A Better Partnership®

Warner Norcross&Judd® LLP
ATTORNEYS AT LAW

Getting Up to Speed on the New Privacy Shield & Steps for Self-Certification

September 7, 2016

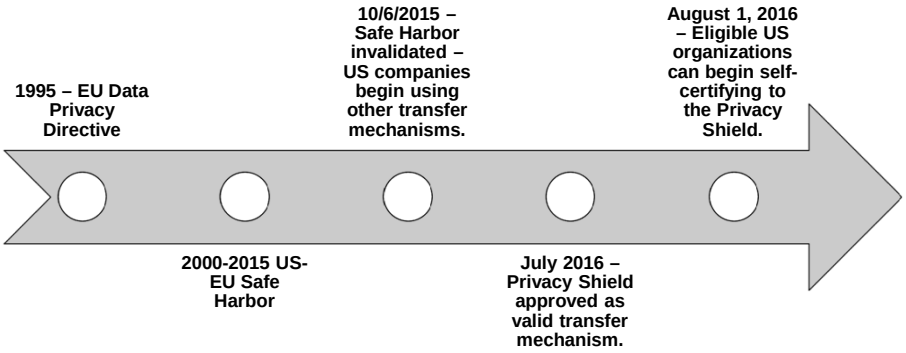
Norbert Kugele & Ken Coleman

What We'll Cover Today

- Overview of Privacy Shield and how it differs from the Safe Harbor.
- Requirements for certification.
- Potential impact of the EU's General Data Privacy Regulations in 2018.
- Is certifying under Privacy Shield worth it?

Overview

Background



Common Privacy Principles

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement, and Liability

Privacy Shield Supplemental Principles

1. Sensitive Data
2. Journalistic Exceptions
3. Secondary Liability
4. Performing Due Diligence and Conducting Audits
5. The Role of the Data Protection Authorities
6. **Self-Certification**
7. **Verification**
8. Access
9. Human Resources Data
10. **Obligatory Contracts for Onward Transfers**
11. **Dispute Resolution and Enforcement**
12. Choice – Timing of Opt Out
13. Travel Information
14. Pharmaceutical and Medical Products
15. Public Records and Publicly Available Information
16. Access Requests by Public Authorities

Privacy Shield vs. Safe Harbor

- Privacy Shield:
  - Provides additional rights for EU individuals.
    - Binding arbitration
    - Independent recourse mechanism
    - Required organization response times
  - Increases compliance monitoring.
  - Adds obligations for transferring data to third parties.
  - Increases potential liability for unauthorized processing by agent of organization.
  - Adds limitations on government access to personal data.

Steps to Self-Certification under Privacy Shield

Confirm Eligibility

- Must be a U.S. organization, and
- Both your organization and the processing itself must be subject to the jurisdiction of:
  - Federal Trade Commission, or
  - Department of Transportation.

Select Independent Recourse Mechanism

- Must have complaint resolution process.
  - Must respond to complaints within 45 days.
- Independent resolution of complaints at no cost to individuals:
  - Private sector dispute resolution program; or
  - Cooperation with the EU DPAs.**
- Right to obligatory binding arbitration.

cooperation with EU DPAs mandatory for ***human resources data* (personal information about employees, past or present, collected in the context of the employment relationship).

Develop Privacy Policy Statement

- Types of personal data collected
- Purposes for collection and use
- How to contact the organization with inquiries or complaints
- If disclose personal information to third parties:
  - Type or identify of the third parties
  - Purposes for which the information is disclosed
- Individuals' rights to access their personal data
- Individuals' ability to limit uses and disclosures
- Which agency has enforcement authority

Develop Privacy Policy Statement

- Adherence to Privacy Shield Principles.
- Link to the Privacy Shield website. (https://www.privacyshield.gov).
- Identify and link to Independent recourse mechanism.

Develop Privacy Policy Statement

- At time of certification:
  - Provide address where policy is available for public viewing.
    - Web address or, if you don't have a public website, a physical address
    - If more than one policy (e.g. HR, non-HR), then location of each policy
- Privacy Policy must be effective prior to self-certification.

Put Verification Mechanism in Place

- Must annually verify adherence to privacy practices
  - Self assessment ;or
  - Outside compliance reviews
- Records relating to implementation must be available in response to:
  - Recourse mechanism authority
  - FTC/DOT
  - Department of Commerce

Designate a Contact

- Contact can be:
  - Corporate officer who certifies compliance with Privacy Shield
  - Chief privacy officer
  - Other official
- Responsible for:
  - Questions
  - Complaints
  - Access requests
  - Any other issues arising under the Privacy Shield
- Must respond within 45 days or receiving complaint.

Submit Self-Certification

- List of required information available at:
  - https://www.privacyshield.gov/article?id=Self-Certification-Information
- Self-certify at:
  - https://www.privacyshield.gov/PrivacyShield/ApplyNow
- Compliant privacy policy, independent recourse mechanism, and verification mechanism all must be effective prior to self-certification.

Effects of Certification

- Consequences:
  - Cross-border transfers permitted immediately.
  - Immediately subject to enforceability
- Existing contracts with third parties receiving personal information:
  - If self-certify by September 30, 2016, have 9 months to modify existing agreements
  - If self-certify after September 30, 2016: existing contracts must be in compliance when self-certify.

Other Implications of Certification

- Certifying organizations must re-certify on an annual basis.
- Continuing obligations of compliance even if the organization subsequently chooses to leave the Privacy Shield.
- Mergers and acquisitions:
  - Notification requirements with Dep't of Commerce
  - Will EU personal information need to be deleted?

Potential Impact EU's General Data Privacy Regulations

EU General Data Privacy Regulations

- Take effect in 2018
- Impose significantly tougher standards on EU personal data, including:
  - Privacy by design requirements
  - Stricter consent requirements (when consent is required)
  - Detailed security requirements for processors
  - Appointment of Data Protection Officer
  - Extraterritorial application

International Transfers under GDPR

- Privacy Shield should still be a recognized mechanism for cross-border transfers under GDPR
- But will Privacy Shield requirements become more onerous?
  - Privacy Shield now subject to annual evaluation.
  - Expect Privacy Shield requirements to change
- Unknowns:
  - How will new requirements apply to certified organizations?
  - What happens if withdraw certification but retain EU personal data?

Is Certification Worth It?

Benefits to Participation

- At this time, all Member States of EU are bound by the European Commission's finding of "adequacy."
- Participants deemed to provide "adequate" privacy protection.

But...

Will it last?

- Annual reassessment could lead to revocation or significant changes.
- Potential court challenges
  - Some DPAs are already questioning certain provisions of Privacy Shield.
  - Individual challenges (e.g., Schremms)

Other Options

- Standard Contractual Clauses
  - Already being used by many companies due to invalidation of Safe Harbor.
  - Currently the subject of another legal attack in the EU Court of Justice.
- Binding Corporate Rules
  - Used primarily by very large corporations
  - Expensive, time consuming process
- Consent of individuals
  - Often impractical

Privacy Shield vs. Contractual Clauses

- For non-HR data, can have an industry-specific recourse mechanism in U.S.
  - SCCs subject you to EU jurisdiction.
- Contracting provisions with processors less onerous under Privacy Shield.
  - But Privacy Shield requires annual verification
- Privacy Shield more streamlined process--new uses do not necessarily require new contract.

Privacy Shield vs. Contractual Clauses

- SCC arrangements subject to less oversight by regulators.
  - Privacy Shield gives rise to prospect of posting on Dep't of Commerce's wall of shame.
- Privacy Shield complaint handling and redress requirements more onerous
- Privacy Shield compliance review likely to be invoked more often than SCC audit rights.

Final Considerations

- Groundwork might not be lost even if you choose later to leave Privacy Shield.
- May help drive engagement by top management if a corporate officer every year has to sign a verification about compliance.

Questions & Answers

Thank you!

Norbert Kugele
nkugele@wnj.com
616.752.2186

Ken Coleman
kcoleman@wnj.com
616.752.2708