DRITTSTAATENÜBERMITTLUNGEN - NEUER ANGEMESSENHEITS-BESCHLUSS FÜR DIE USA

Informationen zum Datenschutz I August 2023

English version

Einleitung

Internationale Datentransfers erfolgen im Unternehmensalltag im Zusammenhang mit der Nutzung einer Vielzahl von Online-Anwendungen. Dies gilt etwa für den Einsatz von Videokonferenzdiensten wie Microsoft Teams und Zoom, die Nutzung von Anwendungen wie Office 365 sowie die Einbindung von Cloud- und E-Mail-Services, aber auch für die Kooperation und den Austausch von Daten mit anderen Konzerngesellschaften. Vor allem die Zusammenarbeit mit amerikanischen Dienstleistern und Partnern ist für einen Großteil der Unternehmen trotz der mit internationalen Datentransfers einhergehenden datenschutzrechtlichen Schwierigkeiten nach wie vor von großer Relevanz. Im Rahmen der Umfrage „Datenschutz in der deutschen Wirtschaft: DSGVO & internationale Datentransfers“, die der Digitalverband Bitkom im Herbst 2022 veröffentlichte, gaben fast zwei Drittel der befragten Unternehmen an, dass der Verzicht auf internationale Datenübermittlungen für sie gravierende negative Folgen hätte. Die Befragten machten zudem deutlich, wie wichtig eine belastbare Rechtsgrundlage für internationale Datentransfers ist.

Datenschutzrechtliche Anforderungen an die Datenübermittlung in Drittstaaten

Ziel der Datenschutzgrundverordnung (DSGVO) ist es, in allen Mitgliedstaaten der EU ein gleichwertiges Schutzniveau für personenbezogene Daten zu gewährleisten. Nach Erwägungsgrund 103 soll das innerhalb der EU vorgesehene Schutzniveau durch die Übermittlung von personenbezogenen Daten aus der EU an Empfänger in einem Drittstaat oder an internationale Organisationen nicht unterschritten werden. Aus diesem Grund bedürfen internationale Datentransfers einer besonderen Absicherung. In Art. 44 DSGVO ist insoweit festgelegt, dass jedwede Übermittlung personenbezogener Daten in einen Drittstaat oder an eine internationale Organisation nur zulässig ist, wenn der für die Datenenverarbeitung Verantwortliche sowie Auftragsverarbeiter hierbei die innerhalb der DSGVO festgelegten Anforderungen und Bestimmungen einhalten. In den Vorschriften des fünften Kapitels der DSGVO (Art. 44 - 50 DSGVO) finden sich spezielle Anforderungen, die bei der Übermittlung personenbezogener Daten in Drittstaaten oder an internationale Organisationen eingehalten werden müssen. Ein Datentransfer darf insbesondere nur dann stattfinden, wenn vorab sichergestellt werden kann, dass in dem betreffenden Drittstaat ein Datenschutzniveau gewährleistet wird, das mit dem Datenschutzniveau in der EU vergleichbar ist. Zur Absicherung sieht die DSGVO verschiedene Mechanismen vor.

Art. 45 DSGVO regelt zunächst die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses. Eine Übermittlung personenbezogener Daten an ein Drittland darf hiernach vorgenommen werden, wenn die Europäische Kommission beschlossen hat, dass der betreffende Drittstaat, ein Gebiet oder ein oder mehrere spezifische Sektoren in dem Drittstaat über ein angemessenes Schutzniveau verfügen. Liegt ein Angemessenheitsbeschluss vor, bedürfen Datenübermittlungen in diesen Staat keiner besonderen einzelfallbezogenen Genehmigung. Entsprechende Beschlüsse bestehen allerdings nur für wenige Länder. Eine vollständige Liste der Staaten, für die derzeit ein Angemessenheitsbeschluss vorliegt, findet sich auf der Internetseite der Europäischen Kommission. Hat die Europäische Kommission in einem Angemessenheitsbeschluss ein vergleichbares Datenschutzniveau festgestellt, dürfen Ziel-Unternehmen in dem jeweiligen Staat datenschutzrechtlich so behandelt werden, als wären sie Unternehmen aus der EU. Bei Datenübermittlungen in die USA ist allerdings die Besonderheit zu berücksichtigen, dass nur solche Unternehmen von dem Beschluss erfasst werden, die an dem neuen „EU-US Data Privacy Framework“ teilnehmen.

Liegt ein entsprechender Beschlusss nicht vor und bietet der betreffende Drittstaat damit kein von der Europäischen Kommission bestätigtes angemessenes Datenschutzniveau, dürfen personenbezogene Daten nur dann übermittelt werden, wenn der für die Datenverarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

In Betracht kommt insoweit vor allem der Abschluss der EU-Standardvertragsklauseln, einem von der Europäischen Kommission vorgegebenen Vertrag zwischen dem Datenexporteur aus der EU und dem Datenimporteur in einem Drittstaat, in dem sich das außereuropäische Unternehmen zur Einhaltung der von der Europäischen Kommission vorgegebenen Anforderungen und eines angemessenen Datenschutzniveaus verpflichtet.

Darüber hinaus kann ein vergleichbares Datenschutzniveau für Unternehmen in Drittstaaten auch durch den Einsatz von verbindlichen unternehmensinternen Datenschutzvorschriften i.S.v. Art. 47 DSGVO („Binding Corporate Rules“), in denen sich die Unternehmen zur Einhaltung eines Datenschutz-Mindeststandards selbstverpflichten, sowie durch genehmigte Verhaltensregeln i.S.v. Art. 46 Abs. 2 lit. e) i.V.m. Art. 40 DSGVO erreicht werden. Diese müssen allerdings von der zuständigen Aufsichtsbehörde jeweils vor der Verwendung genehmigt werden.

Liegen weder ein Angemessenheitsbeschluss noch geeignete Garantien vor, ist ein internationaler Datentransfer nur im Ausnahmefall möglich. In Betracht kommt insoweit etwa das Vorliegen einer ausdrücklichen und informierten Einwilligung des Betroffenen, Art. 49 Abs. 1 S. 1 lit. a) DSGVO.

Bisherige Absicherung von Datenübermittlungen in die USA

Während Datenübermittlungen in die USA in der Vergangenheit mehrheitlich auf das EU-US Privacy Shield, ein spezielles Abkommen zwischen der EU und den USA, durch das zertifizierten Unternehmen ein angemessenes Datenschutzniveau zugesprochen wurde, gestützt wurden, greifen mittlerweile 91 % der Unternehmen zur Absicherung der Datentransfers auf den Abschluss von Standardvertragsklauseln, die von der Europäischen Kommission zur Verfügung gestellt werden, zurück. Der Europäische Gerichtshof (EuGH) hat das EU-US Privacy Shield in seinem Urteil „Schrems II" (EuGH, Urt. v. 16.07.2020 - Az. C-311/18) im Juli 2020 für ungültig erklärt und darüber hinaus zusätzliche Anforderungen im Hinblick auf die Nutzung von Standardvertragsklauseln statuiert. Zur Begründung führte der EuGH in seiner Entscheidung an, dass die USA nicht über ein den Standards innerhalb der EU entsprechendes Datenschutzniveau verfügen und die Grundrechte von EU-Bürgern nicht ausreichend geschützt werden; insbesondere die weitreichenden Zugriffsbefugnisse von amerikanischen Sicherheitsbehörden sowie der Mangel an wirksamen Rechtsbehelfen waren aus Sicht des EuGH problematisch.

Als Reaktion auf das Urteil des EuGH veröffentlichte die Europäische Kommission im Juni 2021 neue angepasste Standardvertragsklauseln, die nunmehr für die Absicherung von Datenübermittlungen in Drittstaaten genutzt werden können. Die neuen Standardvertragsklauseln tragen den Bedenken des EuGH Rechnung indem sie unter anderem konkrete Verhaltenspflichten für den Fall eines staatlichen Offenlegungsersuchens vorgeben (Klausel 15.1 und 15.2 der Standardvertragsklauseln). Zu beachten ist, dass der Abschluss der Klauseln die Prüfpflicht des Datenexporteurs in Bezug auf die Frage, ob ein angemessenes Datenschutzniveau trotz der Datenübermittlung in einen Drittstaat gewährleistet werden kann, allerdings nicht entfallen lässt. Eine Datenübermittlung auf Grundlage der Standardvertragsklauseln ist demnach nur dann zulässig, wenn die anwendbaren nationalen Regelungen die sich aus den Standardvertragsklauseln ergebenden Pflichten nicht konterkarieren. Um diesen Anforderungen gerecht werden zu können, ist die Erstellung einer Folgenabschätzung für den internationalen Datentransfer (Transfer Impact Assessment), im Rahmen derer auch zusätzlich ergriffene Absicherungsmaßnahmen abgebildet werden können, empfehlenswert.

Der neue Angemessenheitsbeschluss für die USA

Die Europäische Kommission hat nunmehr am 10. Juli 2023 einen neuen Angemessenheitsbeschluss für das EU-US Data Privacy Framework angenommen. Sie stellte darin fest, dass die Vereinigten Staaten ein angemessenes Schutzniveau – vergleichbar mit dem der EU – für personenbezogene Daten gewährleisten, die innerhalb des neuen Datenschutzrahmens aus der EU an US-Unternehmen übermittelt werden.

Damit eine Datenübermittlung an ein amerikanisches Unternehmen auf den Angemessenheitsbeschluss gestützt werden kann, muss dieses, wie auch zuvor beim EU-US Privacy Shield, am neuen Datenschutzrahmen teilnehmen und dem Abkommen beitreten. Um sich dem EU-US Data Privacy Framework anzuschließen, müssen sich die Unternehmen zur Einhaltung verschiedener Datenschutzpflichten verpflichten; hierzu zählen etwa die Einhaltung der Datenschutzgrundsätze, Verpflichtungen zur Datensicherheit sowie die Pflichten, personenbezogene Daten zu löschen und den Fortbestand des Schutzes zu gewährleisten, wenn die Daten an Dritte weitergegeben werden. Durch die neuen Garantien soll den zuvor geäußerten Bedenken des EuGH Rechnung getragen werden.

Die neuen Regelungen sehen insbesondere strengere Vorgaben für den geheimdienstlichen Zugriff auf Daten von Europäern vor; der Zugriff von amerikanischen Sicherheitsbehörden soll auf ein notwendiges und verhältnismäßiges Maß beschränkt sein. Die Aktivitäten der US-Geheimdienste sollen zudem verstärkt beaufsichtigt werden. Außerdem soll es für EU-Bürger verschiedene unabhängige und unparteiische Rechtsbehelfsmechanismen für den Fall eines aus ihrer Sicht rechtswidrigen Zugriffs auf ihre Daten geben. Hierzu wurde unter anderem vorgesehen, ein Gericht zur Datenschutzüberprüfung (Data Protection Review Court, DPRC) zu schaffen, an das sich Einzelperson in der EU wenden können. Darüber hinaus sind kostenlose unabhängige Streitbeilegungsmechanismen und eine Schiedsstelle vorgesehen.

Bereits im Frühjahr 2022 hatten die Europäische Kommission und die USA eine grundsätzliche Einigung über einen neuen transatlantischen Datenschutzrahmen erzielt. Joe Biden unterzeichnete sodann im Oktober letzten Jahres ein Dekret, das auf amerikanischer Seite die rechtliche Grundlage für einen neuen Rechtsrahmen zur Datenübermittlung in die USA schafft (wir berichteten im November 2022). Die Europäische Kommission legte sodann im Dezember 2022 den Entwurf eines Angemessenheitsbeschlusses für die USA vor und leitete das Verfahren zur Annahme des Angemessenheitsbeschlusses ein. In der Folge haben verschiedene Stellen in der EU, darunter der Europäische Datenschutzausschusss (EDSA) sowie der zuständige Ausschuss des EU-Parlaments (LIBE), zu dem Entwurf Stellung genommen (wir berichteten im April und im Mai 2023. Der EDSA begrüßte die vorgesehen Verbesserungen gegenüber den Vorgängerregelungen, äußerte sich jedoch gleichzeitig kritisch hinsichtlich verschiedener Punkte und bat die Europäische Kommission insoweit um weitergehende Untersuchungen. Die Anmerkungen des EDSA betrafen insbesondere bestimmte Rechte von Betroffenen, die Weiterübermittlung personenbezogener Daten sowie die praktische Funktionsweise des Rechtsbehelfsmechanismus. Ähnlich äußerte sich der LIBE-Ausschuss, der sich jedoch noch deutlicher positionierte und eine Zustimmung ohne den Versuch weiterer Nachverhandlungen mit den USA ablehnte. Er verwies darauf, dass es weiterhin an ausreichenden Garantien fehle und Massenerhebungen personenbezogener Daten in bestimmten Fällen weiterhin zulässig seien. Kritisiert wurde außerdem, dass die Entscheidungen des DPRC geheim sind, wodurch unter anderem das Recht der Bürger auf Zugang zu ihren Daten verletzt werde.

Mittels des neuen Angemessenheitsbeschlusses sollen personenbezogene Daten nach Angaben der Europäischen Kommission nunmehr sicher an amerikanische Unternehmen, die am Data Privacy Framework teilnehmen, übermittelt werden können, ohne dass darüber hinaus weitere Datenschutzgarantien benötigt werden. Präsidentin Ursula von der Leyen erklärte: „Der neue Datenschutzrahmen EU-USA wird einen sicheren Datenverkehr für die Europäerinnen und Europäer gewährleisten und den Unternehmen auf beiden Seiten des Atlantiks Rechtssicherheit bieten. Nach der grundsätzlichen Einigung, die ich im vergangen Jahr mit Präsident Biden erzielt habe, haben die USA beispiellose Zusagen zur Schaffung des neuen Rahmens gemacht. Heute kommen wir einen wichtigen Schritt dabei voran, den Bürgerinnen und Bürgern Vertrauen in die Sicherheit ihrer Daten zu geben, unsere wirtschaftlichen Beziehungen zwischen der EU und den USA zu vertiefen und gleichzeitig unsere gemeinsamen Werte zu stärken. Der Rahmen zeigt, dass wir durch Zusammenarbeit die komplexesten Fragen angehen können."

Der Datenschutzrahmen wird durch das US-Handelsministerium verwaltet und überwacht; für die Durchsetzung der Vorschriften gegenüber zertifizierten US-Unternehmen ist die amerikanische Federal Trade Commission zuständig. Perspektivisch sind zudem regelmäßige Überprüfungen des EU-US Data Privacy Frameworks durch die Europäische Kommission, Vertreter der europäischen Datenschutzbehörden sowie die zuständigen US-Behörden geplant, um zu prüfen, ob die vorgesehenen Maßnahmen umgesetzt wurden und wirksam funktionieren. Eine erste Überprüfung soll innerhalb des nächsten Jahres erfolgen.

Auswirkungen und Handlungsempfehlungen

Der Angemessenheitsbeschluss trat mit seiner Annahme am 10. Juli 2023 in Kraft und gilt seitdem ohne weitere Umsetzungsschritte unmittelbar, sodass Datentransfers prinzipiell ab sofort auf das EU-US Data Privacy Framework gestützt werden können. Da der neue Angemessenheitsbeschluss aber nur für solche Unternehmen Wirkung entfaltet, die sich zur Einhaltung der neuen Datenschutzregelungen verpflichtet haben und dem Abkommen beigetreten sind, müssen Unternehmen im Vorfeld der Datenübermittlung jeweils für den konkreten Fall überprüfen, ob das betreffende amerikanische Unternehmen unter dem EU-US Privacy Data Framework zertifiziert ist. Das U.S. Department of Commerce veröffentlicht eine entsprechende Liste der zertifizierten Unternehmen, die für die Prüfung herangezogen werden kann. Die großen IT-Konzerne wie Microsoft, Google, Meta und Amazon haben sich bereits zur Einhaltung der Bestimmungen verpflichtet und sind dem Abkommen beigetreten, Apple ist demgegenüber bislang noch nicht auf der Liste zu finden.

Der neue Angemessenheitsbeschluss führt zwar auf der einen Seite dazu, dass Datenübermittlungen in die USA wieder leichter abgesichert werden können, lässt auf der anderen Seite aber die, etwa mit Blick auf die Nutzung von Office 365, im Raum stehenden Kritikpunkte nicht automatisch entfallen. Es kann nicht davon ausgegangen werden, dass das EU-US Data Privacy Framework – zumindest aus technischer Sicht – zu mehr Rechtssicherheit führt, da die Datenübermittlungen trotz der vorgesehenen Verbesserungen nicht unmittelbar sicherer werden. In Anbetracht der bereits im Vorfeld der Annahme des Beschlusses von verschiedenen Stellen geäußerten massiven Kritik und des Umstands, dass grundlegende Probleme nach wie vor nicht gelöst wurden, stellt sich außerdem die Frage, wie belastbar der neue Beschluss ist und ob bzw. wann er von der Rechtsprechung erneut für unwirksam erklärt wird. Dass sich der EuGH in näherer Zukunft mit der Frage, ob das EU-US Data Privacy Framework ein ausreichend hohes Datenschutzniveau gewährleisten kann, zu beschäftigen haben wird, steht vermutlich außer Frage. Es ist insoweit auch durchaus denkbar, dass er sich erneut auf die mangelnde Angemessenheit des Datenschutzniveaus berufen und das Abkommen unter Bezugnahme auf seine Entscheidungen zum „Safe Harbor"-Abkommen und zum „EU-US Privacy Shield" für unwirksam erklärt. Unter Berücksichtigung dieser Problematik bietet sich ein doppelter Ansatz in Form der zusätzlichen Vereinbarung von (in vielen Fällen ohnehin bereits vorliegenden) Standardvertragsklauseln an, um sich für den Fall abzusichern, dass der neue Angemessenheitsbeschluss keinen Bestand hat.

Unternehmen sollten in einem ersten Schritt überprüfen, ob sie direkt oder indirekt mit Anbietern aus den USA sowie Dienstleistern, bei denen eine Datenübermittlung in die USA erfolgt, zusammenarbeiten. Trifft dies zu, ist anhand der vom U.S. Department of Commerce zur Verfügung gestellten Liste zu überprüfen, ob das betreffende Unternehmen unter dem EU-US Data Privacy Framework zertifiziert ist. Ist dies der Fall, kann die Datenübermittlung vom Grundsatz her ausschließlich auf den Angemessenheitsbeschluss gestützt werden. Es sollte jedoch überlegt werden, inwieweit es sich anbietet, einen doppelten Ansatz zu verfolgen und den Datentransfer parallel auf weitere Absicherungsmaßnahmen zu stützen. In vielen Fällen wird die Geltung der Standardvertragsklauseln sowie zusätzlicher Maßnahmen ohnehin in der Vergangenheit bereits vereinbart worden sein und könnte beibehalten werden. Datenschutzfreundliche Konfigurationsmöglichkeiten sollten darüber hinaus in jedem Fall gewählt und eine Risikoabwägung für den konkreten Fall vorgenommen werden. Ist das betreffende US-Unternehmen dem Abkommen noch nicht beigetreten, empfiehlt es sich weiterhin, die neuen Standardvertragsklauseln einzubeziehen, gegebenenfalls zusätzliche Absicherungsmaßnahmen zu ergreifen und sich im Rahmen der Vereinbarung zur Auftragsverarbeitung, ggf. durch Zwischenschalten eines europäischen Dienstleisters, zumindest im Innenverhältnis haftungsrechtlich abzusichern. Es bietet sich zudem an, die ergriffenen Maßnahmen zur Absicherung des Datentransfers zu dokumentieren, um eine Auseinandersetzung mit der Problematik nachweisen zu können.

Fazit

Der Einsatz amerikanischer Dienstleister ist im heutigen Unternehmensalltag in vielen Fällen nicht mehr wegzudenken. Eine Übermittlung personenbezogener Daten in einen Drittstaat darf jedoch grundsätzlich nur dann erfolgen, wenn vorab sichergestellt werden kann, dass in dem betreffenden Drittstaat ein Datenschutzniveau gewährleistet wird, das mit dem Datenschutzniveau in der EU vergleichbar ist. Das EU-US Data Privacy Framework stellt ein solche Möglichkeit zur Absicherung von Datentransfer dar und vereinfacht Datenübermittlungen in die USA zumindest zum jetzigen Zeitpunkt. Soll eine Datenübermittlung auf den neuen Angemessenheitsbeschluss gestützt werden, ist gleichsam im Blick zu behalten, dass die eigentlichen Problempunkte hierdurch nicht entfallen, und zu beobachten, wie sich insbesondere der EuGH, aber auch die Datenschutzbehörden im Rahmen der regelmäßigen Überprüfungen zu dem Abkommen positionieren werden. In bestimmten Fällen kann sich insoweit ein doppelter Ansatz anbieten. Gerne unterstützen wir Sie bei der Prüfung und datenschutzkonformen Ausgestaltung der Prozesse.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net