INTERNATIONAL TRADE ADMINISTRATION

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

What is the Privacy Shield?

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law. On January 12, 2017, the Swiss Government announced the approval of the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States.

Which Organizations Participate in the Privacy Shield?

The authoritative list of Privacy Shield participants is available at www.privacyshield.gov/list. Thousands of organizations are Privacy Shield participants. These organizations span industry sectors and sizes. While many large multinational entities have self-certified, over fifty percent of participants are small and medium-sized companies. Although participants must be based in the United States, U.S. subsidiaries of EU-headquartered companies can and have self-certified.

What are the benefits for organizations that self-certify to the Privacy Shield?

The Privacy Shield provides many important benefits to U.S.-based organizations, as well as their partners in Europe. These include:

- Participating organizations are deemed to provide "adequate" privacy protection, a requirement (subject to limited derogations) for the transfer of personal data outside of the European Union under the EU General Data Protection Regulation (GDPR) and outside of Switzerland under the Swiss Federal Act on Data Protection;
- EU Member State requirements for prior approval of data transfers either are waived or approval will be automatically granted; and
- Compliance requirements are clearly laid out and cost-effective, which should particularly benefit small and medium-sized enterprises.

How can an organization join the Privacy Shield?

The Privacy Shield program is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce. To join the Privacy Shield Framework, a U.S.-based organization is 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 is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment becomes enforceable under U.S. law. See www.privacyshield.gov/Program-Overview for further details and FAQs.

How to Join Privacy Shield:

The following is a brief guide outlining the steps for a successful self-certification process. (For a more detailed version, visit **www.privacyshield.gov/program-overview** and click on "How To Join Privacy Shield")

1. **Confirm Eligibility:** 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 program. Questions about eligibility can be submitted to the Department of Commerce's Privacy Shield team at privacyshield@trade.gov.
2. **Develop a Privacy Shield-Compliant Privacy Policy Statement:**
   - **a.** Your organization must decide whether it will self-certify compliance with EU-U.S., Swiss-U.S., or both Privacy Shield Frameworks and develop its notice(s) accordingly.
   - **b.** Your organization's privacy policy must conform to the Privacy Shield Principles. The list of required elements can be found in the "Notice" Principle.
   - **c.** Privacy policies must include, among other things, a statement of adherence to the EU and/or Swiss Privacy Shield Principles, a hyperlink to the Privacy Shield website, and an identification of your organization's independent recourse mechanism.
   - **d.** A first-time certifier may not claim Privacy Shield participation in its published privacy policy until the Privacy Shield team notifies the organization that its submission is complete.
3. **Identify Your Organization's Independent Recourse Mechanism:**
   - **a.** Your organization must have an independent recourse mechanism in place prior to self-certification.
   - **b.** Organizations may utilize the EU Data Protection Authorities under EU-U.S. Privacy Shield Framework, the Swiss Federal Data Protection and Information Commissioner (FDPIC) under Swiss-U.S. Privacy Shield Framework, or private sector dispute resolution programs.
     - **i.** If its self-certification covers HR data then your organization must agree to cooperate with the EU DPAs or with the Swiss FDPIC under the respective Privacy Shield Frameworks.
     - **ii.** Utilizing the EU DPAs requires an annual payment of US $50. This fee is payable to the United States Council for International Business (USCIB). Payment can be made here: http://privacyshield.uscib.org/
4. **Make the Required Contribution for the Annex I Binding Arbitration Mechanism:** The International Centre for Dispute Resolution-American Arbitration Association (ICDR-AAA) was selected to administer the binding arbitration mechanism described in Annex I of the Framework and manage the arbitral fund. First time certifiers must visit http://go.adr.org/privacyshieldfund.html to make the required contribution.
5. **Ensure Your Verification Mechanism Is In Place:** All self-certifying organizations need procedures in place for verifying compliance with the Framework, either through a self-assessment or through an outside third party.
6. **Designate Two Contacts Within Your Organization:** These contacts are responsible for any issues which may arise under the Privacy Shield Framework.
   - **a.** These contacts must be a Corporate Officer and a general Organization Contact.
   - **b.** The Organization Contact must respond to complaints within 45 days.
7. **Compile Required Information For Certification:**
   - **a.** Prior to self-certifying, your organization should review the Privacy Shield Principles as well as the information required during the self-certification process. The Principles can be found at https://www.privacyshield.gov/EU-US-Framework and information required to self-certify at https://www.privacyshield.gov/article?id=Self-Certification-Information.
8. **Submit Your Self-Certification Application:**
   - **a.** Organizations should go to https://www.privacyshield.gov and click on "Self-Certify".
   - **b.** To self-certify, your organization must create a profile and fill out the online certification form.
   - **c.** There is a self-certification fee based on the annual revenue of your organization. This fee is part of the International Trade Administration's cost recovery program to support the Privacy Shield program.
   - **d.** Organizations must submit the completed application online for review by the Privacy Shield team.
   - **e.** Annual recertification is required to remain in the Privacy Shield program. Your organization may withdraw from the program at any time, but it will retain obligations with respect to the data received under the Framework and would be required to remove references to the Framework in its privacy statement.