

## Datentransfer in die USA unter dem neuen EU-US Privacy Shield

29. September 2016

### 1. Allgemeine Voraussetzungen für eine Datenübermittlung in Länder außerhalb der EU

Für eine Übermittlung personenbezogener Daten aus der EU in andere Länder muss im Empfängerland ein **angemessenes Datenschutzniveau** vorliegen. Für manche Länder wie z.B. die Schweiz, Israel und Kanada hat die EU anerkannt, dass deren Datenschutzniveau angemessen ist. Sofern personenbezogene Daten von der EU in andere Länder übermittelt werden sollen, lässt sich durch die Verwendung sog. **Standardvertragsklauseln** der EU oder mittels verbindlicher Unternehmensregelungen („**Binding Corporate Rules**“) ein solcher internationaler Datentransfer datenschutzrechtlich absichern. Unter der neuen **EU-Datenschutz-Grundverordnung**, die ab 25. Mai 2018 gilt, besteht zudem die Möglichkeit der Übermittlung personenbezogener Daten an Drittländer bei Vorliegen einer datenschutzrechtlichen Zertifizierung oder der Einhaltung verbindlicher Verhaltensregeln, sofern diese von der EU-Kommission für allgemein gültig erklärt worden sind. Schließlich kann eine Datenübermittlung in ein Drittland mit einer Einwilligung des Betroffenen erfolgen, allerdings sehen die Datenschutzbehörden Einwilligungen als kritisch an, wenn diese wiederholt, massenhaft und routinemäßig erfolgen.

### 2. Datenübermittlung in die USA

Eine Besonderheit gilt für die Datenübermittlung in die USA.

#### a) Ungültigkeit der Safe Harbour-Regelungen

Da der Europäische Gerichtshof (EuGH) am 6. Oktober 2015 die **Safe Harbour-Regelungen** zwischen der EU und den USA für ungültig erklärt hatte, war seitdem eine Datenübermittlung in die USA datenschutzrechtlich äußerst problematisch. Der EuGH führte in seinem Urteil aus, dass amerikanische Behörden auf die aus der EU in die USA übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten können, die über das hinausgeht, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig ist. Eine Regelung, die es Behörden gestattet, generell und ohne irgendeine Differenzierung auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze nach Auffassung des EuGH das Grundrecht auf Achtung des Privatlebens. Zudem stehen den Betroffenen keine ausreichenden Rechtsbehelfe zur Verfügung. **Eine Datenübermittlung in die USA konnte seit dem Urteil des EuGH nicht mehr durch die Anwendung der Safe-Harbour-Regelungen gerechtfertigt werden.**

#### b) Datenübermittlung unter dem „EU-US-Datenschutzschild“ (Privacy Shield)

Die EU und die USA haben daraufhin im Juli 2016 mit dem **„EU-US-Datenschutzschild“ (Privacy Shield)** einen neuen Rahmen für den transatlantischen Austausch von personenbezogenen Daten geschaffen. Sofern eine Rechtsgrundlage für die Übermittlung nach dem Bundesdatenschutzgesetz oder künftig der EU-Datenschutz-Grundverordnung vorliegt und US-Unternehmen die im Privacy Shield geregelten Datenschutzgrundsätze einhalten, dürfen an sie personenbezogene Daten aus der EU übermittelt werden.

Unter dem Privacy Shield können sich US-Unternehmen seit dem 1. August 2016 für die **Aufnahme in die Datenschutzschild-Liste** registrieren lassen und jährlich mittels einer **Selbstzertifizierung** bestätigen, dass sie die festgelegten Anforderungen erfüllen. Dies wird vom US-Handelsministerium überwacht und bei Verstößen können betroffene Unternehmen von der Liste gestrichen werden. Die aktuelle Datenschutzschild-Liste kann unter <https://www.privacyshield.gov/list> eingesehen werden.

Die USA haben der EU zugesichert, dass der Datenzugriff von Behörden aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit in den USA künftig klaren Beschränkungen, Garantien und Aufsichtsmechanismen unterliegt. Hierdurch soll ein anlassloser Massenzugriff auf Daten von EU-Bürgern ausgeschlossen werden.

EU-Bürger stehen mehrere Beschwerde- und Rechtsschutzmöglichkeiten zu. Im US-Außenministerium wird eine Ombudsstelle für Rechtsschutzbegehren im Bereich der nationalen Sicherheit eingerichtet. Im Falle einer mutmaßlichen Datenschutzverletzung können sich EU-Bürger an das entsprechende US-Unternehmen wie auch an die eigene **nationale Datenschutzbehörde wenden und sich beschweren. Weiter Beschwerdemöglichkeiten** sind eine **unabhängige Streitbeilegungsstelle** und als letztes Mittel ein **Schiedsverfahren**, dessen Entscheidung für das US-Unternehmen verbindlich ist. Zudem können EU-Bürger bei Datenschutzverstößen in den USA in bestimmten Fällen US-Gerichte anrufen.

In einem **Leitfaden** (abzurufen unter [http://ec.europa.eu/justice/data-protection/document/citizens-guide\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf)) hat die EU-Kommission das Privacy Shield und die Rechte der Betroffenen anschaulich dargestellt.

### c) Kritik am Privacy Shield

Es bleibt abzuwarten, ob das Privacy Shield tatsächlich zu einem angemessenen Datenschutzniveau bei den US-Unternehmen führt, die sich hierunter registrieren lassen. Die Funktionsweise und die Zusicherungen und Zusagen der USA werden durch die Europäische Kommission und das US-Handelsministerium gemeinsam jährlich überprüft.

So scheint fraglich, ob EU-Bürgern nun in den USA der vom EuGH geforderte **wirksame gerichtliche Rechtsschutz** gegen Eingriffe in ihre Grundrechte zusteht und ob eine **wirksame Überwachung der US-Unternehmen**, die unter das Privacy Shield fallen, erfolgt. Auch der Umfang des Zugriffs der US-Nachrichtendienste auf Daten von EU-Bürgern, der jährlich unter Hinzuziehung der Europäischen Datenschutzbehörden überprüft werden soll, wird zu beobachten sein.

### 3. Zusammenfassung

Übermittelt ein in der EU ansässiges Unternehmen personenbezogene Daten an ein Unternehmen in den USA, muss dies datenschutzrechtlich zulässig sein. Zunächst muss eine Rechtsgrundlage für die Übermittlung nach dem Bundesdatenschutzgesetz oder künftig der EU-Datenschutz-Grundverordnung vorliegen. Falls dies der Fall ist, dürfen an US-Unternehmen, die in der Datenschuttschild-Liste registriert sind, personenbezogene Daten aus der EU übermittelt werden. Hierfür muss das übermittelnde Unternehmen durch Einblick in die Datenschuttschild-Liste klären, ob die Zertifizierung unter dem Privacy Shield vorliegt und gültig ist und ob die zu übermittelnden Daten von der Zertifizierung umfasst sind. Allerdings ist das Privacy Shield-Regelungswerk sehr komplex und es bleibt abzuwarten, ob deutsche Datenschutzaufsichtsbehörden zusätzliche Prüfpflichten auferlegen und ob das Privacy Shield der jährlichen Evaluierung und einer gerichtlichen Überprüfung standhält. **Solange jedoch das Privacy Shield nicht vom EuGH für ungültig erklärt oder anderweitig ausgesetzt worden ist, kann ein Datentransfer an US-Unternehmen, die in der Datenschuttschild-Liste gelistet sind, hierauf gestützt werden.**

**Der Autor ist Rechtsanwalt der Kanzlei „TCI Rechtsanwälte“ mit Branchenfokus in den Bereichen Technology, Communications, Information, auf denen die Kurzbezeichnung „TCI“ beruht.**

**TCI Rechtsanwälte München (Tel. 089 / 38367880):**

Dr. Thomas Stögmüller, LL.M. (Berkeley), Fachanwalt für Informationstechnologierecht;  
[tstoegmueller@tcilaw.de](mailto:tstoegmueller@tcilaw.de)

Weitere Informationen: [www.tcilaw.de](http://www.tcilaw.de).

Dieses Merkblatt wurde im Rahmen der Kooperation IT-Sicherheit für Familienunternehmen der IHK Schwaben mit dem Branchennetzwerk aitiRaum e.V. erstellt.

Ansprechpartner:

Dr. Matthias Köppel  
Stettenstraße 1 + 3 | 86150 Augsburg  
Tel 0821 3162-205 | Fax 0821 3162-342  
[Matthias.Koeppel@schwaben.ihk.de](mailto:Matthias.Koeppel@schwaben.ihk.de)