EU-U.S. Privacy Shield: Open for Business

August 2, 2016

Kelly DeMarchis
Mike Signorelli
Venable LLP

Today's Webinar Will Cover

- EU-U.S. Privacy Shield background
- Changes in the finalized text of the Privacy Shield
- Self-Certification through the Department of Commerce
- What's on the Horizon

EU-U.S. Privacy Shield— What is it?

- Agreement replacing the U.S.-EU Safe Harbor invalidated by ECJ in Oct. 2015
- Draft Text was released on Feb. 29, 2016.
- Revised further in response to criticisms from Art. 29 WP and EDPS
- Approved on July 12, 2016

Changes in the finalized text of the Privacy Shield

The Privacy Shield Framework now addresses the issues that the DPAs themselves prioritized:

- bulk collection
  - *Written assurances re: mass surveillance of EU data*
- the independence of the Ombudsperson
  - *Add'l assurance from Sec. Kerry*
- the addition of an explicit data retention principle
  - *Data to be retained only for as long as it serves the purpose(s) for which it was initially collected or subsequently authorized*

Steps to Join Privacy Shield

EU-U.S. DOC Privacy Shield Framework Cost Recovery Program

Organization's Annual Revenue	Annual Fee
$0 to $5 million	$250
Over $5 million to $25 million	$650
Over $25 million to $500 million	$1,000
Over $500 million to $5 billion	$2,500
Over $5 billion	$3,250

1. **U.S. Dept. of Commerce began accepting certifications on Aug. 1st –** *annual fee will be based on sliding scale on company revenue published in Federal Register*: https://www.federalregister.gov/articles/2016/07/22/2016-17508/cost-recovery-fee-schedule-for-the-eu-us-privacy-shield-framework
2. **Review 7 Privacy Shield Principles, 16 Supplemental Principles and accompanying letters from ITA, FTC & DOT: https://www.commerce.gov/privacyshield to develop compliant privacy notice and incorporate into practices.** ***You must post new policy statement immediately prior to self-certifying to DOC's Shield framework.***
3. **Review & look towards updating contract language with 3rd parties.**
4. **For companies that join Shield within first 2 months of enactment, you will have 9-month grace period to get new contracts updated.**
5. **Companies must register with independent recourse mechanism prior to self-certifying with U.S. Dept. of Commerce.**

Shield Privacy Principles

1) **Notice**;
2) **Choice**;
3) **Security**;
4) Accountability for **onward transfer**;
5) **Data integrity** and purpose limitation;
6) **Access**; and
7) Recourse, **enforcement** and liability

Privacy Principles – Notice and Choice

Privacy Principles	Safe Harbor	Shield
Notice	To disclose that an organization adheres to principles/framework and states what information collection, sharing, access, opt-out, enforcement and security measures are in-place.	**New:** • Requires links to DOC Shield participant list and dispute provider website; • Disclose new ability for individuals to pursue binding arbitration if other mechanisms fail; • Disclose that may share PI with lawful requests or for national security; and liability in onward transfers to third parties.
Choice	Provide consumers with the opportunity to opt-out or opt-in (sensitive information) depending on the nature of the data. Set-up appropriate procedures to respect consumers' opt-out/opt-in requests particularly with respect to consumers' requests to not be approached for direct marketing (i.e., in-house suppression system.) Opting-out should not require consumers to incur any fee or expense beyond a first-class stamp or phone call. Opt-in for sensitive information: medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.	Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice. An organization must offer individuals the opportunity to choose to (opt out) whether their PI is to be disclosed to a third party or to be used for a materially different purpose. Choice is not required when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of organization. However, an organization shall always enter into a contract with the agent. Definition of sensitive information is same as safe harbor.

What Should be Included in a Privacy Shield Notice?

Statement of adherence to the Shield and its principles.

Link to DOC Privacy Shield participant list: https://www.privacyshield.gov/list

Types of personal data collected and where applicable, the entities or subsidiaries of the organization also adhering to the Principles.

Purpose and use of data collection.

Type or identity of third parties to whom you disclose/share personal information, and the purposes for which you do so.

Right of individuals to access their personal data.

Choices and means the organization offers individuals for limiting the use and disclosure of their personal data.

Company contact information, for inquiries or complaints.

Link to independent dispute resolution provider designated to address complaints:

1. Link to the panel established by DPAs; OR
2. An alternative dispute resolution provider based in EU.

Possibility, under certain circumstances, for individuals to invoke binding arbitration (*For instance if consumer is unable to resolve complaint directly through company or American/EU dispute provider*.) DOC has 6 months to establish Binding Arbitration Panel – *separate company fee not included in DOC self-certification fee*.

Being subject to the investigatory & enforcement powers of FTC, DOT or other US authorized statutory body.

Requirement to disclose personal information in response to lawful requests or to meet national security requirements, and your organization's liability in cases of onward transfers to third parties. You may also include information about the new Ombudsperson for consumers with national security concerns.

Privacy Principles – Onward Transfer & Security

Privacy Principles	Safe Harbor	Shield
Accountability For **Onward Transfer**	Determine the need for contracts with respect to the transfer of information to third parties. You must ensure that if information is disclosed to agents or subcontractors that they will agree to abide by the safe harbor principles. You should only transfer data to third parties consistent with the notice and choices you have given the consumers. Any agents of yours who handle or process your data, such as your service bureaus, must themselves either be subject to the EU Directive or be members of the safe harbor, or they must agree in writing to be bound by these principles. In all events, you must document your agreement with them as to their treatment of data.	• Same overall themes but participating company now has **liability in cases of onward transfer of data to third parties.** • Agent is obligated to provide at least the same level of privacy protection as is required by the Principles. • Upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing. • Additionally, upon request by DOC, must provide a summary or a copy of relevant contract privacy provisions entered into with its agent.
Security	Organization must take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction.	Same.

Third party contracts – new requirements

- Third party acting as a controller:
  - Notice & Choice Principles
  - Data processed for limited and specified purposes consistent with individual consent
  - Recipient will provide same level of protection as the Principles and will notify if they cannot → cease processing or take other steps to remediate

- Third party acting as an agent:
  - Transfer only for limited and specified purposes
  - Ascertain that agent is obligated to provide at least same level of privacy protection as required
  - Take reasonable and appropriate steps to ensure that data is processed in accordance with Principles
  - Notify if obligations cannot be followed→ steps to cease processing or remediate
  - Provide a summary of representative copy of the relevant privacy provisions to DOC upon request

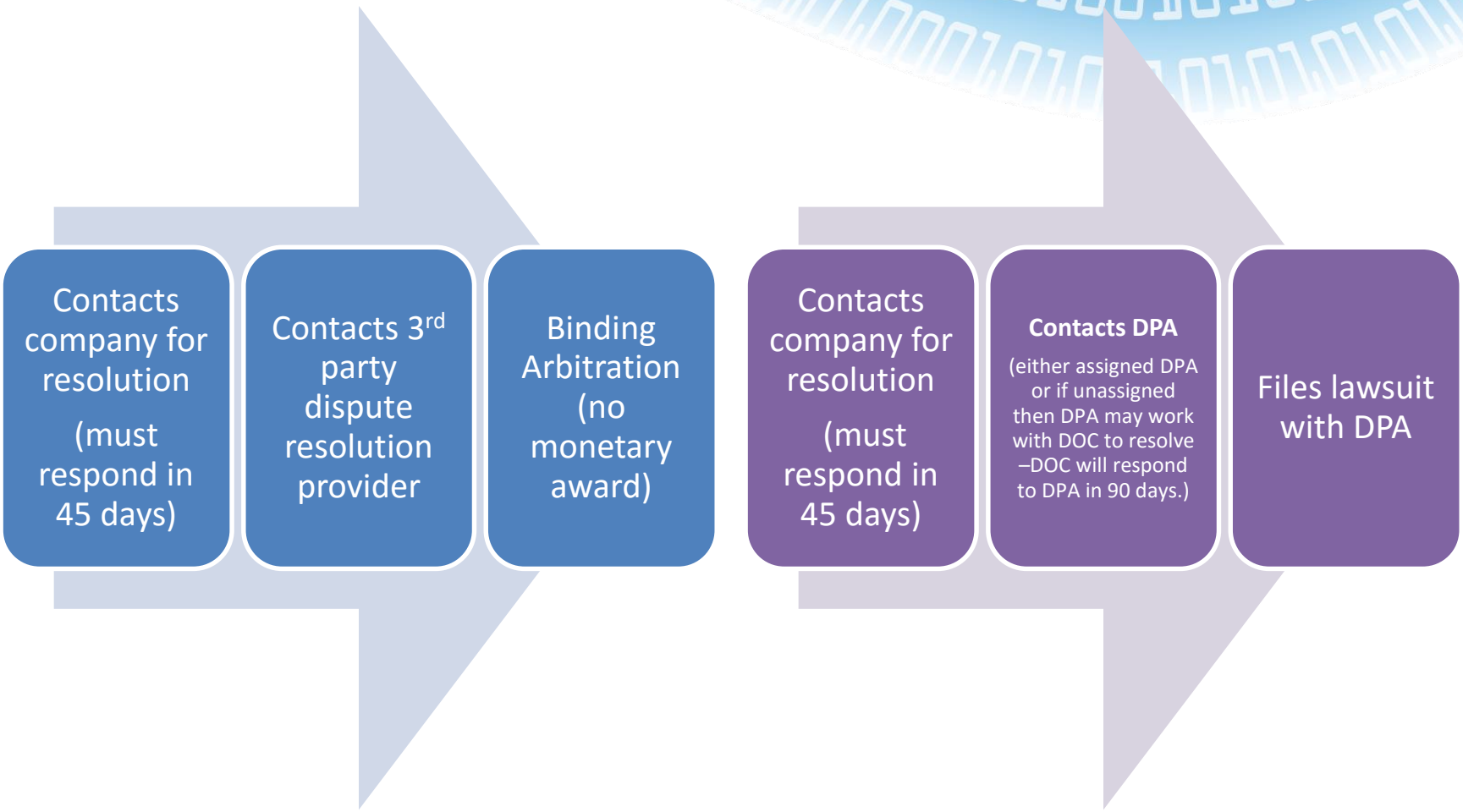
Privacy Principles – Data Integrity & Access

Privacy Principles	Safe Harbor	Shield
Data Integrity And Purpose Limitation	Ensure that the customer's personal information is reliable, accurate, complete, current and used for intended purposes. Your company should not process data that are not relevant to the purpose for which they were collected, unless subsequently authorized by the consumer.	Same. Additional: The organization must adhere to the Principles as long as it retains the data. **Organizations can retain data as long as it serves a purpose for processing consistent with purpose stated at time of collection.** This does not prevent organizations from processing personal information for longer periods if reasonably serves the purpose of archiving in the public interest, journalism, literature, art, scientific or historical research and statistical analysis.
Access	You must provide customers the ability to access PI being maintained by the company and the ability to correct, amend or delete it where it is inaccurate or processed in violation of the Principles (based on a sliding scale principle – the obligation to provide access to information increases where its use is more likely to significantly affect the individual).	Same.

Privacy Principles – Enforcement

Privacy Principles	Safe Harbor	Shield
Recourse, **Enforcement** and Liability	Take reasonable steps to ensure that any consumer privacy concern will be addressed by: (1) referring consumers to your customer service department or other in-house dispute resolution program; (2) subscribing to a third-party dispute resolution mechanism to address any unresolved in-house consumer data privacy complaints; and (3) having appropriate monitoring, verification and remedy procedures in place.	The independent dispute resolution service should be readily available and **at no cost to consumer**. New available remedy for EU individuals is **binding arbitration** – individuals must pursue other mechanisms first such as contacting: 1) company directly; 2) independent dispute provider; and 3) then may pursue binding arbitration. No monetary damages allowed under binding arbitration. Binding arbitration seeks to resolve an individual complaint. A separate complaint process – consumers may also contact appropriate DPA and then DPA resolves complaint or works with DOC to resolve complaint. No binding arbitration under this scenario.

EU Resident Files Complaint Under Shield



Privacy Shield Self-Certification Checklist

Initial Steps:

- ✓ Assess your company's practices against the Principles; make changes as needed
- ✓ Designate an accountable executive
- ✓ Designate a point of contact
- ✓ Engage an independent dispute resolution provider
- ✓ Implement an annual assessment Program
- ✓ Privacy Shield employee training

Privacy Shield Self-Certification Checklist

To Self-Certify:

- ✓ Update your organization's privacy policy to reflect the Privacy Shield principles, and to state adherence to the Privacy Shield
- ✓ Submit Online Self-Certification:
  - ✓ Contact information
  - ✓ Description of activities that involve PI from EU
  - ✓ Description of organization's privacy policy for PI from EU
  - ✓ Human resources information?
- ✓ Pay fee
- ✓ Annually recertify

What's Next?

- Program up for annual joint review ~ May 2017; Art. 29 WP will not challenge prior to that time.
- GDPR on horizon in May 2018—Privacy Shield will have to become compliant with GDPR requirements
- Brexit!

Thank You

Kelly A. DeMarchis | Venable LLP
KADeMarchis@Venable.com

Mike Signorelli | Venable LLP
MASignorelli@Venable.com