How to Join Privacy Shield

To allow companies time to review the Privacy Shield Framework and update their compliance programs, the Department of Commerce will begin accepting self-certifications to the Privacy Shield on August 1.

The following guide to self-certification is provided to assist companies as they review the Framework and prepare to self-certify. As explained in greater detail in section three below, as part of this process, companies will need to identify an independent dispute resolution provider prior to self-certifying and register with that provider where required. Given this sequencing, private sector dispute resolution providers may enable companies to register through their programs prior to August 1.

Guide to Self-Certification

The decision by a U.S.-based organization to join the Privacy Shield program is entirely voluntary. However, once an eligible organization publicly commits to comply with the Privacy Shield Principles through self-certification, that commitment is enforceable under U.S. law by the relevant enforcement authority, either the U.S. Federal Trade Commission (FTC) or the U.S. Department of Transportation (DOT).

In order to receive Privacy Shield benefits, an organization must self-certify annually to the Department of Commerce that it agrees to adhere to the Privacy Shield Principles, a detailed set of requirements based on privacy principles such as notice, choice, access, and accountability for onward transfer. A brief guide to the self-certification process, including steps that the organization must take prior to self-certification, is provided below. This guide should be read in conjunction with the complete set of Privacy Shield Principles, which includes 16 Supplemental Principles as well as the accompanying letters from the International Trade Administration, FTC and DOT, which provide information regarding the oversight, administration and enforcement of the Framework. Following these steps will help to ensure that your organization is meeting the requirements for self-certification, as set forth in Supplemental Principle 6 (Self-Certification).

1. **Confirm Your Organization's Eligibility to Participate in the Privacy Shield**: Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation

(DOT) may participate in the Privacy Shield. The FTC and DOT have both committed that they will enforce the Privacy Shield Framework.

- Generally, the FTC's jurisdiction covers acts or practices in or affecting commerce by any "person, partnership, or corporation." The FTC does not have jurisdiction over most depository institutions (banks, federal credit unions, and savings & loan institutions), telecommunications and interstate transportation common carrier activities, air carriers, labor associations, most non-profit organizations, and most packer and stockyard activities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances.

- The DOT has exclusive jurisdiction over U.S. and foreign air carriers. The DOT and the FTC share jurisdiction over ticket agents that market air transportation.

- If you are uncertain as to whether your organization falls under the jurisdiction of either the FTC or DOT, then please be sure to contact the Privacy Shield Team at the Department of Commerce for more information.

2. **Develop a Privacy Shield-Compliant Privacy Policy Statement**: Your organization must develop a Privacy Shield-compliant privacy policy before submitting its self-certification to the Department of Commerce.

- *Ensure that Your Organization's Privacy Policy Conforms to the Privacy Shield Principles:* In order to be compliant with the Privacy Shield Framework, the privacy policy must conform to the Privacy Shield Principles. Among other things, the privacy policy should reflect your organization's information handling practices and the choices your organization offers individuals with respect to the use and disclosure of their personal information. It is important to write a policy that is clear, concise, and easy to understand.

- *Make Specific Reference in the Privacy Policy to Your Organization's Privacy Shield Compliance:* Supplemental Principle 6 (Self-Certification) requires each organization that self-certifies to state in its relevant published privacy policy that it adheres to the Privacy Shield Principles. In addition, the privacy policy must include a hyperlink to the Privacy Shield website.

- *Identify in the Privacy Policy Your Organization's Independent Recourse Mechanism (see section 3 below for additional information):* If your organization's privacy policy is available online, it must include a hyperlink to the website of the independent recourse mechanism that is available to investigate unresolved complaints regarding your organization's compliance with the Privacy Shield or to the independent recourse mechanism's complaint submission form.

- *Provide an Accurate Location for Your Organization's Privacy Policy and Make Sure that it is Publicly* Available:* At the time of self-certification, your organization must provide accurate information about the location of its applicable privacy policy. If your organization has a public website, it must provide the web address where the privacy policy is available; if your organization does not have a public website, you must provide an address where the privacy policy is available for viewing by the public. In addition, your organization should verify that its privacy policy is effective prior to self-certification. See Supplemental Principle 7 (Verification).

    * If your organization's self-certification relates to human resources data, then the privacy policy covering such data need only be made available to your organization's employees and as part of the Privacy Shield review process. In such instances, your organization may either (1) provide the public web address where the privacy policy is available or (2) specify where the privacy policy is available for viewing by your affected employees and upload a copy to your organization's Privacy Shield submission so that it may be reviewed by the Department of Commerce's Privacy Shield team. See Supplemental Principle 6(c) (Self-Certification) for more information.

3. **Identify Your Organization's Independent Recourse Mechanism**: Under the Framework's Recourse, Enforcement and Liability Principle, self-certifying organizations must provide an independent recourse mechanism available to investigate unresolved complaints at no cost to the individual. (See Supplemental Principle 11 (Dispute Resolution and Enforcement) for more information regarding dispute resolution under Privacy Shield.)

- Your organization must ensure that its recourse mechanism is in place prior to self-certification and must register with the relevant mechanism prior to self-certification when the mechanism requires registration. In addition, your organization must include in its privacy policy a reference to, as well as relevant contact information for, the independent recourse mechanism, as noted in section 2 above.

- Organizations self-certifying under Privacy Shield may utilize private sector dispute resolution programs as the independent recourse mechanism. Organizations like the Council of Better Business Bureaus (BBB), TRUSTe, the American Arbitration Association (AAA), JAMS, and the Direct Marketing Association (DMA) have developed programs that assist in compliance with the Framework's Recourse, Enforcement and Liability Principle and Supplemental Principle 11 (Dispute Resolution and Enforcement).

- Alternatively, organizations may choose to cooperate and comply with the EU data protection authorities (DPAs) with respect to all types of data. In doing so, an organization must follow the procedures outlined in Supplemental Principle 5 (The Role of the Data Protection Authorities).

- If your organization's self-certification will cover *human resources data* (personal information about employees, past or present, collected in the context of the employment relationship), then your organization must agree to cooperate and comply with the EU DPAs with respect to such data. Additional guidance on the handling of human resources data under the Framework is provided in Supplemental Principle 9 (Human Resources Data).

- Organizations that either choose to or must utilize the EU DPAs are required to pay an annual fee to cover the operating costs of the EU DPA panel.

4. **Ensure that Your Organization's Verification Mechanism is in Place**: As discussed in Supplemental Principle 7 (Verification), organizations self-certifying to the Framework are required to have procedures in place for verifying compliance. To meet this requirement, your organization may use either a self-assessment or an outside/third-party assessment program. For additional guidance on the Framework's verification requirement, please see Supplemental Principle 7.

5. **Designate a Contact within Your Organization Regarding Privacy Shield**: Each organization is required to provide a contact for the handling of questions, complaints, access requests, and any other issues arising under the Privacy Shield. This contact can be either the corporate officer that is certifying your organization's compliance with the Framework, or another official within your organization, such as a Chief Privacy Officer. Under the Privacy Shield, organizations must respond to individuals within 45 days of receiving a complaint.