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
Fax: +49 (0)941 60 48 89-8 66
Mobil: +49 (0)152 32 01 04 95

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

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

BSP-SECURITY

Agenda

1 Datenübermittlung in Drittstaaten

2 Safe Harbor war gestern

3 EU-US Privacy Shield ist heute

4 DS-GVO – was kommt morgen?

BSP-SECURITY

„ 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)

BSP-SECURITY

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)

BSP-SECURITY

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.

BSP-SECURITY

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
- …

BSP-SECURITY

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?

BSP-SECURITY

3 EU-US Privacy Shield ist heute

BSP-SECURITY

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

Privacy Shield Framework

BSP-SECURITY

3 EU-US Privacy Shield ist heute

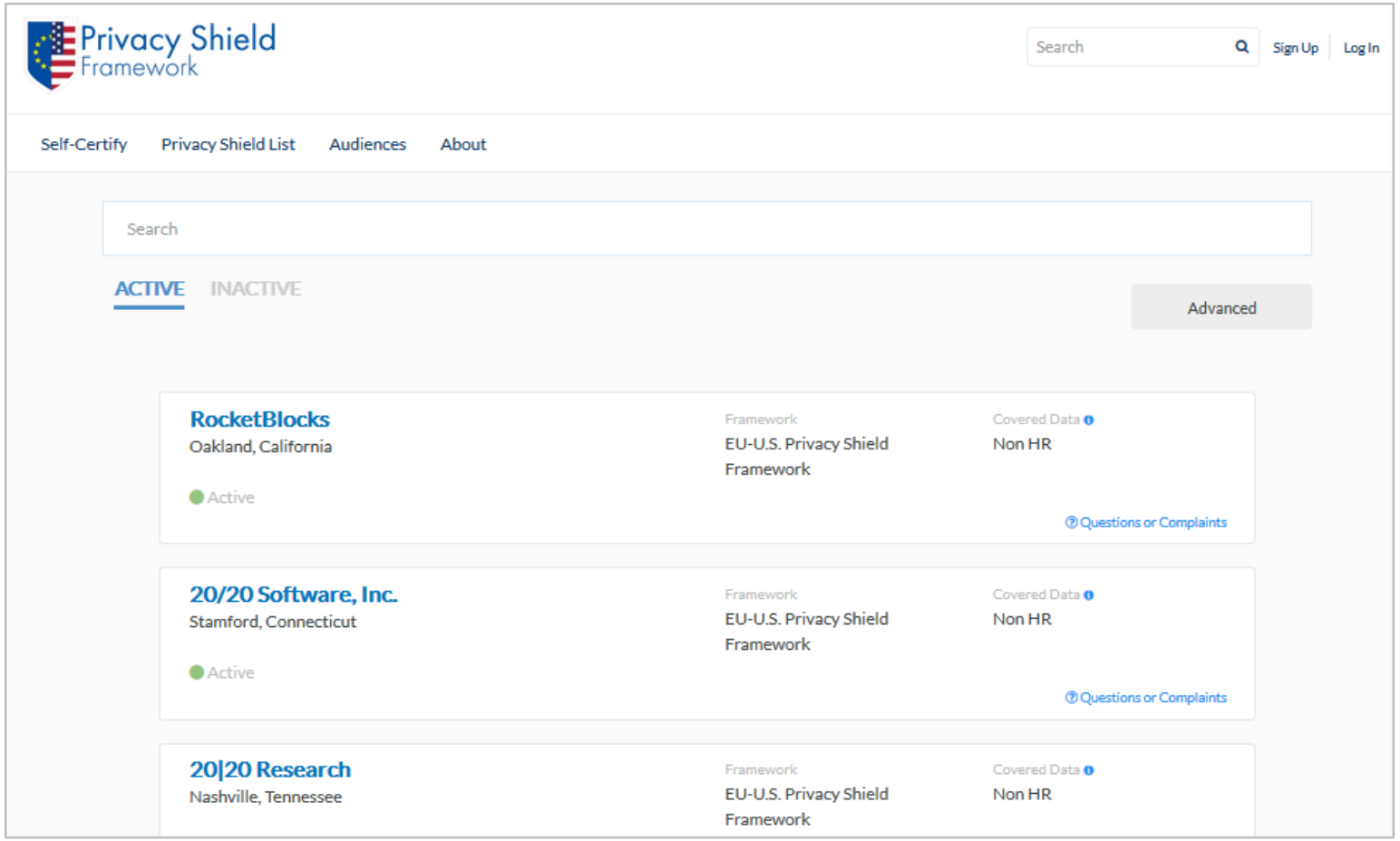
- Was ist EU-US Privacy Shield?
- Selbstzertifizierung durch US-Unternehmen beim US-Handelsministerium ab dem 01.08.2016 möglich
- Folgende Pflichten für US Unternehmen sind ausgehandelt worden:
  - Informationspflicht des Betroffenen
  - Wahlmöglichkeit bei wesentlichen Zweck-Änderungen (opt in bei § 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

Privacy Shield Framework

BSP-SECURITY

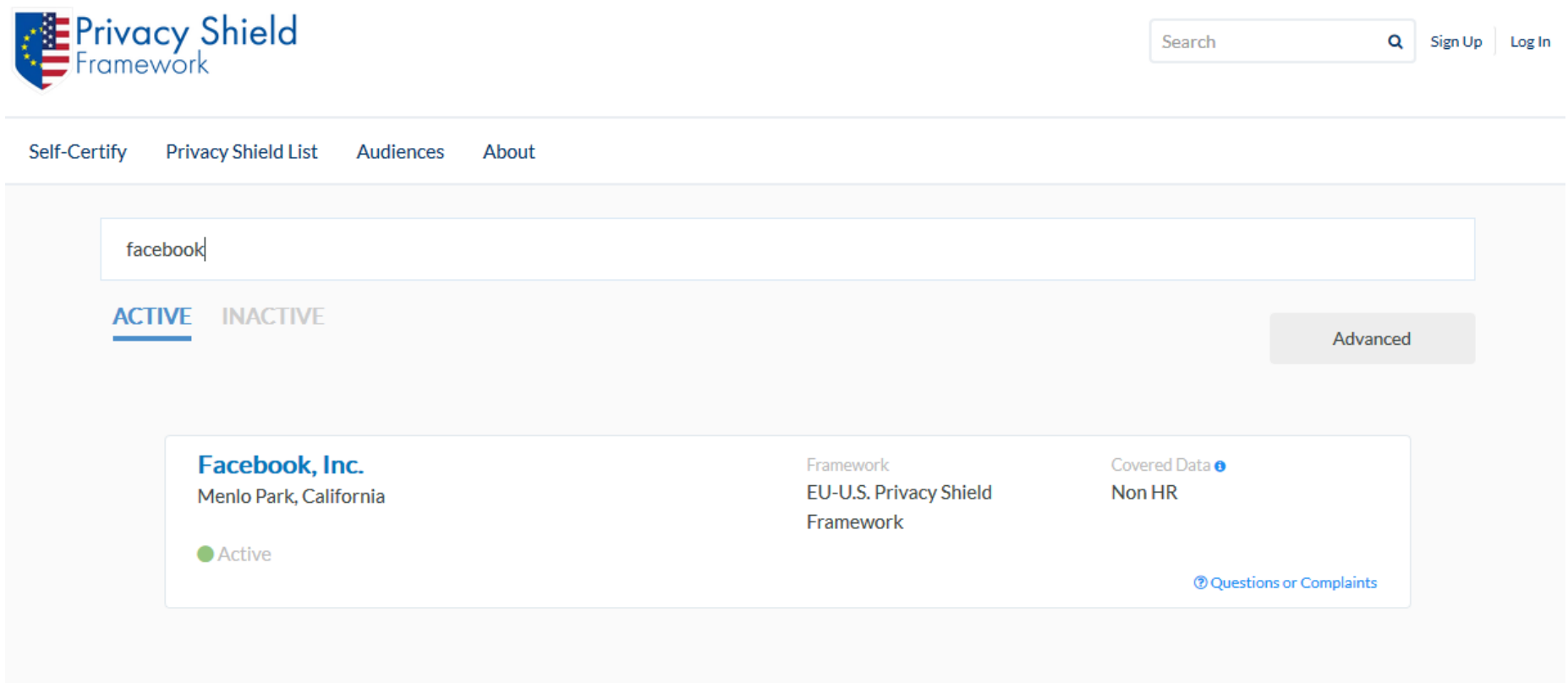
3 EU-US Privacy Shield ist heute

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



BSP-SECURITY

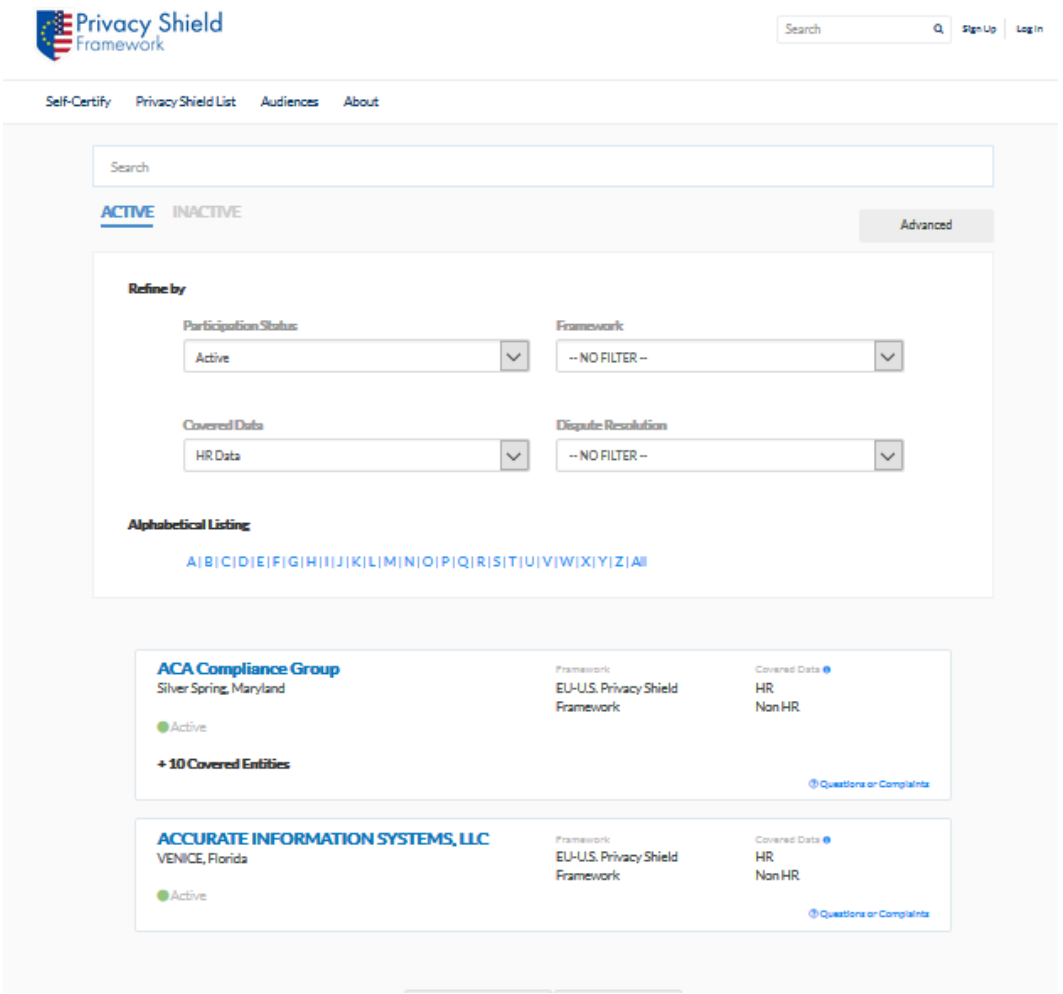
3 EU-US Privacy Shield ist heute



BSP-SECURITY

3 EU-US Privacy Shield ist heute

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



BSP-SECURITY

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

Privacy Shield Framework

BSP-SECURITY

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?

BSP-SECURITY

Privacy Shield Framework

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.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt/Eingangsseite/EU_US_Privacy_Shield_Text_komplett.pdf

BSP-SECURITY

Privacy Shield Framework

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 berechtigte Interessen des Verantwortlichen gerechtfertigt (Art. 49 Abs. 1 Satz 2 DV-GVO)

Alle Inhalte dieser Präsentation unterliegen dem Urheberrecht.

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

^