Introduction to

AIJA

www.aija.org

Lost in Privacy? – How to tackle transatlantic data protection challenges

New York, 2-3 February 2017

Post Safe Harbor:
Solutions for International Data Transfers

New York, 3 February 2017 / Lost in Privacy?

Moderator: Christine Borfiga
Speakers: James J. Pastore and Dr Johannes Struck

www.aija.org

Where is my data?

Before drilling into international transfers

- Is a Data Protection Officer appointed?
- Nature of the data/processing?
- Who shares/accesses the data: affiliates, service providers, clients, distributors, etc.?
- Role of the data importer: processor or controller?
- Information provided to data subjects, works council?
- Notifications/authorizations already filed or to be filed?

www.aija.org

- Transferring data from the EU:

  Dr. Johannes Struck

  Brödermann Jahn, Germany

- A different approach in the US based on cybersecurity:

  James J. Pastore

  Debevoise & Plimpton, USA

Transferring data from the EU

Example Case

- German Company
- Using a software, licensed by US company
- Maintenance and Support Agreement with such US software company
- Maintenance and support services via remote access

Transferring data from the EU

Requirements for international data transfers depend on …

- the **type of data** involved

  only **personal data** according to Article 4 (1) GDPR

> ***'personal data'*** *means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, conomic, cultural or social identity of that natural person;*

Transferring data from the EU

Requirements for international data transfers depend on …

- the **destination** of the data to be transferred

EU (European Union)	EEA (European Economic Area)	„Third Countries“
EU Member States	Iceland Liechtenstein Norway	All other countries

Transferring data from the EU

Solutions for international data transfer to **Third Countries**

- **“2-Step-Test”**

1st step	Is **data transfer permitted** (according to national law)?
2nd step	Does the country of destination have an **adequate level of data protection**?

Transferring data from the EU

Solutions for international data transfer to **Third Countries**

- **adequate level of data protection**

EU adequacy decision (Art. 45 GDPR)

Andorra
Argentina
Canada
Switzerland
Faeroe Island
Guernsey
Israel
Isle of Man
Jersey
New Zealand
USA (Privacy Shield)
Eastern Republic of Uruguay

or

Appropriate Safeguards (Art. 46 GDPR)

- Standard Data Protection Clauses
- Binding Corporate Rules
- Code of Conduct *(new!)*
- Approved Certification Mechanism *(new!)*

or

Derogations for specific situations (Art. 49 GDPR)

- consent by data subject
- Transfer is necessary
  - for the performance of a contract between the data subject and the controller
  - for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
  - for important reasons of public interest
  - (…)

Transferring data from the EU

Solutions for international data transfer to **Third Countries**

- **appropriate safeguards (Art. 46 GDPR)**

Standard Data Protection Clauses

- "(EU-)controller to (Non-EU/EEA-)controller"
  - Decision 2001/497/EC: Set I
  - Decision 2004/915//EC: Set II
- "(EU-)controller to (Non-EU/EEA-)processor"
  - Decision 2010/87/EU (and repealing Decision 2002/16/EC)(101 kB)
- Cannot be changed without approval by Data Protection Authority

or

Binding Corporate Rules (BCR)

- Internal rules adopted by multinational group of companies
- Must contain:
  - Privacy Principles (transparency, data quality, security, etc.)
  - Tools of effectiveness (audit, training, complaint handling systems, etc.)
  - Element proving that BCR are binding.
- Autorization by national Data Protection Authority (resp. European Data Protection Board)

or

Code of Conduct *(new under GDPR! Art. 40)*

- Associations and other bodies representing categories of controllers or processors may prepare codes of conduct
- Specific requirements with regard to the content of such a CoC are laid down in Art. 40 (2) GDPR
- Authorization by national Data Protection Authority (resp. European Data Protection Board)

or

Approved Certification Mechanism *(new under GDPR! Art. 42)*

- Certification bodies are not yet established
- Certification shall be issued for a max. period of 3 years and may be renewed, under the same conditions

Transferring data from the EU

Who needs to comply with the requirements?

Examples Involved Parties	
Companies based within the EU contracting with companies based in a „Third Country“ (including intercompany)	yes
Company based in a Third Country running a website which can be accessed via the internet by persons within the EU	No
Company based in a Third Country running a website which is intended for customers within the EU (e.g. German language, webshop with German hotline etc.)	Yes

Transferring data from the EU

HOWEVER, please note:

- The civil rights organization **Digital Rights Ireland** has filed a nullity suit against "EU-US Privacy Shield" (Az. T-670/16).

- The Irish data protection authority has brought the EU-standard contract clauses before the Irish High Court to clarify their current legal conformity.

Thank you !

- **Christine Borfiga**, Astine, Paris, France, cborfiga@astinelegal.com
- **James J. Pastore**, Debevoise & Plimpton, New York, USA, jpastore@debevoise.com
- **Dr. Johannes Struck**, Brödermann Jahn, Hamburg, Germany, johannes.struck@german-law.com