WELCOME & INTRODUCTIONS

Presenters

Caitlin Fennessy, CIPP/US, Senior Policy Advisor, Data Flows and Privacy Team, International Trade Administration, U.S. Department of Commerce

Allison Brody, CIPP/E, CIPP/US, Deputy Counsel, Privacy, RELX Group

Frances Henderson, CIPP/US, VP and National Director, Privacy Initiatives, Council of Better Business Bureaus
EU-U.S. PRIVACY SHIELD FRAMEWORK

1. Understanding the Privacy Shield Framework
   - Components of the Framework
   - Key elements on which interested participants should focus
   - Program administration - what’s new that matters to you

2. Industry insight into certification logistics
   - Pre-certification Logistics
   - Certification
   - Post-certification Logistics

3. Role of Independent Recourse Mechanisms
   - Types of IRMs
   - How to work with your IRM throughout the certification process
Understanding the Privacy Shield Framework
What does the Privacy Shield contain?

**Privacy Shield Principles**
- Requirements to which U.S.-based organizations can make an enforceable commitment to receive data in compliance with EU data protection laws

**Letters Describing Oversight and Enforcement from:**
- Secretary of Commerce and Under Secretary for International Trade
- Chairwoman of the Federal Trade Commission
- Secretary of Transportation

**Government Access to Data**
- Letter from the Secretary of State on the new Privacy Shield Ombudsperson
- Letter concerning safeguards and limitations from the Office of the Director of National Intelligence
- Letter concerning safeguards and limitations from the Department of Justice
UNDERSTANDING THE PRIVACY SHIELD FRAMEWORK

What should your company focus on to come into compliance?

What’s new compared to Safe Harbor

1. New Privacy Protections

- Notice requirements
- Accountability for onward transfer
- Purpose limitation and data retention

Note: Companies should review the Framework in its entirety. These slides are only meant to highlight certain aspects.
UNDERSTANDING THE PRIVACY SHIELD FRAMEWORK

What should your company focus on to come into compliance?

What’s new compared to Safe Harbor

2. Enhanced Complaint Resolution

- Response time to EU individuals
- Free dispute resolution
- Binding arbitration as last-resort option
UNDERSTANDING THE PRIVACY SHIELD FRAMEWORK

What should your company focus on to come into compliance?

What’s new compared to Safe Harbor

3. Improved Cooperation and Transparency

- Monitoring and dispute resolution requires cooperation with ITA Privacy Shield Team
- Ongoing requirements (if withdraw and maintain data)
- Publication of FTC compliance reports (if subject to enforcement action)
Joining the Privacy Shield Program
JOINING THE PRIVACY SHIELD PROGRAM

How will a company join Privacy Shield?

1. Confirm Your Organization’s Eligibility to Participate
2. Develop a Compliant Privacy Policy
3. Establish an Independent Recourse Mechanism (IRM)
4. Ensure a Verification Mechanism is in place
5. Identify your Privacy Shield Point of Contact
6. Self-certify Using the Privacy Shield Website
7. Reaffirm Self-certification Annually
8. Reply to Inquiries from EU citizens, IRM, Commerce, and/or DPAs as Required
JOINING THE PRIVACY SHIELD PROGRAM

ITA Administration: What’s new that matters to you?

- Maintenance of the Privacy Shield Website
- Verification of Self-Certification Requirements
- Monitoring of Compliance
- Facilitating Resolution of Complaints Referred by EU DPAs
RESOURCES

- Visit [www.privacyshield.gov](http://www.privacyshield.gov) for additional information, including answers to FAQs, a Guide to Self-Certification, and a fact sheet outlining key new requirements for participating organizations.

- We look forward to your organization’s certification.
Considerations for Certification
CONSIDERATIONS FOR CERTIFICATION: PROS

1) Convenient transfer mechanism that reduces paperwork, negotiation time and effort, and alternative commercial proposals with customers

2) Despite criticism, Privacy Shield is stronger and may be perceived as a kind of ‘privacy seal’ that provides a competitive advantage and/or serves as a prerequisite for doing EEA business

3) Covers EU-Processor-to-US-Subprocessor data transfers for which no official model clauses exist

4) For Safe Harbor-certified organizations: Changes under Privacy Shield should not present significant operational impact

5) For “B2B” organizations: Keeping scope of certification limited to personal data received from your EU business customers limits scope of verification assessments and supplier contracts involved in “Onward Transfer”
   • Acting solely as processor (i.e. only on instructions from controller) and not controller limits scope too
CONSIDERATIONS FOR CERTIFICATION: CONS

1) Subject to wider array of enforcement authorities and avenues of redress

2) Legal challenges to Privacy Shield are expected, which may cause unease with customers, which may insist on alternatives anyway

3) Relevant contracts need to be identified and may need update/amendment:
   - Supplier (“agent”) contracts to meet “Onward Transfer” requirements
   - Customer contracts to restrict/condition transfer of any “sensitive information”

4) Costs (outside counsel, consultants, internal resources’ time and effort) to assess and confirm revised language in certification, notice, customer contracts and supplier contracts satisfies requirements and any applicable exemptions

5) To take advantage of 9-month grace period to update supplier contracts, certifications must be submitted by September 30, 2016, so little time to ‘wait and see’
Pre-Certification Logistics
PRE-CERTIFICATION LOGISTICS: WHAT TO CERTIFY

Identify:

✓ Which organization(s) to certify
  ▪ Determine the entities that “receive” personal data either directly or indirectly from EEA
    ▪ Narrowly specify divisions or businesses based on product/service, if appropriate

✓ Which personal data to certify
  ▪ Determine which kinds of personal data to include in scope
    ▪ Non-HR data (customer data, client data, visitor data, clinical trial data, etc.)
    ▪ HR data (personal data about employees, past and present)
PRE-CERTIFICATION LOGISTICS: WHO DOES WHAT

Identify who will:

✓ Serve as internal point of contact in each business/group to validate data flows
✓ Handle access requests, questions, complaints and any other Privacy Shield issues
✓ Conduct staff training
✓ Handle certification renewals and updates
✓ Serve as independent recourse mechanism (a/k/a ADR provider)
✓ Verify compliance
  ▪ Either in-house self-assessment or outside/third-party compliance review
✓ Certify compliance
  ▪ Either in-house or outside/third-party letter of attestation
## PRE-CERTIFICATION LOGISTICS: NOTICE

**Draft/update and verify:**
- Privacy Shield Notice

### Privacy Shield

- Statement of participation
- Commitment to adhere to Principles
- Link to Privacy Shield List

### Rights and remedies

- Rights of access and choice
- Any EU establishment to deal with queries
- Recourse: DPA panel; ADR provider; link to ADR provider site or complaint form; arbitration as last resort
- Role of FTC (or other) enforcement body

### Data processing

- Types of personal data processed
- Group companies relying on the Shield
- Websites on which notice will be posted
- Third parties: What types and why?
- Statement of liability for onward transfer
- Disclosure to meet national security, law enforcement requirements

- For HR Data: Notice need **not** be public; corporate intranet OK
PRE-CERTIFICATION LOGISTICS: POLICIES

Draft/update and verify:

✓ Internal compliance policies and procedures
  ▪ Explain how Privacy Shield Principles are implemented, including:
    ▪ Data integrity and retention policy and procedures
    ▪ Access and correction policy and procedures
    ▪ Complaint handling and escalation policy and procedures
    ▪ Security policies and procedures
      ▪ Cross-reference existing policies, standards and controls as appropriate

✓ Internal compliance training
  ▪ Explain requirements and operating procedures to relevant staff
    ▪ Stand-alone presentation deck or computer-based training (CBT); or
    ▪ Add-on, supplemental training module to existing CBT
Certification
CERTIFICATION

Submit:

✓ Organization name
✓ Organization mailing address, contact and corporate officer
✓ Organization’s annual revenue (to determine fee)
✓ Organization’s number of employees (range), industry, industry sector [optional]
✓ Organization’s affiliates also adhering to Privacy Shield (“covered entities”)
✓ Description of personal data received from the EU, including types of personal data, purposes of processing, and types of third parties, if any, subprocessing the data
✓ Verification method (self-assessment or outside compliance review)
✓ Details about organization’s Privacy Shield Notice, including URL and effective date
✓ Independent recourse mechanism
✓ Payment
Post-Certification Logistics
POST-CERTIFICATION

Draft/update:

✓ References to Privacy Shield adherence in any separate website privacy policies, e.g.:

[Name] [participates in -or- has certified to -or- has certified certain of its services under] the EU-U.S. Privacy Shield framework as set forth by the U.S. Department of Commerce. Please view [Name’s] Privacy Shield Notice here. To learn more about the Privacy Shield program, and view [Name]’s certification, please visit www.privacyshield.gov.

• ADR provider may require specific text
• Display any statements about U.S.-Swiss Safe Harbor, APEC CBPR, etc. separately

Identify, review and update contracts:

✓ Customers: Sensitive information
✓ Suppliers: Onward transfers (9 months to complete, if certify by September 30, 2016)

Annual renewal and updates:

✓ Docket the annual renewal deadline
✓ Keep registrations, notices, policies, trainings up to date
Role of Independent Recourse Mechanisms (ADR Providers)
ROLE OF THE IRM/ADR PROVIDER

- All participants must register with an IRM before self-certification
- May select the EU DPAs or a US-based ADR provider
  - For HR data must use the EU DPAs
  - Many companies use both
- IRMs must:
  - Provide Privacy Shield ADR services free of charge to EU individuals;
  - Inform EU individuals about complaint handling process
  - Respond to regulatory inquiries, publish annual reports
TYPES OF IRM

• Arbitration Services (JAMS, AAA)
  - Available binding arbitration

• Privacy Seal providers (Truste, Verasafe)
  - Assessment, verification assistance, ADR services

• Self-regulatory ADR providers (BBB, DMA, CASRO)
  - ADR services, certification assistance, ongoing compliance support, online resources
TYPES OF IRM: BBB EU PRIVACY SHIELD

• Better Business Bureau: national non-profit organization operates self-regulatory programs for US businesses, with a focus on SMEs

• Offers ADR and compliance support - online resources at www.bbb.org/EU-privacy-shield

• Complaints handled using conciliation, independent arbitration (Data Privacy Review)

• Participants agree to comply with decisions, have noncompliance published, reported to FTC & Commerce
WORKING WITH YOUR IRM: PRE-CERTIFICATION

- Third party review before certification
- Identify all entities and websites to be covered by Privacy Shield policy (and IRM contract)
- 13 privacy policy requirements
- Ensure IRM registration and Commerce certification use the same corporate identity
- Assessment and Verification options: with the IRM, in-house, with attorney or consultant assistance
WORKING WITH YOUR IRM: PRIVACY POLICY TIPS

• 13 requirements: focus on actual data collection, use and sharing, choice and access mechanisms, mandated disclosures—read the Notice Principle!

• Note all entities and websites where policy is posted

• Understand and note your accountability for onward transfer, contract requirements

• Swiss Safe Harbor - can include but address separately
  - Note differences in Principles, onward transfer rules

• Include live links to online ADR mechanism(s)
WORKING WITH YOUR IRM: POST-CERTIFICATION

- IRMs can help you stay in compliance by:
  - ✓ sending recertification reminders
  - ✓ monitoring privacy policy and certification status periodically and before recertification
  - ✓ conducting continuous monitoring to support verification
  - ✓ updating your self-certification information

  ... as well as handling privacy complaints
WORKING WITH YOUR IRM: COMPLAINT HANDLING

- Privacy Shield provides multiple redress mechanisms for EU individuals
  - Participating company (45 days)
  - ADR process
  - DPAs/Commerce
  - FTC
  - Privacy Shield Panel binding arbitration
WORKING WITH YOURIRM: COMPLAINT HANDLING

• Privacy Shield is the only EU-US data transfer mechanism mandating ADR with regulatory oversight
• Privacy complaints and inquiries can help identify compliance gaps in privacy or security practices
• Accessible, customer-focused, responsive complaint handling builds trust
• Managing complaints effectively with your IRM can avoid escalation through other channels
• IRMs must respond to DPA and US regulatory inquiries; notify FTC, DOC of noncompliance with ADR decisions
Thank you!

Allison Brody, CIPP/E, CIPP/US
Deputy Counsel, Privacy
RELX Group

Caitlin Fennessy, CIPP/US
Policy Advisor, Data Flows and Privacy Team
International Trade Administration
U.S. Department of Commerce

Frances Henderson, CIPP/US
VP and National Director, Privacy Initiatives
Council of Better Business Bureaus
HOW DID THINGS GO?
(WE REALLY WANT TO KNOW!)

Did you enjoy this session? Is there anyway we could make it better? Let us know by filling out a speaker evaluation.

• Start by opening the IAPP Events App.

• Select this session and tap “Click the following link for speaker evaluations.”

• Once you’ve answered all three questions, tap “Done” and you’re all set.

• Thank you!