++++ FACHARTIKEL ++++

Datenschutz: Das Ende des Privacy-Shield-Abkommens – was nun?

1. Die Kernaussagen der EuGH-Entscheidungen

Der EuGH hat in seinem Urteil vom 16. Juli 2020 (Aktenzeichen: C-311/18) zwei wesentliche Feststellungen getroffen. Zunächst hat er das Privacy-Shield-Abkommen für unwirksam erklärt und weiterhin hat er festgestellt, dass die sogenannten Standarddatenschutzklauseln weiterhin als Grundlage für die Übermittlung personenbezogener Daten an Drittländer herangezogen werden können. Das klingt zunächst, als könnten Unternehmen, die mit US-amerikanischen Unternehmen kooperieren nach dem ersten Schreck aufatmen und ihre Datenübermittlung zukünftig auf Standarddatenschutzklauseln stützen – doch so einfach macht es der EuGH den europäischen Unternehmen leider nicht.

2. Zu den Hintergründen des Urteils

Gesetzlicher Hintergrund des EuGH-Urteils ist der Umstand, dass die DSGVO für Datenübermittlungen in sogenannte Drittländer – das sind Länder außerhalb der EU, für welche die DSG-VO daher keine unmittelbare Anwendung findet – ein Datenschutzniveau verlangt, das mit den Datenschutzanforderungen der DSGVO jedenfalls vergleichbar ist. Um die Gleichwertigkeit des Datenschutzniveaus in einem Drittland sicherzustellen, gibt es verschiedene Möglichkeiten. Zum einen erlässt die Europäische Kommission sogenannte Angemessenheitsbeschlüsse, mit denen diese offiziell feststellt, dass in einem Drittland ein vergleichbares Datenschutzniveau herrscht. Die Datenübermittlung in ein solches Land (z. B. die Schweiz, Kanada, Japan, Neuseeland oder Argentinien) bedarf dann keiner weiteren Genehmigung im Vorfeld. Eine weitere Möglichkeit der Absicherung bezüglich eines gleichwertigen Datenschutzniveaus in einem Drittland besteht in der Verwendung sogenannte Standarddatenschutzklauseln. Dabei handelt es sich um vorformulierte und von der Europäischen Kommission genehmigte Vertragsklauseln, welche zwischen denjenigen Personen, zwischen denen eine Datenübermittlung stattfindet, abgeschlossen werden. Eine weitere Möglichkeit, personenbezogene Daten datenschutzkonform in ein Drittland ohne angemessenes Datenschutzniveau zu übermitteln, besteht darin, verbindliche interne Datenschutzvorgaben, die durch die Aufsichtsbehörde geprüft werden, festzulegen und auf deren Grundlage Datenübermittlungen vorzunehmen (sog. Binding Corporate Rules). Für bestimmte Verarbeitungssituationen sieht darüber hinaus Art. 49 DSGVO im Ausnahmefall die Zulässigkeit der Datenübermittlung an ein Drittland vor, wenn kein Angemessenheitsbeschluss existiert oder geeignete Garantien, z. B. in Form von Standarddatenschutzklauseln, bestehen.

Für Datenübermittlungen zwischen europäischen und US-amerikanischen Unternehmen bestand daneben das EU-US-Privacy-Shield, mit dessen Unterzeichnung sich die jeweiligen amerikanischen Unternehmen zur Einhaltung bestimmter Datenschutzvorkehrungen

verpflichteten. Man ging daher bislang davon aus, dass die Datenübermittlung an amerikanische Unternehmen, die das Privacy-Shield-Abkommen unterzeichnet haben, datenschutzkonform erfolgt.

Nunmehr hat der EuGH mit Urteil vom 16. Juli 2020 entschieden, dass das Privacy-Shield unwirksam ist, also keine Datenübermittlung in die USA legitimieren kann, da insbesondere die Tatsache problematisch ist, dass amerikanische Unternehmen von den amerikanischen Sicherheitsbehörden verpflichtet werden können, personenbezogene Daten – auch solche nicht-amerikanischer Bürger und Bürgerinnen herauszugeben, ohne dass die betroffenen Personen angemessene Rechtsschutzmöglichkeiten dagegen hätten.

3. Relevanz des EuGH-Urteils

Das Urteil ist demnach zunächst für all diejenigen Unternehmen relevant, die Daten an die USA übermitteln, z. B. weil sie amerikanische Cloud-Dienste oder Software nutzen, die einen Daten-transfer erfordern oder weil sie US-amerikanischen Unternehmen z. B. im Rahmen von IT-Wartungsverträgen den Zugriff auf personenbezogene Daten erlauben. Erfolgt die Datenübermittlung nicht auf der Basis von Standarddatenschutzklauseln, sondern auf der Privacy-Shield-Zertifizierung des amerikanischen Unternehmens, so gibt es unmittelbaren Handlungsbedarf, da das Privacy-Shield-Abkommen keine taugliche Übermittlungsrundlage mehr darstellt.

Die Tücke des EuGH-Urteils besteht jedoch darin, dass es sich nicht nur auf Datenübermittlungen an US-Unternehmen auswirkt, die bisher auf die Privacy-Shield-Zertifizierung des US-amerikanischen Unternehmens gestützt wurden. Vielmehr beeinflusst die Entscheidung auch solche Datenübermittlungen in die USA, die auf Standarddatenschutzklauseln oder Binding Corporate Rules beruhen sowie Datenübermittlungen in andere Drittländer, für die kein Angemessenheitsbeschluss besteht.

Der EuGH stellte in seinem Urteil fest, dass auch Standarddatenschutzklauseln – und die Über-legung lässt sich auch auf Binding Corporate Rules übertragen – keine ausreichende Grundlage für Datenübermittlungen in Drittländer darstellen, wenn die Vereinbarungen nicht genügen, um in dem Drittland ein angemessenen Datenschutzniveau sicherzustellen. Diese Prüfung obliegt der für die Datenverarbeitung verantwortlichen Person, welche sodann gegebenenfalls ergänzende Garantien für die Datenverarbeitung vorzusehen hat. Welche Garantien geeignet sind, ein unzureichendes Datenschutzniveau im Einzelfall zu kompensieren, ist vorerst nicht geklärt. Vereinbarungen zwischen dem datenexportierenden Unternehmen mit Sitz in der EU und dem datenimportierenden Unternehmen mit Sitz in den USA können jedoch von vornherein nur Wirkung zwischen den Vertragsparteien entfalten und binden insbesondere keine ausländischen Nachrichtendienste und Sicherheitsbehörden. Insofern als die US-Nachrichtendienste in großem Stil zur Einsichtnahme in personenbezogene Daten gegenüber US-Unternehmen befugt sind, fehlt es somit an Handlungsoptionen europäischer Unternehmen, um ein angemessenes Datenschutzniveau zur Datenübermittlung in die USA sicherzustellen. Auch die Datenschutzaufsichtsbehörden sind insofern verpflichtet, Datenübermittlungen an Drittländer im Hinblick auf ein

angemessenes Schutzniveau im Zielland zu überprüfen und die Datenübertragung erforderlichenfalls zu unterbinden.

4. Maßnahmen für eine rechtskonforme Datenübermittlung in Drittländer

Im Hinblick auf Datenverarbeitungsvorgänge in Unternehmen, die bisher an US-Unternehmen delegiert wurden, bestünde die rechtssicherste Handlungsoption darin, die bisher delegierten Aufgaben wieder in eigener Verantwortung zu übernehmen oder dazu beispielsweise auf Auftragsverarbeiter in der EU zurückzugreifen. Dass Standarddatenschutzklauseln oder Binding Corporate Rules ausreichen, um eine Datenübermittlung in die USA zukünftig zu rechtfertigen, ist nach der EuGH-Entscheidung äußerst zweifelhaft. Unternehmen haben jedoch die Möglichkeit – und darauf weist auch der EuGH am Schluss seiner Entscheidung hin –, sich auf die Aus-nahmen für bestimmte Fälle in Art. 49 DSGVO für die Datenübermittlung zu berufen. Danach können Daten zum Beispiel auch zur Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen oder auf der Basis einer ausdrücklichen Einwilligung der betroffenen Person an ein Drittland übermittelt werden. Dabei gilt es jedoch zu bedenken, dass die Vertrags-durchführung die Datenübermittlung nur zu legitimieren vermag, wenn der Vertrag zwischen dem amerikanischen Unternehmen und der betroffenen Person selbst geschlossen wurde. Kundendaten eines Unternehmens, das einen Vertrag mit einem amerikanischen Unternehmen geschlossen hat, können auf dieser Basis nicht verarbeitet werden. Die Ausnahmetatbestände des Art. 49 DSGVO gelten zudem nur ergänzend zu den allgemeinen Bestimmungen der DSGVO. Soweit von der Datenübermittlung in das nicht-europäische Ausland demnach beispielsweise gesundheitsbezogene Daten betroffen sind, müssen ergänzend zu den Bestimmungen des Art. 49 DSGVO auch die Voraussetzungen von Art. 9 DSGVO hinzutreten.

Soweit personenbezogene Daten eines Unternehmens an ein anderes Drittland als die USA ohne Angemessenheitsbeschluss übermittelt werden sollen, kann grundsätzlich auf Standarddatenschutzklauseln oder Corporate Binding Rules zurückgegriffen werden. Jedoch ist, wie dargelegt, durch das verantwortliche Unternehmen jeweils zu prüfen, ob in dem betreffenden Land auf der Grundlage der getroffenen Vereinbarungen ein angemessenes Datenschutzniveau sichergestellt werden kann. Zur Beantwortung dieser Frage lohnt sich gegebenenfalls auch ein offener Austausch mit der zuständigen Datenschutzbehörde.

5. Don't panic!

Das EuGH Urteil wird den Umgang mit personenbezogenen Daten bei der Übermittlung von Daten in die USA und andere Drittländer erst einmal durcheinanderwirbeln und niemand kann angesichts der massiven Veränderung der Rechtslage erwarten, dass jedes noch so kleine Unter-nehmen gleich eine Patentlösung an der Hand an. Daher ist kein Grund zur Panik geboten!

Die betroffenen Unternehmen sollten sich jedoch zeitnah mit den Verlautbarungen der

nationalen und europäischen Datenschutzbehörde(n) und den aktuellen Entwicklungen beschäftigen, um ihr Datenschutzkonzept kurzfristig anpassen zu können.

Der Bundesdatenschutzbeauftragte hat das Urteil in einer Stellungnahme bereits begrüßt und angekündigt, in den besonders relevanten Fällen, auf die schnelle Umsetzung der Konsequenzen aus dem EuGH-Urteil zu drängen. Es soll zudem kurzfristig eine Beratung des Europäischen Datenschutzausschusses erfolgen und danach will sich der der Bundesdatenschutzbeauftragte erneut äußern. Die Europäische Kommission hat mit dem Urteil des EuGHs rechnen müssen und daher bereits alternative Instrumente, wie auch eine Überarbeitung der Standarddatenschutzklauseln, angedacht. Es bleibt demnach zu hoffen, dass den betroffenen Unternehmen seitens der Aufsichtsbehörden zeitnah Leitlinien an die Hand gegeben werden, die den Umgang mit grenzüberschreitender Datenverarbeitung erleichtern.

Ansprechpartner:

Prof. Heralt Hug
Augustusplatz 9, 04109 Leipzig
Tel. +49 341 21 67 2135
Mail: Heralt.Hug@cms-hs.com; Web: https://cms.law/de/deu/?rfb=enldeu