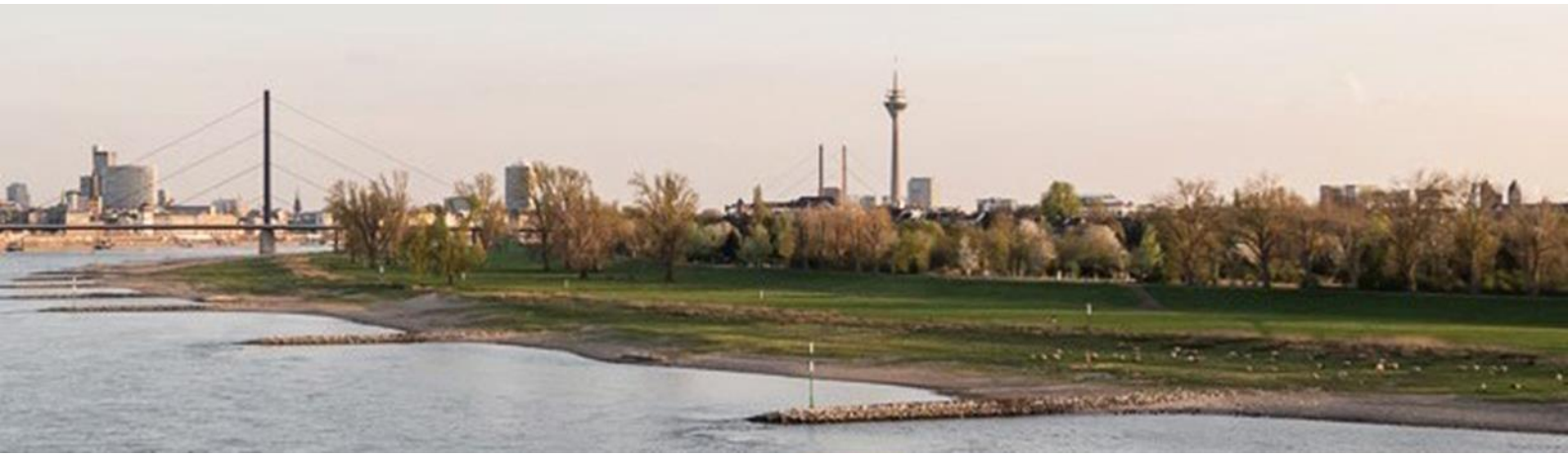

EuGH: Regelungen für Datenübermittlung teilweise ungültig (C-311/18 – „Schrems-II“)

Der EuGH hat im Rahmen eines Vorabentscheidungsverfahrens am 16. Juli 2020 (Rechtssache C-311/18 - „Schrems-II“) den „EU-US Privacy Shield“ - einen Angemessenheitsbeschluss der EU-Kommission (2016/1250) - für nichtig erklärt, da das US-Recht kein den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechendes Schutzniveau für personenbezogene Daten gewährleiste.

Unternehmen, die personenbezogene Daten in Länder außerhalb der EU übermitteln, müssen jetzt umgehend ihre bestehenden Verträge in Bezug auf den Drittstaatentransfer überprüfen.

Den Beschluss 2010/87/EU, mit dem die EU-Kommission Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern erlassen hat, sah der EuGH hingegen zwar als gültig an, stellte jedoch zusätzliche Anforderungen an Verantwortliche, die diese Klauseln im Rahmen ihrer Datenübermittlungen verwenden.

Die Entscheidung des EuGH betrifft einen Großteil der Übermittlungen personenbezogener Daten aus der EU in die USA und ist somit von großer Relevanz, insbesondere auch für europäische Unternehmen, die mit US-Unternehmen kooperieren oder von diesen angebotene Produkte nutzen.

Rechtliche Voraussetzungen für Datenübermittlungen

Die Übermittlung personenbezogener Daten in Drittländer, die nicht Mitgliedstaaten der EU sind sowie Island, Liechtenstein und Norwegen, darf nur unter besonderen Voraussetzungen erfolgen (Art. 44 ff. DSGVO). Es soll sichergestellt werden, dass das besonders hohe Schutzniveau für die Verarbeitung personenbezogener Daten in Europa, das durch die DSGVO geschaffen wurde, nicht umgangen wird. Verantwortliche, die personenbezogene Daten in Drittländer übermitteln wollen, müssen daher

geeignete Garantien für den Schutz der betroffenen Personen vorsehen und diesen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stellen.

Eine Möglichkeit zur Übermittlung personenbezogener Daten ist ein sog. Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO). Mit diesem stellt die Kommission fest, dass in einem bestimmten Drittland ein dem der EU angemessenes Schutzniveau bezüglich des Umgangs mit personenbezogenen Daten besteht.

Die EU-Kommission hatte sowohl mit dem „Safe Harbor"-Abkommen im Jahr 2000 als auch 2016 mit dem „EU-US Privacy Shield" für die USA festgestellt, dass das US-Recht ein angemessenes Datenschutzniveau biete, sodass auf Grundlage dessen personenbezogene Daten grundsätzlich von der EU in die USA übermittelt werden durften.

Neben einem Angemessenheitsbeschluss der EU-Kommission, sehen die Art. 44 ff. DSGVO weitere Möglichkeiten für eine Übermittlung personenbezogener Daten in Drittländer vor. Verantwortlichen selbst stehen als geeignete Garantien unter anderem Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DSGVO) oder Bindung Corporate Rules (BCR, Art 47 DSGVO) zur Verfügung.

Das EuGH-Verfahren

Das nun beendete EuGH-Verfahren (C-311/18) geht ursprünglich auf den österreichischen Datenschützer Max Schrems zurück. Dieser ist Facebooknutzer und hatte 2013 bei der für Facebook Ireland zuständigen irischen Datenschutzaufsichtsbehörde (Data Protection Commissioner, „DPC") Beschwerde bezüglich Facebook Irelands Praxis der Datenübermittlung an die Facebook Inc. in den USA eingelegt.

Max Schrems forderte in seiner Beschwerde, Facebook Ireland die Datenübermittlung in die USA zu untersagen, da das Recht der USA keinen ausreichenden Schutz der dort gespeicherten personenbezogenen Daten gewährleiste, insbesondere hinsichtlich diverser Befugnisse der US-Geheimdienste. Der DPC wies die Beschwerde mit Hinweis auf das „Safe Harbor"-Abkommen zurück, da ein ausreichendes Schutzniveau gewährleistet sei. Infolge dessen erklärte der EuGH das „Safe Harbor"-Abkommen 2015 für ungültig (C-362/14, „Schrems-I").

Infolge der Ungültigkeitserklärung wies Facebook darauf hin, dass Daten der Facebooknutzer nicht auf Grundlage des Abkommens, sondern vielmehr auf Grundlage der Standarddatenschutzklauseln (SDK-Beschluss 2010/87) übermittelt würden. Max Schrems änderte daraufhin seine Beschwerde gegenüber dem DPC und machte insbesondere geltend, auch die Standarddatenschutzklauseln sowie der SDK-Beschluss könnten die Datenübermittlung nicht rechtfertigen, da der Datenimporteur (hier: Facebook Inc.) aufgrund diverser US-Gesetze verpflichtet sei, übermittelte Daten amerikanischen Behörden (u.a. NSA, FBI) zur Verfügung zu stellen und somit die sich aus den Standarddatenschutzklauseln ergebenden Verpflichtungen gar nicht einhalten könne.

Auch der DPC äußerte im Anschluss die Befürchtung, die Standarddatenschutzklauseln könnten als vertragliche Rechte nicht geeignet sein, den von der Datenübermittlung betroffenen Personen ausreichende Rechte gegenüber Facebook einzuräumen, ohne die amerikanischen Behörden zu binden. Der DPC hatte somit Zweifel an der Gültigkeit des SDK-Beschlusses und rief daher den irischen High Court an, der dem EuGH

nachfolgend einige Fragen zur Vorabentscheidung vorlegte, u.a. nach der Gültigkeit des SDK-Beschlusses sowie (inzident) nach der Gültigkeit des „Privacy Shield".

Die Entscheidungen des EuGH („Schrems-II")

„Privacy Shield"

Der EuGH entschied nun, dass der Angemessenheitsbeschluss „Privacy Shield" ungültig sei, da er nicht den sich aus der DSGVO sowie der Charta der Grundrechte der EU ergebenden Anforderungen entspreche. Die USA böten kein der EU angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten. Dies habe die EU-Kommission bei ihrer Beschlussfassung verkannt. Datenübermittlungen von der EU in die USA können somit nicht mehr auf den „Privacy Shield" gestützt werden.

Der EuGH stellte fest, dass der Erlass eines Angemessenheitsbeschlusses durch die EU-Kommission die Feststellung erfordere, dass das betreffende Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften tatsächlich ein Schutzniveau der Grundrechte gewährleiste, das dem in der EU garantierten Niveau der Sache nach gleichwertig sei.

Der Privacy Shield-Beschluss sehe unter anderem vor, dass die darin enthaltenen Grundsätze insoweit eingeschränkt sein könnten, *„als Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss*". Aufgrund dessen seien die US-Organisationen, die vom „Privacy Shield" erfasst seien, ohne jede Einschränkung verpflichtet, die Grundsätze des „Privacy Shield" unangewendet zu lassen, wenn sie in Widerstreit zu den Erfordernissen des US-Rechts stehen.

Für die Einschränkung von Grundrechten enthalte das EU-Recht jedoch konkrete Voraussetzungen, die im Sinne eines angemessenen Schutzniveaus insoweit auch im US-Recht bestehen müssten. Insbesondere dürfe der Wesensgehalt eines Grundrechts nicht angetastet werden und Einschränkungen der Grundrechte müssten verhältnismäßig sein (Art. 52 EU-GRCh).

In die Grundrechte auf Privatheit und Datenschutz (Art. 7, Art. 8 EU-GRCh) eingreifende Regelungen müssten somit Mindesterfordernisse für Einschränkungen aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichten. Im Hinblick auf die Prüfung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus ergebe sich so unter anderem das Erfordernis *„wirksamer und durchsetzbarer Rechte der betroffenen Personen*" (Art. 45 Abs. 2 lit. a DSGVO).

Die US-Gesetze, die einen Zugriff insbesondere der US-Geheimdienste auf aus der EU übermittelte, personenbezogene Daten ermöglichten, enthielten allerdings keine den Anforderungen entsprechenden Einschränkungen. Ebenso wenig sei erkennbar, dass für potenziell von den Programmen der US-Geheimdienste erfasste Nicht-US-Personen, also auch EU-Bürger, Garantien zum Schutz ihrer Rechte existierten. Im US-Recht bestehe daher kein Schutzniveau, das dem durch die Charta garantierten Niveau der Sache nach gleichwertig sei.

Zudem sei das durch Art. 47 der EU-Grundrechtecharta garantierte Recht, bei einem unabhängigen und unparteiischen Gericht

einen wirksamen Rechtsbehelf einzulegen, durch das „Privacy Shield“ nicht gewährleistet. Insbesondere sei dieses Recht nicht hinreichend durch die Einsetzung einer Ombudsperson des „Privacy Shields“ ausgefüllt worden. Daher bestehe auch insoweit im US-Recht kein dem Niveau der EU gleichwertiges Schutzniveau für betroffene Personen.

Aus diesen Feststellungen folgerte der EuGH, dass das US-Recht insgesamt kein dem Niveau der EU angemessenes Schutzniveau für den Umgang mit personenbezogenen Daten gewährleiste und nicht den Anforderungen des Art. 45 Abs. 3 DSGVO entspreche, sodass der „Privacy Shield“-Beschluss ungültig sei.

„Standarddatenschutzklauseln“

Mit dem Abschluss von Standardvertragsklauseln können grundsätzlich personenbezogene Daten in Drittländer übermittelt werden, für die kein Angemessenheitsbeschluss besteht. Die Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO werden dabei zwischen dem sogenannten Datenexporteur und dem Datenimporteur abgeschlossen und dürfen in ihrem gesetzlich vorgegebenen Text dabei grundsätzlich nicht verändert oder angepasst werden.

Den SDK-Beschluss (2010/87) - und somit im Ergebnis die entsprechenden Standarddatenschutzklauseln - sah der EuGH hingegen als gültig an, unabhängig des Umstandes, dass der Beschluss keinerlei Bindungswirkung für die Behörden des Drittlandes entfalte. Der SDK-Beschluss sehe wirksame Mechanismen vor, mit denen in der Praxis grundsätzlich gewährleistet werden könne, dass die auf die Standarddatenschutzklauseln gestützte Übermittlung personenbezogener Daten in ein Drittland ausgesetzt oder verbotene werden könne, wenn der Datenimporteur die entsprechenden Klauseln nicht einhält oder nicht einhalten kann. Ohne einen Angemessenheitsbeschluss liege es grundsätzlich in der Verantwortung des jeweiligen Datenexporteurs, geeignete Garantien vorzusehen.

Sofern festgestellt würde, dass ein Datenimporteur die in den Standarddatenschutzklauseln enthaltenen Verpflichtungen nicht einhalten könne, seien die Datenschutzaufsichtsbehörden, sofern kein gültiger Angemessenheitsbeschluss vorliegt, verpflichtet, Datenübermittlungen auszusetzen oder zu verbieten, sofern der erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann und der entsprechende Verantwortliche, insbesondere also der Datenexporteur, die Übermittlung nicht bereits selbst ausgesetzt oder beendet hat.

Auch für den verantwortlichen Datenexporteur, also beispielsweise das Unternehmen, das personenbezogene Daten in die USA übermittelt, bestehe die entsprechende Pflicht zur Aussetzung oder Beendigung der Übermittlung, wenn es Kenntnis von entsprechenden Mängeln des Datenimporteurs erhält. Um das erforderliche Schutzniveau zu gewährleisten, könne es sich, je nach der in einem bestimmten Drittland gegebenen Lage, grundsätzlich auch als notwendig erweisen, die in den Standarddatenschutzklauseln enthaltenen Garantien zu ergänzen.

Art. 46 Abs. 2 lit. c DSGVO, der die Verwendung der Standarddatenschutzklauseln vorsieht, beruhe darauf, dass das Verantwortungsbewusstsein der in der EU ansässigen Verantwortlichen, und in zweiter Linie der Datenschutzaufsichtsbehörden, geweckt werde. Der EuGH formuliert in seinem

Urteil eine dementsprechende, konkrete Anforderung an Verantwortliche in der EU:

„Folglich obliegt es vor allem diesem Verantwortlichen (…), in jedem Einzelfall - gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung - zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren.“

Der verantwortliche Datenexporteur müsse demnach selbst überprüfen, ob das Recht des jeweiligen Drittlandes entsprechende zusätzliche Maßnahmen erfordere. Sofern der Verantwortliche keine hinreichenden, zusätzlichen Maßnahmen zur Gewährleistung des erforderlichen Schutzniveaus ergreife, sei er - und in zweiter Linie die Datenschutzaufsichtsbehörde - verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden. Der SDK-Beschluss selbst sehe entsprechende Mechanismen vor, eine solche Aussetzung oder ein Verbot der Übermittlung im jeweiligen Einzelfall zu ermöglichen.

Handlungspflichten für Unternehmen

Das Urteil des EuGH und die darin enthaltenen Feststellungen sind von großer Relevanz, insbesondere für sämtliche Unternehmen in der EU, die personenbezogene Daten in die USA, aber auch andere Drittländer, übermitteln. Eine Übermittlung personenbezogener Daten findet dabei häufig bereits bei der Verwendung von Produkten von Unternehmen, die ihren Sitz in einem Drittland haben, statt. Insbesondere die Feststellungen des EuGH zu den Anforderungen an die Verwendung von Standarddatenschutzklauseln gelten zudem nicht nur für Datenübermittlungen in die USA, sondern grundsätzlich für sämtliche Datenübermittlungen in Drittländer.

Die Aufgaben und Handlungspflichten für Unternehmen in entsprechenden Situationen hat der EuGH selbst recht eindeutig formuliert. So können Unternehmen Datenübermittlungen in die USA nun nicht mehr auf den „Privacy Shield“ stützen. Daraus ergibt sich die Anforderung, anderweitige datenschutzrechtliche Garantien für entsprechende Datenübermittlungen vorzusehen. Insoweit kommen insbesondere Standarddatenschutzklauseln oder sog. Binding Corporate Rules (BCR), also verbindliche interne Datenschutzvorschriften, in Betracht, wobei sich Letztere in praktischer Hinsicht grundsätzlich nur für Übermittlungen innerhalb von Konzernen eignen dürften. In bestimmten Einzelfällen können sich Ausnahmen für Datenübermittlungen ergeben (Art. 49 DSGVO).

Doch auch bei der Verwendung von Standarddatenschutzklauseln beschränken sich die von Unternehmen zu ergreifenden Maßnahmen nicht (mehr) auf den bloßen Abschluss der entsprechenden Verträge. Unternehmen sind, gegebenenfalls in Zusammenarbeit mit dem Datenimporteur, verpflichtet, genau zu überprüfen, ob die entsprechenden Klauseln von dem Datenimporteur im Hinblick auf das für ihn geltende Recht des Drittlandes überhaupt eingehalten werden können, sofern kein gültiger Angemessenheitsbeschluss der EU-Kommission für das betreffende Drittland besteht. Diese Prüfung dürfte sich für Unternehmen in praktischer Hinsicht oftmals als schwierig und komplex erweisen. Gegebenenfalls

müssen Unternehmen weitere Maßnahmen ergreifen, um das erforderliche Schutzniveau zu gewährleisten, wobei sich diese zusätzlichen Maßnahmen am jeweiligen Einzelfall orientieren müssen.

Ein erster Schritt für Unternehmen sollte nun die Überprüfung sämtlicher Verträge in Bezug auf Datenübermittlungen in Drittländer, insbesondere in die USA, sein. Entsprechende Datenübermittlungen können sich dabei bereits aus der Verwendung von Produkten (Software etc.) ergeben, sofern die Produktanbieter ihren Sitz in einem Drittland haben. Zudem sollten Verträge mit anderen Verantwortlichen (Joint Control Agreement) und Auftragsverarbeitern (Data Protection Agreement) überprüft und erforderliche Anweisungen getätigt werden.

Einige deutsche Datenschutzaufsichtsbehörden (u.a. Hamburg, Rheinland-Pfalz) haben sich bereits zu dem Urteil geäußert und angekündigt, nun bei Datenübermittlungen „ganz genau hinzuschauen“. Zudem haben sie betont, dass es keine Karenzzeit gebe. Daher sind Unternehmen gehalten, sich kurzfristig mit diesem Thema zu beschäftigten und entsprechende Maßnahmen zu ergreifen.

Kontakt

Dr. Philipp Mels
Rechtsanwalt, Fachanwalt für Gewerblichen Rechtsschutz, Partner

T +49 211 60035-180
philipp.mels@orthkluth.com
Kaistraße 6, 40221 Düsseldorf
orthkluth.com

Prof. Dr. Michael Bohne
Of-Counsel

T +49 211 60035-174
michael.bohne@orthkluth.com
Kaistraße 6, 40221 Düsseldorf
orthkluth.com

Dr. Michael Grobe-Einsler
Rechtsanwalt, Associate

T +49 211 60035-450
michael.grobe-einsler@orthkluth.com
Kaistraße 6, 40221 Düsseldorf
orthkluth.com

Felix Meurer
Wissenschaftlicher Mitarbeiter

T +49 211 600350
felix.meurer@orthkluth.com
Kaistraße 6, 40221 Düsseldorf
orthkluth.com