The End of “Safe Harbor” for E.U./U.S. Data Transfer:

How Can Companies Transfer Personal Data and Remain Compliant?

Presented by:

The FACC-NY, Foley Hoag LLP and the Consulate General of France in New York

Panel Discussion & Networking Reception

May 25, 2016

The End of "Safe Harbor" for E.U./U.S. Data Transfer

25 May 2016

Directive 95/46/EC of 24 October 1995

Articles 25 and 26

The transfer of personal data to a third country is allowed:

- if the third country ensures an adequate level of protection;

  the Commission can assess this, enter into negotiations to remedy the situation and issue an "adequacy decision";
- if the third country does not ensure an adequate level of protection but:
- certain conditions are fulfilled (e.g. consent) or
- the controller adduces adequate safeguards (e.g. appropriate contractual clauses).

Decisions issued to implement the Directive

- Commission decision 2000/520 of 26 July 2000 on the adequation of the protection provided by the safe harbour privacy principles.
- Commission decisions on Standard Contractual Clauses (SCC)
- Working papers of the WP on Binding Corporate Rules (BCR)
- Commission decisions relating to countries that ensure adequate protection (Canada, Switzerland, Israel etc…)

Schrems decision

Edward Snowden

Maximilian Schrems

Schrems Decision of the CJEU of October 6, 2015:

- the Safe Harbour Commission decision is invalid,
- an adequacy decision issued by the Commission *« does not prevent a national DPA from finding that the law and practices in force in the third country do not ensure an adequate level of protection »*.

Privacy Shield

Commission draft adequacy decision released on February 29, 2016

- Same mechanism as the Safe Harbor scheme (self certification).
- Stronger obligations on US companies.
- New means of redress for European citizens.
- Letters explaining rules on the access to Europeans data by US public authorities for national security purposes.

Opinion of the WP (April 13, 2016)

WP has « strong concerns:

<u>Commercial aspects:</u>

- application of the purpose limitation principle is unclear,
- data retention principle is not expressely mentionned,
- no specific wording on protection against automated individual decisions based solely on automated processing,
- onwards transfers to third countries should provide the same level of protection,
- new redress mechanism are too complex and ineffective.

<u>Access by US public authorities:</u>

- massive and indiscriminate collection of data originating from the EU is not excluded.

Next steps

- The article 31 Committee must issue an opinion which is binding,
- The Commission has indicated that it will take into account the WP29 opinion and is aiming at issuing a decision towards the end of June.

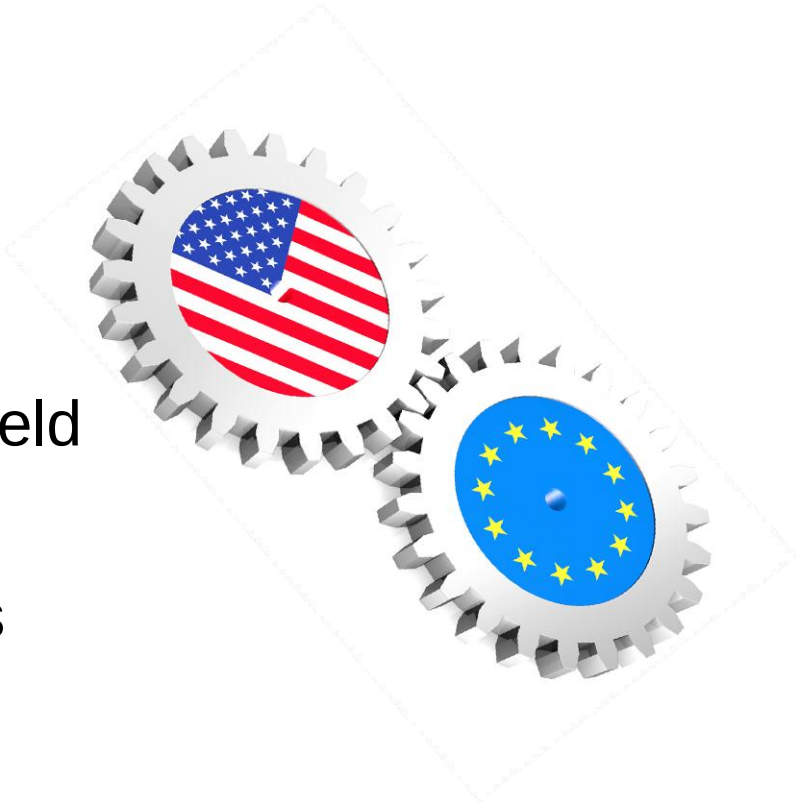
The End of the "Safe Harbor" Rule for E.U./U.S. Data Transfer: EU v. U.S. Cultural/Political/Legal Differences and Why They Matter

May 25, 2016

Colin J. Zick, Partner
Foley Hoag LLP
czick@foleyhoag.com

Differences in the political/legal framework and culture

- What are the differences?
- Can the U.S. and EU mesh despite these differences?
  - Reactions to the Privacy Shield
  - Next steps:
    - for EU and U.S. authorities
    - for businesses



Comparative Structures

- Civilian Regulators
  - EU is consolidated, with individual data protection authorities for enforcement; U.S. is fragmented, both by state and federal, and by type of data.
  - These differences reflect fundamental legal and cultural differences in the approach toward individual privacy.

Differing Reactions to the Privacy Shield

Pros: mainly EU and U.S. officials and certain professional organizations

- Vera Jourova (EU Justice Commissioner)
- Penny Pritzker (U.S. Secretary of Commerce)
- John Higgins (Director general of trade association DigitalEurope)

Cons:

- Max Schrems (the Austrian lawyer/plaintiff)
- Members of the European Parliament:
  - Jan Phillipp Albrecht (German Green who participated in the elaboration of the GDPR)
  - Sophie in't Veld (Dutch)

Mixed:

- Article 29 Working Party, the body of European Data Protection Authorities.

FOLEY HOAG LLP

Next Steps

- **Privacy Shield**
  - The EU Privacy Directive states that a committee composed of representatives of all Member States must also issue an opinion on the Privacy Shield.
  - The opinions of that Committee and of the Article 29 Working Party are not binding, so the European Commission could still issue a favorable adequacy decision on the current version of the Privacy Shield.
  - However, the ECJ also ruled in the Schrems case that EU member DPAs are not bound by the Commission's adequacy decisions.
  - The Privacy Shield is likely be challenged in the ECJ even if the Commission approves it (which could come in June).
- **Other Transfer Mechanisms?**
  - Article 29 Working Party must still consider whether transfer mechanisms such as Standard Contractual Clauses and Binding Corporate Rules can still be used.

Comparative Structures

- Intelligence Community
  - EU itself does not have an intelligence function, but member states do.
    - Although this could change: "Europe's intelligence 'black hole': Paris attacks spur calls for a European FBI, but many remain reluctant to share intelligence." 12/3/15, http://www.politico.eu/article/europes-intelligence-black-hole-europol-fbi-cia-paris-counter-terrorism/
  - U.S. still snooping and storing data after Schrems but "The U.S. Has Taken Multiple and Significant Actions to Reform Surveillance Laws and Programs Since 2013." P. Swire, U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013, http://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf

FOLEY HOAG LLP

U.S. Intelligence Community Privacy Primer

- U.S. IC agencies have strict operational restrictions on information they may collect
  - Must have a legal mission (foreign/counter intelligence)
  - Must comply with a mosaic of laws and policies governing intelligence collection, including the U.S. Constitution, FISA, Executive Order 12333 and its implementing procedures, and other Presidential/departmental/agency regulations

FOLEY HOAG LLP

U.S. Intelligence Community Privacy Primer

- President Obama issued PPD-28 in Jan. 2014
  - SIGINT must *always* be tailored as feasible to be conducted in a targeted (vice indiscriminate) fashion
  - "Bulk" collection (information acquired without discriminants such as specific identifiers/selection terms) restricted to limited topics
    - Detecting foreign intelligence activity, CT, CP, cyber, threats to U.S. person safety, and transational criminal activity
  - Extends privacy protections to non-U.S. persons
    - Information cannot be retained or disseminated unless related to an enumerated intelligence priority, is evidence of a crime, or meets another criterion in EO 12333, Section 2.3

FOLEY HOAG LLP

U.S. Intelligence Community Privacy Primer

- Section 702 of FISA allows collection of non-U.S. person communications located outside the U.S. that relates to critical foreign intelligence categories
  - Categories of collection (such as counterterrorism or weapons of mass destruction) must be approved annually by the FISA Court
  - FISA Court also requires targeting and minimization procedures
    - Targeting ensures that information is collected based on individual selectors, such as email addresses or phone numbers
    - Minimization ensures that personal information is protected, and only disseminated for a valid foreign intelligence or law enforcement purpose

www.icontherecord.tumblr.com

FOLEY HOAG LLP

Next Steps

- **Some Companies Are Not Waiting**
  - Some are adopting Standard Contractual Clauses and Binding Corporate Rules
  - Some are setting up EU member-specific data storage.