Fact Sheet
Overview of the EU-U.S. Privacy Shield Framework

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 Privacy Shield Framework offers EU individuals access to multiple avenues to address any concerns regarding participants' compliance with the Framework, including free dispute resolution. The Framework ensures a continuing level of protection consistent with Privacy Shield Principles when personal data collected under the Framework is transferred to third parties. The Framework also makes it easier for EU individuals to understand and exercise their rights.

The European Commission has proposed that the Privacy Shield Framework be deemed adequate to enable data transfers under EU law, a proposal that is now in the approval process. Once an adequacy determination is in place, the Department of Commerce will begin accepting certifications under the Framework.

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 elements are outlined here.

EU-U.S. Privacy Shield Framework

EU individuals' rights and legal remedies:

- 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.
- The U.S. Federal Trade Commission (FTC) has committed to work closely with the DPA to provide enforcement assistance, which, in appropriate cases, could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB ACT.
- The FTC has committed to vigorous enforcement of the Privacy Shield Framework. This includes prioritizing referrals from EU Member State DPAs, the Department of Commerce, privacy self-regulatory bodies, and independent recourse mechanisms. To better enable handling of EU DPA referrals, the FTC has committed to create a standardized referral process, designate a point of contact at the agency for EU DPA referrals, and exchange information on referrals with referring enforcement authorities, subject to confidentiality laws and restrictions.
- EU individuals are able to pursue legal remedies through private causes of action in U.S. state courts, including private causes of action for misrepresentation and similar types of claims.
- 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.

Program oversight and cooperation with EU DPAs:

- The Department of Commerce has committed to robust administration and supervision of the Privacy Shield Framework, including to:
    - Verify prior to finalizing a company's self-certification that the company has provided all required information and registered with the identified independent recourse mechanism, in instances where the provider requires registration;
    - Follow up with organizations whose self-certifications lapse or who have voluntarily withdrawn from the Privacy Shield Framework to verify whether the organization will return, delete or continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield Framework;
    - Search for and address false claims of participation and where appropriate refer matters to the FTC, Department of Transportation or other appropriate enforcement agency; and
    - Conduct periodic ex officio compliance reviews and assessments of the program.
- The Department of Commerce has committed to increase cooperation with EU DPAs, including to:
    - Establish a dedicated point of contact at the Department to act as a liaison with DPAs and receive and undertake best efforts to facilitate resolution of complaints referred;
    - Assist DPAs seeking information related to specific organization's participation in the program or implementation of specific Privacy Shield requirements; and
    - Provide DPAs with material regarding the Privacy Shield Framework for inclusion on their own websites to increase transparency for EU citizens and EU businesses.

- The FTC has committed to increase cooperation with EU DPAs, including to:
    - Establish a dedicated point of contact at the FTC and standardized process through which EU DPAs can refer complaints;
    - Exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions; and
    - Work closely with EU DPAs to provide enforcement assistance.
- The Department of Commerce, the FTC and other agencies as appropriate will hold annual meetings with the Commission, interested DPAs and appropriate representatives from the Article 29 Working Party, where the Department will discuss current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield Framework.

Key new requirements for participating companies:

<u>Informing individuals about data processing</u>

- 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.

Maintaining data integrity and purpose limitation

- Privacy Shield participants must limit personal information to the information relevant for the purposes of processing.

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
    - 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.
- 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;
    - 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.

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.

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.

Demonstration of limitations and safeguards on national security and law enforcement access to data:

- In connection with finalization of the new Privacy Shield Framework, the U.S. Intelligence Community has laid out in writing to the European Commission the multiple layers of constitutional, statutory, and policy safeguards that apply to its operations, with active oversight provided by all three branches of the U.S. Government.

- The Department of Justice has provided an overview regarding limits on U.S. Government access to commercial data and other record information held by corporations in the United States for law enforcement and public interest purposes.

- The Privacy Shield Framework provides, for the first time, a specific channel for EU individuals to raise questions regarding signals intelligence activities. The Department of State has committed to establish a new Ombudsperson through whom European Union individuals will be able to submit inquiries regarding the United States' signals intelligence practices. As a part of this process, the United States is making the commitment to respond to appropriate requests regarding these matters, consistent with our national security obligations.