LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Litigation & Trial and Data Privacy & Security Practices

24 Juli 2020 | Nummer 2781

Das *Schrems II*-Urteil des EuGH: Was müssen Unternehmen bei internationalen Datentransfers ändern?

Das Privacy Shield zur Datenübermittlung in Drittländer ist ungültig. Die EU-Standarddatenschutzklauseln dürfen Unternehmen weiter einsetzen, allerdings nur in eigener Verantwortung und nach einer Einzelfallprüfung.

Der Europäische Gerichtshof (EuGH) hat in einem wegweisenden Urteil (Urteil vom 16. Juli 2020, Rechtssache C-311/18 — „***Schrems II***“) über Instrumente für internationale Datentransfers entschieden. Er hat den sogenannten *EU-U.S.-Privacy Shield* (Beschluss 2016/1250 — „***Privacy Shield***“) für unwirksam erklärt. Zugleich entschied der EuGH auch über die sogenannten EU-Standarddatenschutzklauseln (Beschluss 2010/87/EU — „**Standarddatenschutzklauseln**“). Diese sind nach dem Gericht zwar wirksam und dürfen weiterhin eingesetzt werden. Allerdings müssen Unternehmen beim Einsatz der Standarddatenschutzklauseln künftig im Einzelfall prüfen, ob die Gesetze im Empfängerland den darin enthaltenen Vertragspflichten entgegenstehen. Damit bleibt die Überprüfung den übermittelnden Unternehmen überlassen, ob im Drittland das geforderte Schutzniveau für die auf Basis der Standarddatenschutzklauseln übermittelten Daten tatsächlich eingehalten wird. Ist dies nicht der Fall, drohen einige Datenschutzaufsichtsbehörden damit, künftig einzuschreiten.

Anforderungen an Datentransfers in Drittländer

Für internationale Datentransfers in Länder außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftraums (EWR) sieht die EU-Datenschutz-Grundverordnung (DSGVO) zusätzliche Anforderungen vor. Bei solchen Drittlandtransfers muss stets gewährleistet sein, dass in dem jeweiligen Drittland des Empfängers ein angemessenes Schutzniveau hinsichtlich der übermittelten personenbezogenen Daten herrscht. Dies Niveau können Unternehmen auf verschiedenen Wegen sicherstellen.

Hat die Kommission mit einem Angemessenheitsbeschluss festgestellt, dass ein bestimmtes Drittland das geforderte angemessene Schutzniveau generell gewährleistet, dürfen Unternehmen ohne Weiteres Daten dorthin transferieren (eine Liste der angemessenen Drittländer ist hier verfügbar).

Liegt für das jeweilige Empfängerdrittland kein derartiger Beschluss vor, darf eine Übermittlung dorthin nur erfolgen, wenn das Daten exportierende Unternehmen aktiv Schutzmechanismen umsetzt. Die DSGVO hält eine Reihe solcher Schutzmechanismen bereit.

- In der Praxis am gebräuchlichsten sind von der EU-Kommission verabschiedeten Standarddatenschutzklauseln. Mit deren Abschluss verpflichtet sich das Daten importierende Unternehmen im Drittland gegenüber dem EU-Unternehmen vertraglich, die übermittelten Daten gemäß bestimmten EU-Datenschutzstandards zu verwenden. Die Unternehmen müssen diese Klauseln mit unverändertem Inhalt abschließen.

- Für Datentransfers in die USA bestand bislang für dort ansässige Unternehmen die Möglichkeit, sich unter dem *Privacy Shield* zu zertifizieren und sich damit freiwillig bestimmten zwischen der EU und den USA vereinbarten Datenschutzstandards zu unterwerfen. Auf diese Weise konnten teilnehmende US-Unternehmen ein angemessenes Schutzniveau für an sie transferierte Daten herstellen.

- In Konzernen können Unternehmen schließlich *Binding Corporate Rules* („**BCR**“) für Drittlandübermittlungen implementieren. Diese rechtfertigen jedoch nur konzerninterne Datentransfers und bedürfen einer aufwendigen Genehmigung durch eine Aufsichtsbehörde.

Hintergrund der Entscheidung

Das EuGH-Urteil geht auf eine Beschwerde des Datenschutzaktivisten Maximilian Schrems im Zusammenhang mit dem damaligen Safe Harbour-Abkommen für transatlantische Datentransfers bei der Nutzung von Facebook zurück. Mit dieser rügte er, dass seine Nutzerdaten in die USA übermittelt und dort aufgrund geltender Sicherheitsgesetze dem weitreichenden Zugriff von Behörden — etwa der NSA und des FBI im Rahmen von Überwachungsprogrammen — ausgesetzt seien. In einem ersten Urteil erklärte der EuGH das Safe Harbour-Abkommen für ungültig (Urteil vom 6. Oktober 2015, Rechtssache C-362/14 — „Schrems I“).

Nach dem Urteil änderte Herr Schrems seine Beschwerde ab und griff auch die Gültigkeit der von vielen Unternehmen ebenfalls für US-Datentransfers eingesetzten Standarddatenschutzklauseln an. Auch diese wurden schließlich dem EuGH zur Überprüfung vorgelegt. Zudem warf der mit dem Rechtsstreit befasste Irische High Court die Frage der Wirksamkeit des Privacy Shield auf, das zwischenzeitlich als Nachfolger des Safe Harbour-Abkommens in Kraft getreten war, und legte sie dem EuGH vor.

Das *Schrems II*-Urteil des EuGH

Neben einer Reihe weiterer Fragen hatte der EuGH im *Schrems II*-Urteil über die Gültigkeit des *Privacy Shield* sowie der Standarddatenschutzklauseln zu befinden. Im Wesentlichen entschied das Gericht Folgendes:

- Der *Privacy Shield* ist wegen Verstoßes gegen das EU-Datenschutzrecht unwirksam. Datenübermittlungen in die USA allein auf Basis des *Privacy Shield* sind künftig nicht mehr zulässig.

- Dagegen sind die Standarddatenschutzklauseln weiterhin gültig, da sie aufgrund der darin enthaltenen Vertragsklauseln grundsätzlich ein angemessenes Schutzniveau gewährleisten können.

- Allerdings sind Unternehmen beim Einsatz der Standarddatenschutzklauseln künftig dazu verpflichtet, im Einzelfall zu prüfen, ob in dem jeweiligen Drittland — insbesondere unter Berücksichtigung der dortigen nationalen Sicherheitsgesetze — tatsächlich ein angemessenes Datenschutzniveau eingehalten wird. Ist dies zu verneinen, muss das Unternehmen die Datenübermittlung stoppen.

- Auch die Datenschutzbehörden müssen auf Standarddatenschutzklauseln gestützte Datenübermittlungen im Einzelfall aussetzen oder verbieten, wenn sie zu dem Schluss gelangen,

dass es dem Empfänger in dem betreffenden Drittland nicht möglich ist, die Pflichten aus den Standarddatenschutzklauseln einzuhalten, weil die dortige Rechtslage entgegensteht.

Zunächst stellt der EuGH fest, dass auf den gesamten Vorgang der Datenübermittlung in das Drittland einschließlich der dortigen Verarbeitungen EU-Datenschutzrecht als Bewertungsmaßstab Anwendung findet. Dies gilt selbst, wenn die übermittelten Daten im Empfängerland von den dortigen Sicherheitsbehörden für Zwecke der nationalen Sicherheit verarbeitet werden. Es ist durchgehend ein angemessenes Datenschutzniveau zu gewährleisten. Dieses muss der Sache nach gleichwertig sein wie das in der EU durch die DSGVO nach Maßgabe der EU-Grundrechte-Charta garantierte Schutzniveau.

Ungültigkeit des Privacy Shields

Nach diesen Maßstäben stellt der *Privacy Shield* nach Auffassung des EuGH kein angemessenes Datenschutzniveau sicher und biete deshalb keine wirksame Grundlage für Datentransfers in die USA. Grund hierfür sei, dass die US-amerikanischen Sicherheitsgesetze den zuständigen Behörden weitreichende Zugriffsbefugnisse auf personenbezogene Daten einräumten, ohne dass die Betroffenen europäischen Staatsbürger eine gerichtliche Kontrolle erreichen könnten. Diese Eingriffe in die nach der EU-Grundrechtecharta geschützten Rechte auf Achtung der Privatsphäre (Art. 7 Charta), Schutz personenbezogener Daten (Art. 8 Charta) und effektiven gerichtlichen Rechtsschutz (Art. 47 Charta) seien nach EU-Standards nicht wirksam begrenzt. Auch die Regeln des *Privacy-Shields* räumten der Einhaltung der US-Sicherheitsgesetze gegenüber den Betroffenenrechten den Vorrang ein.

Gültigkeit der Standarddatenschutzklauseln

Die Standarddatenschutzklauseln bewertet der EuGH hingegen als gültig. Sie enthielten wirksame Schutz-mechanismen, die in der Praxis sicherstellen könnten, dass das verlangte Schutzniveau eingehalten wird. So versichere der Empfänger, keinen Gesetzen im Drittland zu unterliegen, die ihm das Einhalten seiner Pflichten aus den Standarddatenschutzklauseln unmöglich machen und etwaige Änderungen sofort mitzuteilen. Dass die Standarddatenschutzklauseln für die Behörden des Drittlands nicht bindend seien, ändere daran nichts. Daher seien die Klauseln grundsätzlich eine taugliche Basis für Drittlandtransfers.

Neue Prüfpflichten für Unternehmen und Datenschutzbehörden

Allerdings macht das Gericht eine wichtige Einschränkung. Setzen Unternehmen Standarddatenschutzklauseln ein, hätten sie umfangreiche Prüfpflichten. Das betreffende Unternehmen müsse bei jeder Datenübermittlung anhand aller Umstände des Einzelfalls prüfen, ob in dem jeweiligen Drittland das erforderliche Schutzniveau tatsächlich eingehalten werden kann. Dies sei nicht der Fall, wenn es nationalen Sicherheitsgesetze im Drittland dem Empfänger unmöglich machten, seine Pflichten aus den Standarddatenschutzklauseln einzuhalten, weil er entgegen den Garantien in den Klauseln Daten offenlegen muss. Könne das Unternehmen das Schutzniveau auch nicht mit anderen Mitteln herstellen, habe es die Datenübermittlung von Beginn an zu unterlassen oder sofort auszusetzen bzw. zu beenden.

Auch die Datenschutzbehörden unterliegen nach dem EuGH einer solchen Prüfplicht. Sie seien verpflichtet, auf Standarddatenschutzklauseln gestützte Datenübermittlungen im Einzelfall auszusetzen oder zu verbieten, wenn sie zu dem Schluss kommen, dass es dem Empfänger in dem Drittland nicht möglich ist, seine Pflichten aus den Standarddatenschutzklauseln einzuhalten. Die Aufsichtsbehörden sollten laut EuGH kein Ermessen haben, von einem Einschreiten abzusehen.

Praxisfolgen und Handlungsempfehlungen für Unternehmen

Die praktischen Auswirkungen des Schrems II-Urteils für den internationalen Datenaustausch und Geschäftsprozesse von Unternehmen sind erheblich.

Sofortiger Wegfall des Privacy Shield

Nach dem Safe Harbor-Abkommen fällt mit dem Privacy Shield nun erneut ein Instrument speziell für Datentransfers zwischen der EU und den USA ersatzlos weg. Dies wirkt sich vor allem auf Unternehmen aus, die personenbezogene Daten bislang allein auf Grundlage des Privacy Shield in die USA übermittelt haben. In der Praxis setzten Unternehmen bei solchen Datentransfers aber selten allein auf den Privacy Shield. Die meisten verwenden zugleich auch Standarddatenschutzklauseln. Eine einzige Rechtsgrundlage reicht für eine zulässige Datenübermittlung aber aus. Bei allein auf den Privacy Shield gestützten Datenübermittlungen müssen Unternehmen nun schnell zumindest auf die Standarddatenschutzklauseln umstellen. Andernfalls sind sie unzulässig und können von der zuständigen Datenschutzbehörde untersagt und sanktioniert werden.

Rechtsunsicherheit bei Standarddatenschutzklauseln

Standarddatenschutzklauseln sind nach wie vor das wichtigste Instrument, um Datenübermittlungen in Drittländer einschließlich den USA zu legitimieren. Obwohl der EuGH die Standarddatenschutzklauseln explizit als wirksam bestätigt hat, bringt das Urteil für Unternehmen große Rechtsunsicherheit. Grund hierfür ist die nun vom EuGH geforderte einzelfallbezogene Angemessenheitsprüfung. Diese weist die gesamte Verantwortung für den rechtmäßigen Einsatz von Standarddatenschutzklauseln den betreffenden Unternehmen sowie den Datenschutzbehörden zu.

Problematisch dabei ist, dass das Urteil wenig konkrete Maßstäbe für diese Einzelfallprüfung nennt. Dies dürfte nicht nur Unternehmen häufig überfordern, sondern eröffnet auch Raum für übermäßig strikte Interpretationen der Datenschutzbehörden. Einzelne Behörden werden die Aussagen des EuGH zum Anlass nehmen, Datenübermittlungen in die USA pauschal in Frage zu stellen, wie erste aufsichtsbehördliche Positionen zeigen:

- So hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (BfDI Hamburg) in einer Pressemitteilung angekündigt, auf Standarddatenschutzklauseln gestützte Datenübermittlungen kritisch zu überprüfen. Zudem deutet er an, die für die Ungültigkeit des *Privacy Shield* herangezogene Begründung, die US-Sicherheitsgesetze seien zu weitreichend, müsste auch für Standarddatenschutzklauseln gelten.

- Auch der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI Rheinland-Pfalz) betont in seinen FAQ zum *Schrems II*-Urteil die Prüfpflichten von Unternehmen, wenn sie Standarddatenschutzklauseln einsetzen. Diese müssten sich dauerhaft mit der Gesetzeslage im Zielland auseinandersetzen, um nicht von den Aufsichtsbehörden für Datenschutzverstöße durch die importierenden Stellen im Drittland belangt zu werden. In den USA betreffe dies z.B. die Anwendung des *Foreign Intelligence Surveillance Act* (FISA) 702 und der US-amerikanischen *Executive Order 12.333* im jeweiligen Einzelfall.

- Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BfDI Berlin) fordert sogar pauschal alle Unternehmen in ihrem Zuständigkeitsbereich auf, in den USA gespeicherte Daten (zurück) nach Europa zu verlagern. Kunden von Cloud-Diensten etwa sollten zu Anbietern in der EU wechseln. Bei Verstößen gegen diese Vorgaben solle den betroffenen Personen ein Schadensersatzanspruch in abschreckender Höhe zustehen, der auch immaterielle Schäden umfasse. Die rechtliche Begründung

dieser Forderungen lässt sich der Entscheidung des EuGH allerdings nicht ohne weiteres entnehmen.

Handlungsempfehlungen

Wegen der aktuell unklaren Rechtslage kann man Unternehmen nicht ernsthaft raten, sämtliche Datenübermittlungen in die USA auf Basis der Standarddatenschutzklauseln sofort zu stoppen. Dies würde viele Geschäftsprozesse oder Dienste unmöglich machen und wäre ebenso unwirtschaftlich wie unverhältnismäßig. Außerdem wird Unternehmen in vielen Fällen eine Alternative zu Standarddatenschutzklauseln schlicht fehlen. Maßgeschneiderte Individualverträge über Datentransfers zwischen den beteiligten Unternehmen bedürfen der behördlichen Genehmigung und stellen daher oft keine kurzfristig umsetzbare Lösung dar. Einwilligungen der betroffenen Personen für den Datentransfer in die USA dürften — abgesehen von den hohen rechtlichen Anforderungen —vielfach schon aus praktischen Gründen scheitern. Die gesetzlichen Ausnahmetatbestände für Drittlandtransfers sind schließlich eng zu interpretieren und bieten deshalb keine in der Geschäftspraxis verlässliche Grundlage.

Um die mit einem weiteren Einsatz der Standarddatenschutzklauseln verbundenen rechtlichen Risiken zu minimieren, können Unternehmen die folgenden Ansätze in Betracht ziehen:

- Zunächst ist Unternehmen zu empfehlen, die vom EuGH verlangte Prüfung des Datenschutzniveaus im Drittland durchzuführen. Hierfür sollte in einem ersten Schritt die Rechtslage im Zielland u.a. mit Blick auf behördliche Zugriffsbefugnisse auf die übermittelten Daten analysiert werden. Dabei sollten es Unternehmen aber nicht bewenden lassen. Als weiterer Schritt empfiehlt es sich, eine gut dokumentierte Risikoanalyse in Bezug auf die übermittelten Daten durchzuführen. Dabei sind möglichst alle risikorelevanten Faktoren zu berücksichtigen. Dazu gehören etwa die Fragen, wie sensitiv die betroffenen Daten sind, in welchem Umfang Daten übermittelt werden (Datenminimierung), wie hoch die Wahrscheinlichkeit eines tatsächlichen Behördenzugriffs bei dem konkreten Empfängerunternehmen ist (z.B. Anzahl von Behördenzugriffen in der Vergangenheit), ob die Daten mit technischen Mitteln wie Verschlüsselung (z.B. Ende-zu-Ende- oder Speicherverschlüsselung) besonders geschützt sind, oder ob der Empfänger besondere vertragliche Pflichten übernimmt (z.B. erhöhte Beobachtungs- und Mitteilungspflichten). Das Ergebnis diese Risikoanalyse sollte — z.B. angelehnt an eine Datenschutz-Folgenabschätzung — umfassend dokumentiert werden.

- Unternehmen sollten zudem sicherstellen, dass sie auch die formellen Aspekte von Standarddatenschutzklauseln sorgfältig umsetzen, beispielsweise durch die genaue Beschreibung von Datenflüssen. Dabei ist wichtig, dass der Inhalt der Standarddatenschutzklauseln übernommen und nicht verändert wird. Ihre Garantiefunktion wird nur dann erfüllt, wenn die Klauseln ohne Einschränkungen vereinbart werden. Zusätzliche Schutzregelungen sind hingegen zulässig.

- Trotz dieser Maßnahmen ist nicht auszuschließen, dass Datenschutzbehörden weiterhin auf Basis der Standarddatenschutzklauseln vorgenommene Datentransfers in die USA als unzulässig werten. Daher sollten Unternehmen sich bereits jetzt darauf vorbereiten, ihr Vorgehen zur Not vor Gericht zu verteidigen. Der EuGH hat mit dem *Schrems II*-Urteil die Möglichkeit gehabt, Datenübermittlungen in die USA auf Basis von Standarddatenschutzklauseln für unzulässig zu erklären. Dass er dies nicht explizit getan hat, kann ein wichtiges Argument für die Verteidigung vor Gericht sein. Denn der gerichtlichen Wertung kommt besonderes Gewicht zu, weil eine eindeutige Aussage des EuGH angesichts der klar formulierten Vorlagefragen nahe gelegen hätte.

Offene Fragen und Ausblick

Es bleibt abzuwarten wie sich weitere Datenschutzbehörden in Deutschland und der EU zur „Gretchenfrage“ des rechtskonformen Einsatzes von Standarddatenschutzklauseln bei Datentransfers in die USA positionieren. Vor allem die entsprechenden Empfehlungen des Europäischen Datenschutzausschusses dürften hier in der Praxis einige Bedeutung haben, Zudem ist fraglich, welche konkreten Konsequenzen Unternehmen im Falle der Nichteinhaltung der im Urteil formulierten Anforderungen zu erwarten haben, beispielsweise ob Betroffenen Schadensersatzansprüche zustehen. In Deutschland könnte eine zeitnahe Stellungnahme der Datenschutzkonferenz — dem gemeinsamen Gremium der Datenschutzbehörden des Bundes und der Länder — gegebenenfalls zu mehr Rechtssicherheit beitragen, falls sich die deutschen Behörden auf einen gangbaren Kurs verständigen sollten.

Offen ist auch die Reaktion der EU-Kommission auf die neue Situation. Es scheint durchaus denkbar, dass ein Nachfolger des Privacy Shield — zumindest als Zwischenlösung - erarbeitet wird. Um ein solches Instrument langfristig belastbar zu gestalten, müsste dies aber zumindest eine wirksame Beschränkung der US-Sicherheitsgesetze und Rechtsschutzmöglichkeiten umfassen. Jedoch ist fraglich, wie realistisch dies derzeit in den USA ist. Schließlich erwägt die EU-Kommission auch eine Modernisierung der Standarddatenschutzklauseln. Auch dies würde jedoch das strukturelle Problem wohl nicht lösen. Die EU-Kommission hat in einer Stellungnahme nach Veröffentlichung des Urteils auf die Wichtigkeit der Datenübertragung auch in Drittländer hingewiesen und eine Lösung in Aussicht gestellt, um weiterhin sichere Datenübertragung in Drittländer zu gewährleisten.

Wir halten Sie gerne auf dem Laufenden, ob und wann es zu einer konstruktiven und rechtssicheren Lösung für Datenübermittlungen in die USA und andere Drittländer kommen wird.

Wenn Sie Fragen zu diesem Client Alert haben, wenden Sie sich bitte an einen der unten aufgeführten Verfasser oder an den Latham Anwalt, mit dem Sie normalerweise Kontakt aufnehmen:

Tim Wybitul
tim.wybitul@lw.com
+49.69.6062.6560
Frankfurt

Valentino Halim
valentino.halim@lw.com
+49.69.6062.6556
Frankfurt

Das könnte Sie auch interessieren

Wie es nach Schrems II weitergehen kann

Aktuelles zu Bußgeldern wegen Datenschutzverstößen

Die wichtigsten Fragen und Antworten zum neuen DSGVO-Bußgeldmodell der Datenschutzkonferenz (DSK)

Datenschutzklagen als Geschäftsmodell kommerzieller Anbieter – Was müssen Unternehmen jetzt beachten