# Kundeneninformation

**EU-US-Datenschutzschild: Der Safe Harbor Nachfolger für Datentransfers in die USA ist da.**

Sehr geehrte Damen und Herren,

am **12. Juli 2016** hat die Europäische Kommission das **EU-U.S. Privacy Shield** angenommen. Hierbei handelt es sich um die Nachfolgeregelung der im Oktober 2015 durch den europäischen Gerichtshof für ungültig erklärten Safe Harbor-Entscheidung.

Beim Privacy Shield handelt es sich, rechtlich betrachtet, um eine **Angemessenheitsentscheidung** der Europäischen Kommission basierend auf Art. 25 Abs. 6 der Datenschutzrichtlinie (RL 95/46/EG). Der Anwendungsbereich des Privacy Shield beschränkt sich **auf US-amerikanische Unternehmen**, die sich selbst dazu verpflichten, bestimmte Vorgaben beim Umgang mit personenbezogenen Daten zu beachten. Zweck dieser Angemessenheitsentscheidung ist es, die Übertragung personenbezogener Daten an Unternehmen in den USA datenschutzrechtlich zulässig zu ermöglichen.

Die komplette Angemessenheitsentscheidung der Europäischen Kommission finden Sie hier (PDF).[1]

Im Folgenden möchten wir Ihnen einen kurzen Überblick über die zentralen Aspekte des Privacy Shield geben.

**Inhaltsübersicht**



[1] Die Entscheidung liegt bisher nur in englischer Sprache vor; daher werden wir nachfolgend zur Erläuterung auch die englischen Fachbegriffe verwenden.

## 1. Anwendungsbereich

Das Privacy Shield gilt allein für Übermittlung personenbezogener Daten aus dem europäischen Wirtschaftsraum an Unternehmen mit Sitz in den **USA**. Es kann also nicht für Datentransfers in andere Drittstaaten, wie etwa Japan, Russland oder China genutzt werden.

Das Privacy Shield und insbesondere die zugehörigen Anlagen verpflichten dem Grunde nach amerikanische Unternehmen, bestimmte Vorgaben bei der Verarbeitung personenbezogener Daten aus dem europäischen Wirtschaftsraum einzuhalten. Überwacht wird diese Einhaltung auf amerikanischer Seite durch das **Handelsministerium**. Dieses wird auch eine öffentlich abrufbare Liste mit Unternehmen führen, die sich zur Einhaltung der Vorgaben des Datenschutzschildes verpflichtet haben.

Wie auch in der Vergangenheit bei Safe Harbor wird das System des Privacy Shield auf der **Selbstzertifizierung** amerikanischer Unternehmen beruhen. Die Teilnahme an dem Programm ist freiwillig.

## 2. Bestandteile des Datenschutzschild

Das Privacy Shield besteht indes nicht nur aus der Angemessenheitsentscheidung der Europäischen Kommission selbst, sondern vor allem auch aus den **Privacy Principles** (Annex 2) und einer Reihe von erläuternden Dokumenten bzw. Zusicherungen verschiedener amerikanischer Behörden.

Aus Sicht amerikanischer Unternehmen sind insbesondere die Privacy Principles (Annex 2) relevant. An diese müssen sich die Unternehmen halten, wenn sie in den Genuss der **privilegierenden Wirkung** der Angemessenheitsentscheidung der Europäischen Kommission kommen möchten.

## 3. Pflichten für US-Unternehmen

Die für US-Unternehmen einzuhaltenden Pflichten ergeben sich insbesondere aus dem Privacy Principles, deren Inhalt wir nachfolgend kurz skizzieren.

Nach dem **Notice Principle** sind teilnehmende amerikanische Unternehmen dazu verpflichtet, betroffenen Personen bestimmte Informationen hinsichtlich der Verarbeitung der sie betreffenden personenbezogener Daten zur Verfügung zu stellen. Auf ihren Webseiten müssen die amerikanischen Unternehmen einen deutlich sichtbaren Link zu einer **Datenschutzerklärung** bereithalten ebenso wie einen Link zur Webseite des amerikanischen Handelsministeriums, auf der sich weitere Informationen zum Privacy Shield finden.

Nach den Vorgaben des **Data Integrity and Purpose Limitation Principle** dürfen personenbezogene Daten nur in dem **Umfang** verarbeitet werden, wie es für den jeweilig verfolgten Zweck erforderlich ist. Zudem müssen die personenbezogenen Daten **richtig, vollständig und aktuell** sein. Amerikanische Unternehmen dürfen personenbezogene Daten nicht für einen Zweck verarbeiten, der mit dem ursprünglichen Zweck unvereinbar ist.

Das heißt aber auch: personenbezogene Daten dürfen durchaus für einen anderen Zweck als den ursprünglich bestimmten verarbeitet werden, solange dieser andere Zweck mit dem ursprünglichen vereinbar ist und wenn die Unternehmen betroffenen Personen die Möglichkeit des Widerspruchs einräumen (Opt-out) (**Choice Principle**). Diese Widerspruchsmöglichkeit wird auch für eine Verarbeitung personenbezogener Daten für Zwecke der **Direktwerbung** verlangt.

Nach dem **Security Principle** sind US-amerikanische Unternehmen, die personenbezogene Daten verarbeiten, dazu verpflichtet, angemessene und geeignete **Sicherheitsmaßnahmen** einzusetzen. Im Fall einer **Unterbeauftragung** müssen amerikanische Unternehmen mit dem Unterauftragnehmer einen Vertrag schließen, der hinsichtlich der Privacy Principles ein **gleichwertiges Schutzniveau** für die betroffenen personenbezogenen Daten garantiert.

Nach dem **Access Principle** haben betroffene Personen das Recht, von dem amerikanischen Unternehmen **Auskunft** zu gespeicherten personenbezogenen Daten der jeweiligen Person zu erhalten. Betroffene Personen müssen zudem die Möglichkeit haben, personenbezogene Daten **korrigieren** und **löschen** (lassen) zu können, wo diese Daten unrichtig oder entgegen den Vorgaben der Privacy Principles verarbeitet wurden.

Zudem gilt nach dem **Recourse, Enforcement und Liability Principle**, dass betroffenen Personen mehrere Möglichkeiten der Streitbeilegung offen stehen müssen, von denen sie leicht und ohne große Kosten Gebrauch machen können müssen. Eine **Beschwerde** kann sich stets gegen das amerikanische Unternehmen selbst richten. Außerdem steht ein kostenloses Verfahren der **alternativen Streitbeilegung** zur Verfügung. Zudem können sich betroffene Personen auch an die **nationalen Datenschutzbehörden** in der Europäischen Union wenden, die dann zusammen mit der amerikanischen Federal Trade Commission (FTC) dafür sorgen, dass Beschwerden nachgegangen wird. Amerikanischen Unternehmen, die grundsätzlich der Aufsicht von US-Behörden (wie der FTC) unterliegen, ist es zudem freigestellt, ob sie sich dazu verpflichten, mit den jeweils zuständigen nationalen Datenschutzbehörden in Europa zusammenarbeiten und deren Anweisungen zu folgen. Eine solche Wahlmöglichkeit besteht jedoch nicht, wo personenbezogene Daten von **Beschäftigten** übermittelt werden. In diesem Fall sind die betreffenden Unternehmen nach den Privacy Principles verpflichtet, direkt mit der jeweiligen europäischen Aufsichtsbehörde zusammenzuarbeiten und etwa deren Anweisungen zu befolgen.

Amerikanische Unternehmen müssen sich zudem **jährlich** beim Handelsministerium **re-zertifizieren**.

Besondere Vorgaben gelten auch unter dem **Accountability for Onward Transfer Principle** für die Weitergabe personenbezogener Daten in den USA oder an Stellen in einem anderen Drittstaat. Eine solche Übermittlung darf nur erfolgen, wenn hierfür ein **spezifischer** und begrenzter **Zweck** festgelegt ist, wenn ein entsprechender Vertrag für die Weitergabe vorliegt und nur

wenn dieser **Vertrag** dasselbe Schutzniveau garantiert, welches die Privacy Principles vorsehen.

## 4. Kein Einfluss auf andere Instrumente für Datentransfers

Das Privacy Shield hat keinen Einfluss auf die Wirksamkeit und den Einsatz alternativer Instrumente für Datentransfers in Drittstaaten. Insbesondere können Unternehmen also weiterhin etwa die sogenannten **EU-Standardvertragsklauseln** für Datenübermittlungen in die USA nutzen.

Wir möchten Sie jedoch darauf hinweisen, dass die Frage der Gültigkeit der EU-Standardvertragsklauseln wahrscheinlich in näherer Zukunft durch den **europäischen Gerichtshof** geprüft wird. Ein hierfür erforderlicher Vorlagebeschluss eines irischen Gerichts wird allgemein erwartet.

## 5. Verantwortlichkeit der europäischen Unternehmen

Datenschutzrechtlich bleibt stets das europäische Unternehmen verantwortlich, welches, bildlich gesprochen, als „Exporteur" der personenbezogenen Daten fungiert, und damit auch potentieller Adressat **aufsichtsbehördlicher Maßnahmen**.

Insbesondere liegt es im Verantwortungsbereich des europäischen Unternehmens, die Übermittlung personenbezogener Daten an das US-amerikanische Unternehmen auf einen passenden **gesetzlichen Erlaubnistatbestand** (zum Beispiel eine Einwilligung der betroffenen Person oder auf der Grundlage eines Vertrages mit dieser) zu stützen. Das Privacy Shield sorgt nur für die Zulässigkeit der Weitergabe personenbezogener Daten in einen, aus dem Blickfeld des europäischen Datenschutzrechts, unsicheren Drittstaat. Die Datenverarbeitung an sich (meist eine Übermittlung) bedarf aber dennoch eines gesetzlichen Erlaubnistatbestandes.

## 6. Was ist zu tun?

Europäische Unternehmen, die personenbezogene Daten in die USA übermitteln möchten, können sich in Zukunft auf die Angemessenheitsentscheidung der europäischen Kommission zum Privacy Shield berufen. Es wird jedoch noch ein wenig dauern, bis amerikanische Unternehmen ihre interne Datenschutzorganisation entsprechend den Vorgaben des Privacy Shield angepasst haben. Das US Handelsministerium hat bekannt gegeben, dass die öffentlich zugängliche Liste mit teilnehmenden amerikanischen Unternehmen ab dem 1. August 2016 verfügbar sein wird.

Auch wenn die europäischen Datenschutzbehörden grundsätzlich an die Entscheidung der Europäischen Kommission gebunden sind, ist, blickt man auf die vergangenen Jahre unter **Safe Harbor**, nicht auszuschließen, dass von europäischen Unternehmen **zusätzliche Garantien** verlangt werden, um Datenübermittlung in die USA (zumindest nach Auffassung der Behörden) rechtskonform auszugestalten. Insbesondere ist damit zu rechnen, dass die **deutschen Aufsichtsbehörden** wie auch schon unter Safe Harbor den **Abschluss eines Vertrages** mit dem jeweiligen amerikanischen Unterneh-

men in Betracht, der sich inhaltlich im Wesentlichen an den Vorgaben zur Auftragsdatenverarbeitung orientiert. Daneben sind europäische Unternehmen grundsätzlich verpflichtet, den **Zertifizierungsstatus** des amerikanischen Unternehmens anhand eines Abgleichs mit der öffentlich abrufbaren Liste zum Datenschutzschild zu **prüfen**.

Wenn Sie Fragen zu diesem Thema haben oder Unterstützung bei der Umsetzung der notwendigen Änderungen benötigen, wenden Sie sich gerne an uns: info@jbbdataconsult.de

Ihre Berater
der JBB Data Consult GmbH

JBB Data Consult GmbH
Christinenstraße 18/19
10119 Berlin

Tel. + 49 30 443 765 124
Fax + 49 30 443 765 125

Mail info@jbbdataconsult.de
Web www.jbbdataconsult.de