TIGGES
RECHTSANWÄLTE

Juli 2020

JUS Letter
Datenschutz

EuGH: EU/US-Privacy Shield ist unwirksam – Und nun?

Datentransfers in die USA sind ein sensibles Thema, jedenfalls aus der Perspektive europäischer Bürger und Unternehmen, die sich an den Standards der DSGVO orientieren.

Dass das Schutzniveau für die Übermittlung personenbezogener Daten in die Staaten nicht an europäische Maßstäbe heranreicht, mag in der Sache zunächst nicht mehr überraschen. Mit seinem gestrigen Urteil hat der EuGH das offiziell und gewissermaßen schwarz auf weiß nochmals bestätigt. Denn der EuGH hat mit seiner jüngsten Entscheidung nunmehr die Hauptgrundlage des Datentransfers zwischen der EU und den USA, den sog. „Privacy Shield" für unwirksam erklärt (EuGH, Urteil vom 16. Juli 2020, C 311/18 - Schrems II) und damit zugleich das Gros des Datenverkehrs zwischen den USA und der EU. Praktisch und von Unternehmerseite aus betrachtet dürfen damit die meisten US-Dienstleister nicht eingesetzt werden. Auch Anbieter wie Google oder Facebook stehen nun vor einem großen Problem, wenn Sie Daten der EU-Bürger in den USA verarbeiten wollen. Die Entscheidung wurde lange erwartet, nun stellt sich die Frage, wie Unternehmen damit umgehen sollen.

1. Hintergrund des Verfahrens

Das Urteil knüpft an an die Grundsatzentscheidung des EuGH aus dem Jahr 2015, in der der Gerichtshof den „Safe Habor"-Angemessenheitsbeschluss aufhob (EuGH, Urteil vom 6. Oktober 2015, C-362/14 - Schrems I). Als Reaktion auf das „Safe-Habor"-Urteil setzten vielen Unternehmen zur Legalisierung von Datentransfers in die USA auf Standardvertragsklausel sowie das 2016 als angemessen anerkannte EU-US-Privacy Shield-Abkommen. Maximilian Schrems, der schon den Anstoß für das „Safe-Habor"-Urteil gegeben hatte, stellte sodann auch die Rechtsmäßigkeit von Datentransfers aufgrund der Standardvertragsklauseln und des Privacy Shields in Frage, worüber der EuGH nunmehr entschieden hat.

2. Zum Urteil des EuGH

Der EuGH hat entschieden, dass auch das Privacy Shield Abkommen unwirksam ist. Im Hinblick auf die Wirksamkeit der Standardvertragsklausel stellte der Gerichtshof fest, dass diese grundsätzlich wirksam sind, im Einzelfall aber hohe Anforderungen an die Nutzung zu stellen seien. Nachfolgend ein kurzer Überblick über die wesentlichen Kernaussagen der Entscheidung:

- **Allgemeine Voraussetzungen des Datentransfers in Drittländer**

Wie auch im „Safe Harbor"-Urteil betont der EuGH, dass im Falle von internationalen Datentransfers ein **Schutzniveau** gewährleistet sein muss, das dem in Europa garantierten Niveau der Sache nach **gleichwertig** ist. Bei der Beurteilung dieses Schutzniveaus seien sowohl die vertraglichen Regelungen zu berücksichtigen, die zwischen dem Datenexporteur

und dem Empfänger im Drittstaat vereinbart wurden, als auch die Rechtslage im Drittstaat, insbesondere was einen etwaigen Zugriff der dortigen (Sicherheits-)Behörden auf die übermittelten Daten betrifft.

- **Bewertung der Situation in den USA**

Den Voraussetzungen werde der Privacy Shield Beschluss nicht gerecht – ein gleichwertiges, angemessenes Schutzniveau sei nicht sichergestellt. Insbesondere sei nicht gewährleistet, dass die u.a. auf § 702 FISA und Executive Order 12333 gestützten Überwachungsmaßnahmen der US-Behörden auf das zwingend erforderliche Maß beschränkt sind. Zudem bestünden keine hinreichenden Rechtsschutzmöglichkeiten für Betroffene.

- **Bewertung der Standardvertragsklauseln**

Die sog. Standardvertragsklausel bewertet der EuGH dagegen als grundsätzlich wirksam. Die enthaltenen Mechanismen seien dem Grunde nach geeignet, sicherzustellen, dass das in der EU verlangte Schutzniveau eingehalten wird. Der EuGH macht aber deutlich, dass es dem Datenexporteur obliegt, im Einzelfall zu prüfen, ob die Standardvertragsklauseln unter Berücksichtigung des Rechts des Drittlandes einen angemessenen Schutz bieten.

Dazu müssen ggf. zusätzliche Maßnahmen ergriffen werden, um ein angemessenes Schutzniveau sicherzustellen. Welche Maßnahmen dies sein sollen, lässt der EuGH offen. Für den Fall, dass trotz zusätzlicher Maßnahmen kein angemessener Schutz gewährleistet werden kann, müsse der in der EU ansässige Verantwortliche, oder, wenn dieser nicht tätig wird, die zuständige Aufsichtsbehörde den betroffenen Datentransfer aussetzen oder untersagen.

Das Urteil eröffnet Unternehmen daher grundsätzlich weiterhin die Möglichkeit Datentransfers auf die Standardvertragsklauseln zu stützen. Unbeantwortet bleibt jedoch, ob diese auch für den Datentransfer in die USA genutzt werden können.

3. Was bedeutet die Entscheidung in der Praxis?

Ähnlich der Situation nach Einstufung des Safe Habor-Abkommens als unwirksam, hat das Urteil auch dieses Mal zur Folge, dass für Unternehmen ein Rechtsvakuum entsteht. Strenggenommen darf ein Datentransfer in die USA auf Basis des US-Privacy Shield nicht mehr erfolgen. Und nun? Nachfolgend finden Sie erste Handlungsempfehlungen für Unternehmen – es sollte jedoch stets im Einzelfall geprüft werden, welcher Weg für Ihr Unternehmen der richtige ist!

Der sicherste Weg

- Keine US-Dienstleister und/oder keine Dienstleister mit US-Subunternehmen einsetzen

  Der Einsatz von US-Dienstleistern (sowohl unmittelbar als auch mittelbar) sollte vermieden werden. Jedenfalls sollte eine Evaluation angestoßen werden, um im Falle einer Überprüfung durch die Aufsichtsbehörden nachweisen zu können, dass man die Entscheidung des EuGH ernst nimmt und sich um Alternativen bemüht.

- Datentransfers in die USA (zunächst) einstellen

  In Einzelfällen kann es angezeigt sein, den Datentransfer zumindest vorläufig einzustellen, bis eine anderweitige – sichere –Rechtsgrundlage geschaffen wurde. Dies kann z.B. im Falle der Verarbeitung von Arbeitnehmerdaten durch amerikanische Konzerngesellschaften angezeigt sein. Hier sollte geprüft werden, welche Alternativen bestehen.

- Verträge und Datenschutzhinweise anpassen

  Verträge und Datenschutzerklärungen, die eine Bezugnahme auf das US-Privacy Shield enthalten, sollten angepasst werden.

Mögliche alternative Grundlagen für Datentransfers

Für Unternehmen, die sich beim Datentransfer in die USA auf den Privacy Shield verlassen haben, bieten sich folgende alternative Maßnahmen an:

- Standardvertragsklauseln „plus“: Abschluss der Standardvertragsklauseln unter Berücksichtigung zusätzlicher Garantien und Maßnahmen (z.B. Regelungen zum Umgang mit Anfragen von US-Sicherheitsbehörden)
- Binding Coporate Rules (BCR)
- Genehmigte „Ad-Hoc-Klauseln“
- In Einzelfällen ist es möglich sich auf Art. 49 DSGVO zu stützen. Hier dürfte allerdings wenig Handlungsspielraum bestehen und regelmäßige wiederkehrende Datentransfers fallen in der Regel nicht hierunter.

Oder besser doch erst zuwarten?

Alternativ können Sie auch erst einmal abwarten, wie die EU-Kommission und die Datenschutzbehörden reagieren werden. Diese Vorgehensweise birgt indes nennenswerte Risiken. Denn dem Grunde nach ist klar, dass die Voraussetzungen der DSGVO zu erfüllen sind. Untätigkeit könnte zudem als Organisationsversagen ausgelegt werden. Dies gilt umso mehr als mit einer schnellen Lösung seitens der Politik kaum zu rechnen ist. Die Situation entspricht der Lage in 2015, als das Safe-Habor-Abkommen als Vorgänger des Privacy Shields aufgehoben wurde. Seinerzeit dauerte die Phase der Rechtsunsicherheit sechs Monate. Eine derart „schnelle“ Lösung dürfte mit der derzeitigen US-Regierung aber eher nicht zu erwarten sein. Vielmehr ist damit zu rechnen, dass mit wenig Kooperationsbereitschaft zu rechnen ist, wenn es darum geht, EU-Bürgern einen höheren Rechtsschutz mit Blick auf den Umgang mit ihren personenbezogenen Daten zuzugestehen. Zudem ist nicht auszuschließen, dass jedenfalls einzelne Aufsichtsbehörden hier nicht lange mit einer Beanstandung, jedenfalls Nachfrage zum Datentransfer in die USA warten werden. Dies gilt auch für betroffene Personen (Kunden, Arbeitnehmer etc.), da diese über die Medien über derartige Themen stets sehr gut informiert und zum Teil auch „aufgestachelt“ werden.

Praxishinweise:

Um die Folgen zu mindern sollten Sie daher Maßnahmen ergreifen, auch wenn sie nicht perfekt sein sollten. Stimmen Sie mit Ihrem Datenschutzbeauftragten etc. ab, welche Möglichkeiten bestehen, um im Einzelfall kurzfristige Lösungen zu erzielen. In jedem Fall sollte eine sorgfältige Evaluation internationaler Datentransfers erfolgen. Zudem empfiehlt es sich, die Stellungnahmen der Datenschutzbehörden zu beobachten. Insoweit ist zu erwarten, dass

sowohl die nationalen Behörden als auch der Europäische Datenschutzausschuss sich in der Sache positionieren wird.

Einzelne Stellungnahmen wurden bereits veröffentlicht – diese finden Sie hier:

- BfDI: „BfDI zum Schrems II-Urteil des EuGH“
- Hamburg: „Schwere Zeiten für den internationalen Datenaustausch“
- Rheinland-Pfalz: „Paukenschlag: EuGH schreddert den Privacy Shield, Datenübermittlung in Staaten jenseits der EU aber auf Vertragsbasis weiter möglich“
- Thüringen: „Max Schrems lässt auch Privacy-Shield-Abkommen beim EuGH durchfallen –Dr. Hasse: Keine Überraschung, leider.“

***

Die Autorin sowie Ihre gewohnten Ansprechpartner bei TIGGES und TIGGES DCO stehen Ihnen für Fragen gern zur Verfügung!

Yvonne Quad

Rechtsanwältin und betriebliche Datenschutzbeauftragte (GDDcert. EU)

Zertifizierte IT-Sicherheitsbeauftragte (ITSiBe) gemäß ISO 27001 und BSI IT-Grundschutz

+49 211 8687 137

quad@tigges.legal

TIGGES Rechtsanwälte und Steuerberater Partnerschaft mbB

Zollhof 8 | 40221 Düsseldorf