Fact Sheet
Overview of the EU-U.S. Privacy Shield Framework
For Interested Participants
July 12, 2016

The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

The Privacy Shield Framework provides a set of robust and enforceable protections for the personal data of EU individuals. The Framework provides transparency regarding how participating companies use personal data, strong U.S. government oversight, and increased cooperation with EU data protection authorities (DPAs).

The European Commission deemed the Privacy Shield Framework adequate to enable data transfers under EU law. Commerce will allow companies time to review the Framework and update their compliance programs and then, on August 1, will begin accepting certifications.

To join the Privacy Shield Framework, a U.S.-based company will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield Framework will be voluntary, once an eligible company makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. All companies interested in joining the Privacy Shield Framework should review its requirements in their entirety. To assist in that effort, key new requirements for participating companies are outlined here.

EU-U.S. Privacy Shield Framework
Key New Requirements for Participating Companies

Informing individuals about data processing

- A Privacy Shield participant must include in its privacy policy a declaration of the organization's commitment to comply with the Privacy Shield Principles, so that the commitment becomes enforceable under U.S. law.
- When a participant's privacy policy is available online, it must include a link to the Department of Commerce's Privacy Shield website and a link to the website or complaint submission form of the independent recourse mechanisms that is available to investigate individual complaints.
- A participant must inform individuals of their rights to access their personal data, the requirement to disclose personal information in response to lawful request by public authorities, which enforcement authority has jurisdiction over the organization's compliance with the Framework, and the organization's liability in cases of onward transfer of data to third parties.

Providing free and accessible dispute resolution

- Individuals may bring a complaint directly to a Privacy Shield participant, and the participant must respond to the individual within 45 days.
- Privacy Shield participants must provide, at no cost to the individual, an independent recourse mechanism by which each individual's complaints and disputes can be investigated and expeditiously resolved.
- If an individual submits a complaint to a data protection authority (DPA) in the EU, the Department of Commerce has committed to receive, review and undertake best efforts to facilitate resolution of the complaint and to respond to the DPA within 90 days.
- Privacy Shield participants must also commit to binding arbitration at the request of the individual to address any complaint that has not been resolved by other recourse and enforcement mechanisms.

Cooperating with the Department of Commerce

- Privacy Shield participants must respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield Framework.

Maintaining data integrity and purpose limitation

- Privacy Shield participants must limit personal information to the information relevant for the purposes of processing.
- Privacy Shield participants must comply with the new data retention principle.

Ensuring accountability for data transferred to third parties

- To transfer personal information to a third party acting as a controller, a Privacy Shield participant must:
    - Comply with the Notice and Choice Principles; and
    - Enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
- To transfer personal data to a third party acting as an agent, a Privacy Shield participant must:
    - Transfer such data only for limited and specified purposes;
    - Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles;

- Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles;
- require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles;
- Upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and
- Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

Transparency related to enforcement actions

- Privacy Shield participants must make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC if the organization becomes subject to an FTC or court order based on non-compliance.

Ensuring commitments are kept as long as data is held

- If an organization leaves the Privacy Shield Framework, it must annually certify its commitment to apply the Principles to information received under the Privacy Shield Framework if it chooses to keep such data or provide "adequate" protection for the information by another authorized means.