SCHEJA & PARTNER

Rechtsanwälte
Externe Datenschutzbeauftragte

Praxiserfahrungen mit Privacy Shield

BvD-Verbandstag - 4. Mai 2017

Volker Schaa
Dr. Gregor Scheja

Aktuelles

27.01.2017

31.03.2017

07.04.2017

- Ca. 2000 zertifizierte Unternehmen
  - z.B. Microsoft, Google, Facebook, Amazon, Salesforce, Oracle
  - derzeit nicht: Apple, ADP
- Erste jährliche Überprüfung nun wohl erst im September
- Swiss-U.S. Privacy Shield seit 12. April 2017

Agenda

1. Rechtlicher Rahmen für internationale Datentransfers
2. Privacy Shield im Überblick
3. Praxiserfahrungen

1. Rechtlicher Rahmen für internationale Datentransfers

Rechtlicher Rahmen für internationale Datentransfers

- Zwei Stufen Theorie:
  - Erste Stufe:
    - Legitimation nach nationalem bzw. „einfachem“ europäischen Recht
  - Zweite Stufe:
    - angemessenes Datenschutzniveau oder hinreichende Garantien
    - falls beides (-): internationale Übermittlung unzulässig, sofern keine Ausnahme vorliegt
  - Angemessenes Datenschutzniveau: Angemessenheitsentscheidung, auch Privacy Shield
  - Hinreichende Garantien: z.B. SCC, BCR
- DSGVO behält zweistufiges Regelungskonzept bei

Ausnahmen von der zweiten Stufe

- Übermittlungen in ein Drittland auch ohne angemessenes Schutzniveau möglich, Art. 26 Abs. 1 RL 95/46/RG, § 4 c Abs. 1 BDSG bzw. Art. 49 Abs. 1 DSGVO

- Einwilligung des Betroffenen
- Erfüllung eines Vertrags mit dem Betroffenem
- Abschluss/Erfüllung eines Vertrags im Interesse des Betroffenen
- Wahrung wichtiger öffentlicher Interessen oder Rechtsansprüche
- Wahrung lebenswichtiger Interessen des Betroffenen
- Daten aus zur Information der Öffentlichkeit bestimmten Registern

- Vorliegen einer Ausnahme stets im Einzelfall zu beurteilen

Standardvertragsklauseln

- Durch EU-Kommission verabschiedete standardisierte Vertragsklauseln
- „Ausreichende Garantien" im Sinne von Art. 26 Abs. 2, 4 RL 95/46/EG
- Verschiedene Sets für „Controller-to-Controller"- bzw. „Controller-to-Processor"-Übermittlungen
- Standardvertragsklauseln dürfen inhaltlich nur sehr eingeschränkt abgeändert werden

- Aktuell: Verfahren vor Irish High Court, wahrscheinlich Vorlage zum EuGH
- Anpassung der Standardvertragsklauseln angesichts der Datenschutz-Grundverordnung zu erwarten

Binding Corporate Rules

- Verbindliche Unternehmensregeln für konzerninterne internationale Datentransfers
- „Ausreichende Garantien“ im Sinne von Art. 26 Abs. 2, RL 95/46/EG
- Vergleichsweise flexible Gestaltungsmöglichkeiten, aber hoher Umsetzungsaufwand
- Empfehlungen und Stellungnahmen der Artikel-29-Gruppe zur Ausgestaltung
- Seit 2013 auch für Auftragsdatenverarbeitung im Konzern
- Prüfung und Genehmigung durch europäische Aufsichtsbehörden erforderlich

- DSGVO: nunmehr ausdrücklich geregelt in Art. 47, einschließlich Aufzählung von Pflichtinhalten

2. Privacy Shield im Überblick

Privacy Shield im Überblick

- Angemessenheitsentscheidung der EU-Kommission
- Selbstzertifizierung durch US-Unternehmen
- Einhaltung bestimmter Datenschutzprinzipien
- Begleitende Dokumente zur geplanten Kontrolle und Dursetzung, Beschränkung der Befugnisse von Sicherheitsbehörden, Einführung einer Ombudsperson

Privacy Shield Principles

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation
- Access
- Recourse, Enforcement and Liability

Supplemental Principles:

- Sensitive Data, Journalistic Exceptions, Secondary Liability, Performing Due Diligence and Conducting Audits, The Role of the Data Protection Authorities, Self-Certification, Verification, Access, Human Resources Data, Obligatory Contracts for Onward Transfers, Dispute Resolution and Enforcement, Choice – Timing of Opt Out, Travel Information, Pharmaceutical and Medical Research, Public Record and Publicly Available Information, Access Requests by Public Authorities

Was ist neu – Notice / Choice

- Erweiterter Umfang der Informationspflichten, z.B. über bestehende Rechtsschutzmöglichkeiten

- Keine Ausnahme von der Informationspflicht bezüglich Weitergabe von Daten an (Unter-)Auftragsverarbeiter

Was ist neu – Onward Transfer

- Grundsätzliche Verpflichtung zum Abschluss von Verträgen mit Dritten bei Weitergabe von Daten
- Sowohl bei Weitergabe an Agents als auch an Controller
- Verpflichtung auf dasselbe Datenschutzniveau wie nach den Privacy Shield Principles
- Ausnahmen:
  - Weitergabe an Controller innerhalb einer Unternehmensgruppe + andere „Instrumente" vorhanden
  - Weitergabe an Controller für „gelegentliche beschäftigungsbezogene operative Erfordernisse", z.B. Buchung von Flügen oder Hotelzimmern, Abschluss von Versicherungen
- Übergangsfrist: bei Registrierung bis 30. September 2016 Frist von 9 Monaten zum Abschluss erforderlicher Verträge
- Verantwortlichkeit/Haftung bei Weitergabe an Agents

Was ist neu – Recourse, Enforcement & Liability

- Dreistufiges Rechtsschutzsystem für Betroffene:
  - 1. Stufe: interne Prozesse zur Bearbeitung von Beschwerden
    - Antwortfrist von 45 Tagen
  - 2. Stufe: unabhängige Beschwerdestellen
    - kostenlos für Betroffene
    - für Beschäftigtendaten: europäische Aufsichtsbehörden
    - sonst: entweder europäische Aufsichtsbehörden oder private Stellen (z.B. TRUSTe, AAA, BBB, JAMS)
  - 3. Stufe: Rechtlich bindendes Schiedsverfahren („Privacy Shield Panel")
    - wird derzeit erst noch aufgesetzt
- Durchsetzungsbefugnisse in den USA bei der Federal Trade Commission, in Europa bei den Aufsichtsbehörden
- Ombudsperson als Vermittler zwischen EU-Betroffenen/Aufsichtsbehörden und U.S.-Sicherheitsbehörden

Was ist neu – HR Data

- Human Resources Data: “Personal information about employees (past or present) collected in the context of the employment relationship”
- Separate HR-Policy erforderlich
- Opt out oder Verweigerung von Opt in im Rahmen von Choice darf nicht zu Nachteilen für Arbeitnehmer führen
- Daten dürfen nicht für Zwecke verwendet werden, die mit dem Erhebungszweck nicht vereinbar sind
- Ausnahmen von Onward Transfer und Access-Anforderungen für “gelegentliche beschäftigungsbezogene operative Erfordernisse“, z.B. Buchung von Flügen oder Hotelzimmern, Abschluss von Versicherungen

3. Praxiserfahrungen

Erforderliche Maßnahmen für US-Unternehmen

- Einhaltung der Privacy Shield Principles
- Öffentlich verfügbare Privacy Shield Policy
- Ggf. zusätzliche Policy für Beschäftigtendaten („HR Data“)
  - Nicht öffentlich, aber dem Department of Commerce zur Verfügung zu stellen
- Auswahl und ggf. Registrierung bei einer unabhängigen Beschwerdestelle
- Registrierung auf der Privacy-Shield-Website des Department of Commerce
  - Prüfung der Policies und weiterer Informationen durch DoC
  - Zahlung von Gebühren
  - Anschließend Aufnahme in die Privacy-Shield-Liste
- Jährliche Re-Zertifizierung erforderlich

Anforderungen an die Selbstzertifizierung

- Anforderungen ergeben sich aus Supplemental Principle „Verification“
- Unternehmen muss sicherstellen, dass die eigenen Privacy Shield Policies vollständig ungesetzt sind und eingehalten werden
- Überprüfung kann eigenständig durchgeführt werden („self-assessment“) oder durch Dritte („outside compliance review“)
- Self-assessment setzt insbesondere voraus:
  - Regelmäßige objektive Überprüfung der Einhaltung der Privacy Shield Principles
  - Schulung der Mitarbeiter
  - Interne Prozesse zum Umgang mit Beschwerden und Auskunftsbegehren
  - Dokumentation der Ergebnisse

Privacy Shield Policies

- Mindestinhalte:
  - Erklärung, dass die Privacy Shield Principles eingehalten werden
  - Link zur Privacy Shield Website
  - Benennung der unabhängigen Beschwerdestelle einschließlich Link zu deren Website und ggf. zu einem Beschwerdeformular

- Empfehlenswert: Information gemäß Notice ebenfalls aufnehmen:
  - Nennung aller zertifizierten Legaleinheiten
  - Datenkategorien und Verarbeitungszwecke
  - Bei Weitergabe von Daten an Dritte: Benennung der Zwecke und Kategorien von Empfängern
  - Kontaktmöglichkeit für Fragen und Beschwerden
  - Hinweise auf Auskunftsrecht sowie opt-out / opt-in Möglichkeiten (Choice)
  - Nennung der einschlägigen US-Aufsichtsbehörde (z.B. FTC)
  - Hinweis auf Möglichkeit bindender Schiedsverfahren
  - Hinweis auf Verpflichtung, Daten auf Anfrage gegenüber Behörden offenzulegen
  - Hinweis auf Haftung im Rahmen von Onward Transfer

Verträge mit Dritten (Onward Transfer)

Agent	Controller
Verpflichtung, weitergegebene Daten nur für festgelegte Zwecke zu verarbeiten	Verpflichtung, weitergegebene Daten nur für festgelegte Zwecke und ggf. im Einklang mit der erteilten Zustimmung (Choice) der Betroffenen zu verarbeiten
Verpflichtung zur Gewährleistung des Datenschutzniveaus des Privacy Shields	Verpflichtung zur Gewährleistung des Datenschutzniveaus des Privacy Shields
Verpflichtung zur Information, falls das Datenschutzniveau des Privacy Shields nicht mehr gewährleistet werden kann	Verpflichtung zur Information, falls das Datenschutzniveau des Privacy Shields nicht mehr gewährleistet werden kann
Regelungen zur Sicherstellung der Datenverarbeitung durch den Agent im Einklang mit dem Privacy Shield, z.B.: • Weisungsgebundenheit • Technische und organisatorische Maßnahmen • Unterbeauftragung • Kontrollrechte • Unterstützungspflichten	Verpflichtung, den Betroffenen einen Beschwerdemechanismus zur Verfügung zu stellen

Informationen über zertifizierte Unternehmen

- Öffentlich einsehbar: Privacy Shield Website (www.privacyshield.gov/list)
  - Gültige Zertifizierung vorhanden?
  - Auf welche Datenkategorien bezieht sich die Zertifizierung?
  - Ergeben sich weitere Informationen/Einschränkungen aus der Policy?
  - Welcher Rechtsschutzmechanismus steht zur Verfügung?

- Anzufordern – keine Pflicht zur Herausgabe:
  - Berichte bzw. Dokumentation über Umsetzung der Privacy Shield Principles
  - Dokumentation interner Beschwerdeprozesse und Schulungskonzept für Mitarbeiter
  - Musterverträge für Onward Transfer

Privacy Shield im Vergleich

- Standardvertragsklauseln: US-Unternehmen unterzeichnet Vertrag – und dann?

- Privacy Shield: US-Unternehmen…
  - … bestätigt Einhaltung der Privacy Shield Principles gegenüber US-Behörde jährlich neu
  - … veröffentlicht eine für jedermann einsehbare Policy
  - … muss Einhaltung der Privacy Shield Principles regelmäßig überprüfen (oder überprüfen lassen) und Ergebnis dokumentieren
  - … muss interne Prozesse zum Umgang mit Beschwerden und Anfragen entwickeln und Mitarbeiter schulen

- Ermöglicht das Privacy Shield die Einschaltung weltweiter (Unter-) auftragsverarbeiter?
  - Privacy Shield setzt nur Abschluss eines Onward Transfer-Vertrags voraus
  - Aber: möglicherweise Unterwanderung des angemessenen Datenschutzniveaus
  - Gemäß Privacy Shield haftet zertifiziertes Unternehmen grundsätzlich für eingeschaltete Agents

Zukunft des Privacy Shield

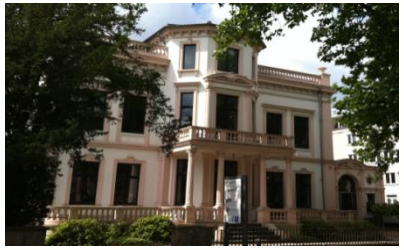
- Jährliche Überprüfung: voraussichtlich erstmals im September 2017
- Bestandsschutz für Angemessenheitsentscheidungen unter der DSGVO
- Neue Regierung in den USA – werden 2016 gemachte Zusagen Bestand haben?
- Gerichtsverfahren irischer und französischer Verbraucherverbände gegen Privacy Shield beim EuG anhängig

Fragen & Diskussion

Vielen Dank!

Kontakt

Scheja und Partner Rechtsanwälte mbB
Externe Datenschutzbeauftragte



Adenauerallee 136 · 53113 Bonn
T +49 228 227 226-0 · F +49 228 227 226-26

Große Bleichen 17 · 20354 Hamburg
T +49 40 228 207 16-0 · F +49 40 228 207 16-9

Leopoldstr. 244 · 80807 München
T +49 89 215 559 16-0 · F +49 89 215 559 16-9

Unter den Linden 16 · 10117 Berlin
T +49 30 120 769 63-0 · F +49 30 120 769 63-9

info@scheja-partner.de
www.scheja-partner.de