

Datenübermittlung in die USA

EU-US Privacy Shield



Forum Datenschutz
13.10.2016
TechBase Regensburg

BSP-SECURITY

Michael Gruber

Senior Consultant
Datenschutz und Informationssicherheit

ISIS12 Netzwerkpartner
Fachbeirat Bayerischer IT-Security Cluster e.V.

Tel:	+49 (0)941 60 48 89-8 64	BSP-SECURITY
Fax:	+49 (0)941 60 48 89-8 66	Franz-Mayer-Str. 1
Mobil:	+49 (0)152 32 01 04 95	D-93053 Regensburg

E-Mail: michael.gruber@bsp-security.de
www.bsp-security.de

Agenda

- 1 Datenübermittlung in Drittstaaten
- 2 Safe Harbor war gestern
- 3 EU-US Privacy Shield ist heute
- 4 DS-GVO – was kommt morgen?

1 Datenübermittlung in Drittstaaten

„ Der Datentransfer ins Ausland gehört zu den schwierigsten Materien des Datenschutzrechts“ (Niko Härting)

1. Ursache

- Rechtslage ist sehr komplex
- viele Varianten in der Praxis
- Aufsichtsbehörden sind z. T. verschiedener Auffassung

2. Ursache

- US Unternehmen haben Probleme mit D bzw. EU Datenschutzrecht

1 Datenübermittlung in Drittstaaten

- Datenübermittlung ins Ausland verlangt prinzipiell eine zweistufige datenschutzrechtliche Prüfung durch die verantwortliche Stelle:
 - 1 Rechtsgrundlage prüfen (§ 4 Abs. 1 BDSG) + (Auftrags(daten)verarbeitung)
 - 2 Sicherheitsprüfung des Export-Landes (angemessenes Schutzniveau)

1 Datenübermittlung in Drittstaaten

EWR = EFTA + EU



EWR = keine Drittstaaten

Der EWR besteht aus den
■ EFTA-Mitgliedstaaten (ohne die Schweiz)

🇮🇸 Island 🇱🇮 Liechtenstein 🇳🇴 Norwegen

■ EU-Mitgliedstaaten

🇧🇪 Belgien	🇮🇹 Italien	🇷🇺 Rumänien
🇧🇬 Bulgarien	🇰🇷 Kroatien ¹	🇸🇪 Schweden
🇩🇰 Dänemark	🇱🇹 Lettland	🇸🇰 Slowakei
🇩🇪 Deutschland	🇱🇮 Litauen	🇸🇮 Slowenien
🇪🇪 Estland	🇱🇺 Luxemburg	🇪🇸 Spanien
🇫🇮 Finnland	🇲🇹 Malta	🇨🇪 Tschechien
🇫🇷 Frankreich	🇳🇱 Niederlande	🇭🇺 Ungarn
🇬🇷 Griechenland	🇦🇹 Österreich	🇬🇧 Vereinigtes Königreich
🇮🇪 Irland	🇵🇱 Polen	🇨🇾 Zypern
	🇵🇹 Portugal	

¹ provisorisch seit 12. April 2014^[1]

(Quelle: www.wikipedia.de)

1 Datenübermittlung in Drittstaaten

- Bei Datenübermittlung innerhalb des EWR wird ein angemessenes Datenniveau angenommen.
- Dies trifft auch auf die folgenden Länder zu: Schweiz, Kanada, Israel, Argentinien, Andorra, Färöer, Guernsey, Isle of Man, Jersey, Australien, Neuseeland und Uruguay.
- Dies bedeutet es wird ein angemessenes Schutzniveau angenommen.
- Dies ist der einfachste Fall.

1 Datenübermittlung in Drittstaaten

Bei Datenübermittlung in Drittstaaten:

- Genehmigung der Datenübermittlung durch die zuständige Aufsichtsbehörde.
- Binding Corporate Rules (BCR): Datenübermittlung innerhalb eines Konzerns (Genehmigung durch EU-Aufsichtsbehörden)
- Einwilligung der Betroffenen nach Aufklärung der Risiken
- Verwendung der EU Standardvertragsklauseln (keine Änderungen möglich)
- Im Falle USA: ~~Safe Harbor~~ EU-US Privacy Shield
- ...

2 Safe Harbor war gestern

- Sonderfall USA: Edward Snowden
- bis zum 05.10.2015
Safe Harbour (Angemessenheitsentscheidung der EU-Kommission)
- ab dem 06.10.2015
EuGH erklärt die Angemessenheitsentscheidung der EU-Kommission zu Safe Harbor als ungültig (Az. C-362/14; Max Schrems)
- ab dem 07.10.2015
Ratlosigkeit bei Verantwortlichen, Betroffenen, Aufsichtsbehörden, EU-Kommission, Datenschutzbeauftragten, Juristen ...
- Wie können personenbezogene Daten legal in die USA übermittelt werden?

3 EU-US Privacy Shield ist heute



The screenshot shows the website of the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI). The header features the HmbBfDI logo and the text 'Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit'. Below the header is a navigation menu with five items: 'Wir über uns Kontakt', 'Ihr Recht auf Datenschutz', 'Datenschutz für Firmen und Behörden', 'Transparenz Informationsfreiheit', and 'Pressemitteilungen und -informationen'. The main content area displays a breadcrumb trail: 'Home > News > Detail > Unzulässige Datenübermittlungen in die USA'. The article title is 'Unzulässige Datenübermittlungen in die USA' in red. Below the title is the sub-headline 'Erste Bußgelder rechtskräftig, weitere Verfahren noch offen'. The main text, dated 6.6.2016, states that the EuGH has annulled the Safe Harbor decision from October 2015, rendering it ineffective for data transfer to US companies. It also mentions that 35 international companies in Hamburg have been inspected.

HmbBfDI Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Wir über uns Kontakt | Ihr Recht auf Datenschutz | Datenschutz für Firmen und Behörden | Transparenz Informationsfreiheit | Pressemitteilungen und -informationen

[Home](#) > [News](#) > [Detail](#) > Unzulässige Datenübermittlungen in die USA

Unzulässige Datenübermittlungen in die USA

Erste Bußgelder rechtskräftig, weitere Verfahren noch offen

(hmbbfdi, 6.6.2016) Der EuGH hat die Safe Harbor-Entscheidung im Oktober 2015 aufgehoben und damit einen wesentlichen Pfeiler für eine rechtmäßige Datenübermittlung an US-Unternehmen für unwirksam erklärt. Daraufhin wurden durch den Hamburgischen Datenschutzbeauftragten Prüfungen bei 35 international agierenden Hamburger Unternehmen durchgeführt.

3 EU-US Privacy Shield ist heute

- 13.04.2016 (Presseerklärung)
Artikel-29-Gruppe sieht Bedenken :
 - Widerspruchsrecht des Betroffenen
 - Zugang staatliche US-Behörden zu den übermittelten Daten
 - ...
- 24.05.2016
EU Parlament Entschließungsantrag: EU-Kommission soll Mängeln beseitigen
- 12.07.2016
EU-US Privacy Shield: angemessenes Datenschutzniveau für Datenübermittlungen in die USA



3 EU-US Privacy Shield ist heute

- Was ist EU-US Privacy Shield?
- Selbstzertifizierung durch US-Unternehmen beim US-Handelsministerium ab dem 01.08.2016 möglich
- Folgende Pflichten für US Unternehmen sind ausgehandelt worden:
 - Informationspflicht des Betroffenen
 - Wahlmöglichkeit bei wesentlichen Zweck-Änderungen (opt in bei § 3 Abs. 9 BDSG und Art. 9 DS-GVO)
 - Weitergabe der Daten an Dritte (Pflichten müssen weitergereicht werden)
 - Sicherheit (angemessener Schutz)
 - Datenintegrität und Zweckbindung
 - Auskunftsrecht
 - Rechtsschutz, Durchsetzung und Haftung



3 EU-US Privacy Shield ist heute

<https://www.privacyshield.gov/list> (US Handelsministerium): Allgemein

The screenshot shows the Privacy Shield Framework website. At the top left is the logo with the text "Privacy Shield Framework". To the right is a search bar and "Sign Up" and "Log In" links. Below the logo are navigation links: "Self-Certify", "Privacy Shield List", "Audiences", and "About". A large search bar is present, followed by "ACTIVE" (underlined) and "INACTIVE" tabs, and an "Advanced" button. The main content area displays three active participants:

Company Name	Location	Framework	Covered Data
RocketBlocks	Oakland, California	EU-U.S. Privacy Shield Framework	Non HR
20/20 Software, Inc.	Stamford, Connecticut	EU-U.S. Privacy Shield Framework	Non HR
20 20 Research	Nashville, Tennessee	EU-U.S. Privacy Shield Framework	Non HR

Each entry includes a green "Active" indicator and a link for "Questions or Complaints".

3 EU-US Privacy Shield ist heute



Search [Sign Up](#) [Log In](#)

[Self-Certify](#) [Privacy Shield List](#) [Audiences](#) [About](#)

facebook

ACTIVE INACTIVE

Advanced

Facebook, Inc. Menlo Park, California ● Active	Framework EU-U.S. Privacy Shield Framework	Covered Data ⓘ Non HR Questions or Complaints
---	--	---

3 EU-US Privacy Shield ist heute

<https://www.privacyshield.gov/list> (US Handelsministerium): HR Data

The screenshot shows the Privacy Shield Framework website interface. At the top, there is a search bar and navigation links for 'Self-Certify', 'Privacy Shield List', 'Audiences', and 'About'. Below the search bar, there are tabs for 'ACTIVE' and 'INACTIVE', with 'ACTIVE' selected. A 'Refine by' section contains four dropdown menus: 'Participation Status' (set to 'Active'), 'Framework' (set to '-- NO FILTER --'), 'Covered Data' (set to 'HR Data'), and 'Dispute Resolution' (set to '-- NO FILTER --'). Below this is an 'Alphabetical Listing' with a link to 'A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|All'. The main content area displays two organization cards:

Organization Name	Location	Framework	Covered Data	Status
ACA Compliance Group	Silver Spring, Maryland	EU-U.S. Privacy Shield Framework	HR, Non HR	Active
ACCURATE INFORMATION SYSTEMS, LLC	VENICE, Florida	EU-U.S. Privacy Shield Framework	HR, Non HR	Active

3 EU-US Privacy Shield ist heute

- Gibt es Ausnahmen beim EU-US Privacy Shield?

Ja,

wenn Erfordernisse der nationalen Sicherheit, das öffentliche Interesse oder der Strafverfolgung Rechnung getragen werden muss.

- Gibt es besonderen Vorgaben bei Beschäftigtendaten?

Ja,

„HR-Zertifizierung“ notwendig



3 EU-US Privacy Shield ist heute

Prüfpflichten der verantwortlichen Stelle:

- Besitzt das datenempfangende Unternehmen ein gültiges Zertifikat?
- Sind die übermittelten Daten vom Zertifikat abgedeckt (HR vs. Non HR)?
- Kommt das US Unternehmen seinen Informationspflichten gegenüber den Betroffenen nach?



3 EU-US Privacy Shield ist heute

Leitfaden zum EU-US-Datenschutzschild:

http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf

Datenübermittlungen in die USA – Fragen und Antworten zum EU-US Privacy Shield:

https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt/Eingangsseite/EU_US_Privacy_Shield_Text_komplett.pdf



4 DS-GVO – was kommt morgen?

Regelungen in Art. 44 ff. DS-GVO (vergleichbar mit dem BDSG):

- Genehmigung der Datenübermittlung durch die zuständige Aufsichtsbehörde
- Binding Corporate Rules (BCR): Datenübermittlung innerhalb eines Konzerns (Genehmigung durch Aufsichtsbehörden)
- Einwilligung der Betroffenen nach Aufklärung der Risiken
- Neu: Verwendung EU Standardvertragsklauseln (nun auch modifizierbar)
- Neu: Ausnahmetatbestände Art. 49 Abs. 1 Satz 1 b – g DS-GVO
- Neu: Datentransfer hat überschaubaren Umfang und ist durch zwingende berechnete Interessen des Verantwortlichen gerechtfertigt (Art. 49 Abs. 1 Satz 2 DV-GVO)

Alle Inhalte dieser Präsentation unterliegen dem Urheberrecht.

© copyright BSP-SECURITY 2016

BSP-SECURITY
Franz-Mayer-Str. 1
93053 Regensburg

Tel. (09 41) 60 48 89-8 64,
Fax (09 41) 60 48 89-8 66
E-Mail: info@bsp-security.de
www.bsp-security.de

^

Es ist ausdrücklich untersagt, Texte, Bilder, Grafiken, Animationen oder sonstige Inhalte dieser Seite zu kopieren, zu verfremden oder anderweitig einzusetzen oder weiter zu verwerten.