

## Privacy Shield gekippt – Datenübermittlung in die USA kritisch

Der Europäische Gerichtshof (EuGH) hat letzte Woche das US-Privacy Shield als zweite transatlantische Vereinbarung zum Datenschutz für ungültig erklärt. Damit verbunden sind zahlreiche Probleme und Unsicherheiten. Mit diesem Newsletter möchten wir Ihnen ein paar Hinweise und Handlungsmöglichkeiten an die Hand geben.

### I. ENTSCHEIDUNG DES EUGH ZUM PRIVACY SHIELD

Den Stein ins Rollen brachte der österreichische Datenschutzaktivist Max Schrems, dessen Klage bereits zum Ende des Safe-Harbour-Abkommens geführt hatte.

Schrems hatte bei der irischen Datenschutzbehörde beanstandet, dass Facebook Irland seine Daten an den Mutterkonzern in die USA weiterleite. Aufgrund der Enthüllungen Snowdens war u.a. bereits bekannt, dass die NSA bspw. Daten von Facebook-Nutzern abgreift. Hinzukommend sind US-Unternehmen u.a. aufgrund des American Patriot Acts dazu verpflichtet, US-Behörden die Daten zugänglich zu machen.

Das Privacy Shield wurde als Abkommen zwischen der EU-Kommission und den USA geschlossen; US-Unternehmen konnten diesem durch eine Selbstzertifizierung beitreten, was auch zahlreiche Unternehmen in Anspruch nahmen.

Ein irisches Gericht wollte in Folge der Beschwerde nun wissen, ob das Privacy Shield und die Standardvertragsklauseln mit dem europäischen Datenschutzrecht vereinbar sind.

Der EUGH hat geurteilt, dass die Überwachungsgesetze der USA zu weitreichend seien, als dass der Privacy Shield EU-Bürger angemessen vor ihnen schütze. Folglich können ein angemessenes Schutzniveau nicht sichergestellt werden, weshalb das Privacy Shield ungültig sei.

Die Standardvertragsklauseln seien zulässig – aber nur, wenn der Datenschutz in dem anderen Land gewährleistet sei, was gerade bei den Tech-Konzernen Apple, Facebook, Google, Microsoft und Yahoo fraglich sei.

Die USA müssen nun dringend ihre Überwachungsgesetze ändern, wenn US-Konzerne weiterhin in Europa tätig sein wollen.

### II. DER BREXIT UND DER DATENSCHUTZ

Nach dem Brexit ist Großbritannien nun ein Drittland. Die europäische Kommission hat hierzu noch keinen Angemessenheitsbeschluss erlassen. Damit unterliegen Datenübermittlungen nach Großbritannien den üblichen Bestimmungen der Art. 44 ff. DSGVO (vgl. unten).

Sofern Sie also Dienstleister oder Auftragsverarbeiter einsetzen, die Daten nach Großbritannien einsetzen, gilt das zu I. und den USA Gesagte. Dies gilt insbesondere für OpenStreetMaps.

Bei OpenStreetMap empfehlen wir derzeit, dies entweder nicht zu verwenden oder die Karten herunterzuladen und so einzubinden, dass der Nutzer keine Verbindung zu dem Anbieter OSMF herstellen muss. Hier müssen Sie aber ggf. Nutzungsrechte erwerben.

### III. **HANDLUNGSEMPFEHLUNGEN FÜR DIE ÜBERMITTLUNG IN DRITTLÄNDER UND SPEZIELL IN DIE USA**

#### **1. Grundsätzliches**

Sie müssen für die Übermittlung der Daten in Drittländer außerhalb der EU die Voraussetzungen des Art. 44 DSGVO einhalten, d.h.

*„Jedwede Übermittlung personenbezogener Daten (...) ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden“*

Eine Übermittlung ist damit unter folgenden Voraussetzungen möglich:

#### a) Angemessenheitsbeschlüsse, Art. 45 DSGVO

Solche liegen derzeit nur für die Länder Andorra, Argentinien, Färöer Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Kanada, Neuseeland, Schweiz, Uruguay vor (vgl. [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_de](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de)).

#### b) Datenübermittlung vorbehaltlich geeigneter Garantien, Art. 46 DSGVO

Diese Garantien müssen durch den Verantwortlichen oder den Auftragsverarbeiter vorgesehen werden und diese müssen geeignete sein, den Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung zu stellen. Derzeit vorhandene Garantien sind lediglich Standardvertragsklauseln der EU-Kommission (engl.: Standard Contractual Clauses), Art. 48 DSGVO. Diese sind weiterhin zulässig. Sichern Anbieter diese zu und halten diese auch ein, kann eine Übermittlung auf dieser Basis erfolgen.

Alternativ sind sog. Binding Corporate Rules möglich, welche sich die Unternehmen selbst geben. Aber auch hier müssen Genehmigungen durch die zuständige Aufsichtsbehörde erfolgen. Ein solcher Prozess ist regelmäßig sehr aufwändig.

### c) Ausnahmen für bestimmte Fälle gem. Art. 49 DSGVO

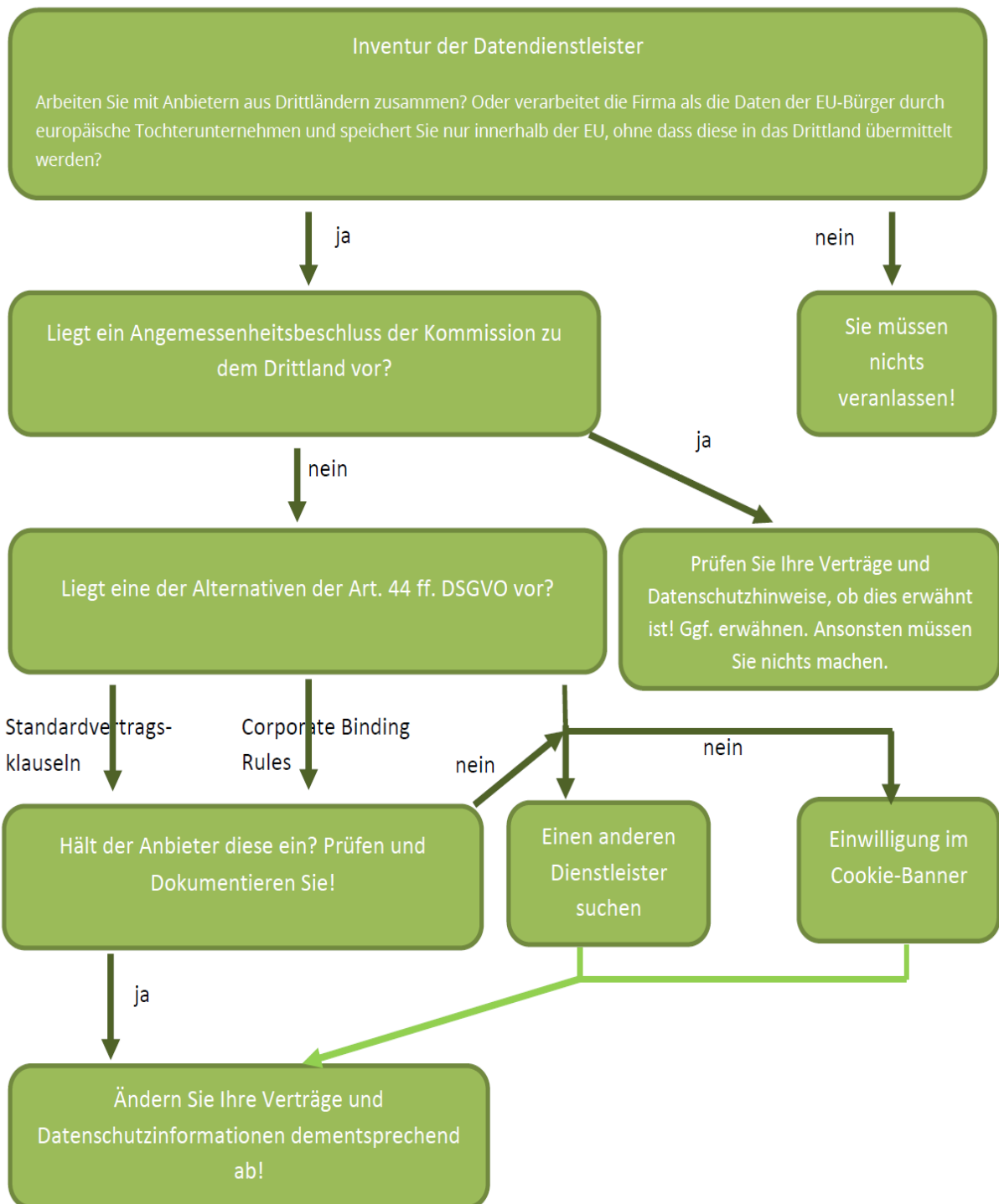
Hiernach ist eine Übermittlung an ein Drittland zulässig, sofern

- Der Betroffene in die Datenübermittlung ausdrücklich einwilligt, nachdem er über die bestehenden Risiken derartiger Übermittlungen (d.h. kein angemessenes Datenschutzniveau und Risiko der Durchsetzung von Betroffenenrechten) und über deren Widerrufsmöglichkeit unterrichtet wurde
- Die Übermittlung für den Abschluss oder die Erfüllung eines Vertrages zwischen dem Betroffenen und dem Verantwortlichen erforderlich ist
- Zur Verfolgung von Rechtsansprüchen
- Keine der vorgenannten Möglichkeiten besteht und die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, zur Wahrung zwingender berechtigter Interessen des Verantwortlichen erforderlich ist und keine Interessen oder Rechte des Betroffenen überwiegen und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. In diesem Fall muss der Verantwortliche die Aufsichtsbehörden von der Übermittlung in Kenntnis setzen und den Betroffenen über die Übermittlung und seine Interessen unterrichten. Hierüber ist eine Dokumentation gem. Art. 30 anzufertigen.

## 2. Folgen

Befolgen Sie diese Voraussetzungen nicht, sind die Übermittlungen nichtig und können zu hohen Bußgeldern durch die Datenschutzbehörden und/oder zu Abmahnungen führen.

## 3. Checkliste



## a) Inventur

Machen Sie eine Inventur über die Datendienstleister/Auftragsverarbeiter? Arbeiten Sie mit Anbietern aus Drittländern zusammen? Oder verarbeitet die Firma als die Daten der EU-Bürger durch europäische Tochterunternehmen und speichert Sie nur innerhalb der EU, ohne dass diese in das Drittland übermittelt werden? (Erkundigen Sie sich bei den Dienstleistern; Dokumentieren Sie!)

➔ Aber auch hier ist Vorsicht walten zu lassen. Nach dem US-Cloud Act von 2019 ist US-Behörden der Zugriff auch auf im Ausland gespeicherte Daten erlaubt, sofern die betroffenen Server unter der Kontrolle von US-Unternehmen oder deren Tochtergesellschaften stehen.

b) Angemessenheitsbeschluss

Prüfen Sie zunächst, ob die Kommission zu dem Drittland bereits einen Angemessenheitsbeschluss erlassen hat.

c) Alternativen des Art. 44 ff.

Prüfen Sie, ob die anderen Alternativen der Art. 44 ff. DSGVO vorliegen, insbes. ob der Dienstleister die Standardvertragsklauseln zusichert.

➔ MailChimp bietet bspw. die Standardvertragsklauseln an

➔ Wichtig: Der EUGH hat auch entschieden, dass die Datenübertragung von Facebook und anderen Unternehmen, die unter das strenge US-Überwachungsgesetz FISA fallen, nicht über die Standardvertragsklauseln möglich ist.

d) Einhaltung der Klauseln

Hält der Dienstleister die Vereinbarungen ein? (hier sind Sie in der Prüfpflicht; Erkundigen Sie sich bei den Dienstleistern; Dokumentieren Sie, was Sie prüfen, wann, wen, wie etc.!) )

➔ Einen Fragebogen, den Sie an die Dienstleister schicken können, finden Sie hier ([https://noyb.eu/files/CJEU/EU-US\\_form\\_v3.docx](https://noyb.eu/files/CJEU/EU-US_form_v3.docx)).

➔ Achtung: Meist wird das Ergebnis eher negativ ausfallen.

e) Cookie-Banner

Notlösung: Einwilligung im Cookie-Banner möglich, ist aber mit viel Information verbunden! Zudem wird die Wirksamkeit bezweifelt!

Wie könnte so eine Zusatzinformation (also zusätzlich zu den bisherigen Cookie-Informationen) aussehen?

Beispiel (bitte passen Sie dies an):

*„Hinweis zur Verarbeitung der auf dieser Webseite erhobenen Daten durch .... in den USA:*

*Mit Anklicken des Buttons „...“ stimmen Sie gem. Art. 49 Abs. 1 S. 1 lit. a) DSGVO zu, dass Ihre Daten in die USA übermittelt werden. Der Europäische Gerichtshof*

*betrachtet die USA als Land mit unzureichendem Datenschutzniveau. Es besteht daher das Risiko, dass Ihre Daten durch US-Behörden zu Kontroll- und Überwachungszwecken verarbeitet werden, ohne dass Sie Ihre Betroffenenrechte oder sonstige Rechtsbehelfsmöglichkeiten haben. Sie können Ihre Einwilligung jederzeit widerrufen, indem Sie in Ihren Einstellungen Ihre gesetzten Cookies löschen. Wenn Sie nur die essenziellen Cookies akzeptieren, findet eine Übermittlung nicht statt.“*

***Hinweis: Das Beispiel stellt lediglich eine Formulierungshilfe nach Ansicht der Autorin (kein Muster!) dar, wobei das Beispiel natürlich derzeit von Rechtsprechung und Datenschutzbehörden ungeprüft ist und daher keinen Anspruch auf Wirksamkeit erhebt.***

Können die Datenschutzbestimmungen nicht gewährleistet werden, müssen Sie die Verträge mit den Dienstleistern im äußersten Fall kündigen!

## **5. Speziell zum Privacy Shield**

Betroffen sind v.a. die Anbieter und deren Dienste (die Liste ist nicht abschließend, sondern spiegelt nur die häufigsten Anwendungen wider)

- Zoom
- Skype
- Google und alle damit verbundenen Unternehmen sowie deren Dienste (Google Ads, Google Analytics, Doubleclick, Google Maps, Recaptcha, WebFonts usw.)
- Facebook und alle damit verbundenen Unternehmen (Instagram, WhatsApp) und Dienste (Facebook Connect)
- Weitere Social Media Anbieter (Twitter, LinkedIn und Co.) und deren Plugins
- Microsoft
- PayPal
- Cloudflare
- Wordpress Stats
- MailChimp
- YouTube, Vimeo
- SoundCloud
- Stripe
- Klarna
- GoToMeeting
- Microsoft Teams
- GoogleMeet

Facebook und Microsoft haben bereits eine Stellungnahme abgegeben, dass sich erst einmal nichts verändern werden; dennoch werde man die Auswirkungen genauer prüfen.

Löschen Sie in Ihren Datenschutzerklärungen und Verträgen alle Hinweise auf das Privacy Shield!

Bei Fragen oder sofern Sie Hilfe benötigen, können Sie gerne jederzeit auf uns zukommen.

*Hinweis: Es handelt sich um eine Rechtsansicht der Autorin. Das Datenschutzrecht ist jedoch ein ungeformtes Rechtsgebiet, das erst noch zahlreicher Entscheidungen und Praxis bedarf, um sicher gehen zu können. Wir bitten, dies bei der Lektüre zu beachten.*

© Dr. Carmen Fritz, LL.M.

Fachanwältin für Urheber- und Medienrecht

Fachanwältin für Gewerblichen Rechtsschutz

Datenschutzbeauftragte (TÜV)

[www.fritz-gern.de](http://www.fritz-gern.de)