

EU-US Privacy Shield Overview

Greg Guice and David Turetsky

Roadmap for Presentation

- Background
- Seven Principles
- Special Requirements to Transfer Human Resource Data
- Redress Mechanism
- Next Steps
- Questions

Background

- 1995 - Data Privacy Directive adopted in EU prohibiting the sending of personal data to “third countries” unless they can guarantee adequate levels of protection (data subject agrees, BCR or SCC authorized)
- 2000 - EU-US Safe Harbor adopted to allow for the transfer of data between EU and US
- 2013 – EC determines that the basis for the Safe Harbor must be reviewed because of rapid growth in data collection, increase in US companies adhering to Safe Harbor, and new information on US intelligence community activities that raised concerns
- 2014 – EU-US talks begin on reforms to Safe Harbor
- 2015 – *Schrems* decision invalidated Safe Harbor concluding that the EC had not stated that the US “ensured an adequate level of protection by reason of its domestic law or its international commitments.”
 - The Court further explained while protections need not be identical, they must offer “essentially equivalent” protections
- July 12, 2016 – EU-US Privacy Shield adopted by EC

Seven Principles

■ Notice

- Organizations must provide information to individuals (“data subjects”) on the processing of personal data (type, purpose, right to access and choice, conditions for onward transfer) and that the organization is participating the Privacy Shield

■ Choice

- Allows opt-out where certain information is to be disclosed to third party or use is materially different, but compatible with, the purpose for which it was originally collected
- Obtain opt-in for sensitive information (e.g. health, race/ethnicity, political opinion, belief, trade union, sex life) and information a third party identifies and treats as sensitive
- No additional choice required where third party is acting as an agent of the organization

■ Individual Access

- Individuals have a right to obtain confirmation of whether an organization is processing personal data about them and get access to the data, without justification and for a “non-excessive fee.”
- Individuals have a right to correct, amend, or delete personal information that is inaccurate or processed in violation of the principles
- Very limited exceptions for access: where the legitimate rights of persons other than the individual would be violated or where burden of expense is disproportionate to privacy risk
- Automated processing to be monitored (and part of first annual review)

Seven Principles (cont.)

■ Data Integrity and Purpose Limitation

- Limited to what is relevant, reliable for intended use, complete and accurate
- Retention for only as long as it serves the purpose for its collection
 - Exceptions for: public interest, journalism, art/lit, scientific and historical research and statistical analysis

■ Security

- Organizations must take reasonable and appropriate measures (based on risk involved and nature of the data). Sub-processors must guarantee same level of protection

■ Accountability For Onward Transfer

- Only for limited and specific purposes consistent with the consent provided and must be contractual (narrow exception for intragroup compliance and control programs) and provide the same level of protection
- Notice and Choice Principles apply

■ Recourse, Enforcement and Liability

- Annual recertification of participation
- Verify via self-assessment or independent corroboration that privacy policy conforms to these Principles
 - Self-assessment must include: employee training, periodic objective review
- Organization must have redress mechanism in place (more detail in Slide 6)

Special Requirements for Transfer of Human Resource Data

HR-specific provisions:

■ Notice and Choice applicability

- Privacy policy need not be public, but must be available to employees
- Disclosure to third parties or for different purposes than originally collected must be done in accordance with Notice and Choice principle.
- Choice cannot be used to restrict employment opportunities or used punitively
- Member States rules remain effective and may further limit use
- Employers should make reasonable efforts to accommodate employees' privacy preferences
- No need to offer notice or choice for use in promotion, appointment or similar decisions

■ Access

- Local and national law of EU Member states still applies
- Organizations processing data must provide access directly or through the EU employer

■ Enforcement

- Personal information used only in the context of employment remains with the EU employer and thus recourse is through the state or national data protection or labor authority
- US organization must commit to cooperate in investigations and comply with the advice of EU authority

■ Onward Transfer

- Occasional, operational needs (flight, hotels, insurance) data transfer permitted without Access principle or third party contract rules applying

Redress Mechanisms

Seven redress mechanisms (for individual complaints)

- Address directly with the organization – Self-certifying organizations must offer and privacy policy must include POC.
 - Response required within 45 days of receipt
- Independent dispute resolution body (IDR) – provides appropriate recourse free of charge and sanctions and remedies must be “sufficiently rigorous” to ensure compliance
 - IDR can be located in US or EU and failure to comply with a ruling requires notification to Commerce and the FTC and de-listing for repeated failure to comply
 - IDR must publish annual report of aggregate statistics on its services
- National DPA – Individuals can bring complaints through DPAs
 - Organizations must cooperate
 - Both sides are afforded opportunity for comment and decision should be made in a reasonable time period (generally 60 days). Compliance required within 25 days after advice delivered
 - Failure to comply could result in referral to FTC or removal from the list

Redress Mechanisms (cont.)

- Dept. of Commerce (DOC) – Committed to receive, review and resolve complaints from DPAs on behalf of individuals
 - DOC will provide status updates every 90 days on pending complaints and an annual report of aggregate data on complaints received
- FTC (or other regulatory agency where FTC lacks authority) – Priority given to independent dispute resolution bodies and self-regulatory bodies, DOC, and DPAs
 - It will take complaints from individuals and investigate as part of broader privacy enforcement
- “Last resort” binding arbitration – Available where the other mechanisms have “not satisfactorily resolved an individual’s complaint.” (Article 57-58)
 - Organizations must inform individuals about the possibility of this mechanism
 - Individuals can seek relief even where another process provided remedies (but see Annex 2 limitations, prohibiting monetary relief, etc.)
- Judicial redress – US courts under common law claims (tort, fraudulent misrepresentation, breach of contract)

Next Steps

- EU Member States representatives approved the package on July 12
- Federal Register publication of the Privacy Shield Package within 30 days from July 12
- August 1 – self certification begins through website at Dept. of Commerce
- Organizations filing with in the first 60 days get an additional 9 months to finalize contract terms with third parties for purposes of onward transfer