schutz der Grundrechte der EU-Bürger, insbesondere weil Daten von den US-Geheimdiensten ausgelesen werden könnten. Mit ähnlicher Argumentation hatte der

EuGH schon die Vorgängerregelung, das Safe-Harbor-Abkommen vom 26.07.2000 (Entscheidung 2000/520/EG der Kommission vom 26.07.2000), für unwirksam erklärt (EuGH, Urt. v. 06.10.2015, Az. C-362/14). Weil in der Zwischenzeit keine Verbesserung des Datenschutzniveaus in den USA eingetreten ist, kam die neue Entscheidung nicht überraschend.

Der EuGH stützt sich in seiner Entscheidung wieder auf die begrenzten Schutzmöglichkeiten von Daten in den USA aufgrund der dortigen restriktiven Gesetzgebung. Ein besonderes Risiko ergibt sich etwa aus dem amerikanischen CLOUD-Act („Clarifying Lawful Overseas Use of Data Act"), an den sich US-Unternehmen halten müssen. Basierend auf dem Regelwerk müssen US-Unternehmen unter Umständen die Daten ihrer Kunden auf Verlangen der US-Regierung unabhängig vom Speicherort herausgeben.

Im Ergebnis kann eine Datenübertragung in die USA somit seit dem Urteil nicht mehr auf das EU-US Privacy Shield gestützt werden. Auch zu den EU-Standardvertragsklauseln äußert sich der EuGH in diesem Zusammenhang. Grundsätzlich kann auf die EU-Standardvertragsklauseln nach Auffassung des EuGH weiterhin zurückgegriffen werden. Ein datenexportierendes EU-Unternehmen müsse aber vor der Datenübermittlung in einen Drittstaat im Einzelfall überprüfen, ob das Ziel-Unternehmen die Anforderungen aus den Standardvertragsklauseln auch wirklich einhalten kann (vgl. Randziffer 134 des Urteils). Es ist dabei insbesondere zu prüfen, ob es dem Empfänger effektiv möglich ist, das zugesagte Datenschutzniveau einzuhalten, wofür die vertragliche Zusicherung alleine nicht genügt.

Da US-Unternehmen unter Umständen die Daten ihrer Kunden auf Verlangen der US-Regierung unabhängig vom Speicherort herausgeben müssen, können sie die Standardvertragsklauseln insofern allerdings möglicherweise nicht einhalten. Im Ergebnis bieten damit auch die Standardvertragsklauseln keine vollständig belastbare Rechtsgrundlage für den Datenaustausch mit den USA und anderen Drittstaaten, deren Recht den Datenempfängern ähnliche Verpflichtungen, die die vertraglichen Garantien eines angemessenen Schutzniveaus untergraben können, auferlegt.

Auswirkungen des Urteils

Aufgrund der starken Vernetzung in der digitalisierten und globalisierten Welt hat das Urteil große Auswirkungen für europäische Unternehmen. Potenziell betroffen sind von dem Urteil alle Unternehmen, die Daten in die USA übermitteln, etwa weil sie Dienstleister aus den USA für die Verarbeitung personenbezogener Daten einsetzen. Das Urteil ist auch in den Fällen relevant, in denen zwar nur europäische Dienstleister eingesetzt werden, diese aber ihrerseits US-Unternehmen als Subdienstleister, zum Beispiel für das Hosting von Daten, einsetzen.

Betroffen ist beispielsweise die Zusammenarbeit mit großen US-Unternehmen wie Microsoft, Amazon, Google und Apple. Unternehmen und Dienstleister nutzen verbreitet die Dienste dieser Unternehmen, zum Beispiel Office 365, Amazon Web Services, Google-Dienste oder die Apple-Cloud. Auch in den Fällen, in denen nur Verträge mit den europäischen Tochtergesellschaften dieser US-Unternehmen abgeschlossen wurden, haben diese in ihren Vereinbarungen regelmäßig die jeweiligen US-Gesellschaften als Subdienstleister vermerkt. Es ist denkbar, dass US-Unternehmen in dieser Angelegenheit schnell reagieren, um den Zugang zum europäischen Markt nicht zu verlieren. Microsoft hat zum Beispiel bereits angekündigt, proaktiv mit der Europäischen Kommission und der US-Regierung zusammenarbeiten zu wollen, um die durch das Urteil aufgeworfenen Fragen zu klären und neue Ansätze zu gestalten.

Auch Datenübermittlungen in andere Drittstaaten, deren Recht den Datenempfängern ähnliche Verpflichtungen, die die vertraglichen Garantien eines angemessenen Schutzniveaus untergraben können, wie in den USA auferlegt, können von dem Urteil entsprechend betroffen sein.

Umsetzung des Urteils und Handlungsempfehlungen

Formal gibt es für das Urteil keine Umsetzungsfrist, da keine rechtliche Änderung erfolgt ist, sondern nur die Auslegung der rechtlichen Bestimmungen der DSGVO durch den EuGH konkretisiert wurde. Auch der Europäische Datenschutzausschuss (EDSA), der auf seiner Internetseite Antworten auf häufige Fragen zu den Konsequenzen des Urteils veröffentlicht hat, stellt fest, dass es keine „Gnadenfrist" für Datenverarbeitungen auf Grundlage des EU-US Privacy Shields gebe, weshalb mit der Umstellung ohne Verzögerung begonnen werden müsse.

Unternehmen sollten daher überprüfen, in welchen Situationen sie mit Unternehmen in Drittstaaten, insbesondere in den USA, zusammenarbeiten und welche Absicherung für den Einsatz des Dienstleisters sowie die Datenübermittlung jeweils erfolgt ist. Für den zukünftigen Einsatz neuer Dienstleister sollten die bestehenden Risiken sowie die Möglichkeiten zur Rechtfertigung der Datenübermittlung und zur Absicherung bereits vorab in die Überlegungen einbezogen werden.

Die dargestellten Probleme können weitgehend vermieden werden, indem auf einen Datenaustausch mit den USA beziehungsweise die Beauftragung von Anbietern mit Sitz in den USA so weit wie möglich verzichtet wird. Für viele Dienste gibt es alternative Anbieter, die oftmals ganz bewusst auf ihren Sitz in der EU und die Einhaltung der Vorgaben der DSGVO verweisen. Entsprechend hat bereits die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, in einer Pressemitteilung zur Beachtung des Urteils aufgerufen und datenverarbeitende Stellen in Berlin aufgefordert, in den USA gespeicherte personenbezogene Daten in die EU oder einen anderen Staat mit angemessenem Datenschutzniveau zu verlagern.

Ist dies nicht praktikabel, kann versucht werden, die Risiken des Drittstaatentransfers zu reduzieren, indem beispielsweise europäische Dienstleister zwischengeschaltet werden, die vertraglich die rechtskonforme Einbeziehung von amerikanischen Subdienstleistern zusagen. Dies führt jedoch nicht zu einer Freizeichnung in der Außenhaftung und gegenüber den Aufsichtsbehörden.

Auf die EU-Standardvertragsklauseln kann grundsätzlich weiter zurückgegriffen werden, allerdings ist ergänzend im Einzelfall zu prüfen, ob das Ziel-Unternehmen die Anforderungen aus den Standardvertragsklauseln einhalten kann. Es sollte dann dokumentiert werden, warum davon ausgegangen wird, dass der amerikanische Anbieter die von ihm geforderten Garantien auch wirklich umsetzen kann.

Theoretisch ist es auch denkbar, eine andere in der DSGVO genannte Rechtsgrundlage für die Datenübermittlung in die USA zugrunde zu legen, etwa die Einwilligung der betroffenen Person. Wird der Betroffene vor der Übermittlung der Daten über die bestehenden Risiken der Datenübermittlung informiert und willigt er dennoch ausdrücklich in die Datenübermittlung ein, dürfen die Daten in den Drittstaat übertragen werden. Diese Variante

ist aber in der Praxis regelmäßig ebenfalls mit Risiken behaftet, da eine datenschutzrechtliche Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Außerdem hängt die Wirksamkeit der Einwilligung davon ab, dass die verantwortliche Stelle alle entscheidungserheblichen Informationen zur Verfügung stellt, wofür wiederum die Zuarbeit des Dienstleisters erforderlich ist.

Fazit

Eine Übermittlung personenbezogener Daten in Drittstaaten darf nur stattfinden, wenn vorab sichergestellt werden kann, dass in dem betroffenen Drittstaat ein Datenschutzniveau gewährleistet wird, das mit dem Datenschutzniveau in der EU vergleichbar ist.

Seit dem Urteil des EuGH vom 16.07.2020 kann eine Datenübertragung in die USA nicht mehr auf das EU-US Privacy Shield gestützt werden. Auch die EU-Standardvertragsklauseln bieten seitdem für den Datenaustausch mit den USA keine uneingeschränkt belastbare Rechtsgrundlage mehr.

Die Datenübermittlung in die USA ist folglich mit datenschutzrechtlichen Risiken und Rechtsunsicherheiten belastet. Dies sollten Unternehmen bei dem Einsatz von Dienstleistern berücksichtigen. Falls sie sich dennoch für eine Datenübermittlung in die USA entscheiden, sollten sie die Risiken so weit wie möglich absichern, etwa durch den Rückgriff auf alternative Rechtsgrundlagen und vertragliche Regelungen mit den Dienstleistern.

Vor dem Hintergrund, dass viele Unternehmen auf die Nutzung amerikanischer Anbieter und die damit einhergehende Datenübermittlung angewiesen sind, bleibt zu hoffen, dass zukünftig Gestaltungen gefunden werden, die die Datenübertragung in Drittstaaten durch US-Unternehmen eindeutig regeln und datenschutzkonform ermöglichen. Bis dahin lassen sich datenschutzrechtliche Risiken für Unternehmen, die Daten in die USA übermitteln, allerdings nicht vollständig ausschließen

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin
T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net
www.brandi.net