INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION® | AMERICAN ARBITRATION ASSOCIATION®

ICDR®/AAA® Program Information for the EU-U.S. and Swiss-U.S. Privacy Shield Programs

The EU–U.S. Privacy Shield program replaces the U.S.–EU Safe Harbor program and the Swiss-U.S. Privacy Shield replaces the U.S.–Swiss Safe Harbor program.

The full text of the EU-U.S. and Swiss-U.S. Privacy Shield programs along with all supplemental documents can be found on the Department of Commerce's website at https://www.privacyshield.gov.

Below are highlighted some of the key new requirements for Privacy Shield and information on the ICDR/AAA and how to designate the ICDR/AAA as your independent recourse mechanism for the EU-U.S. and Swiss-U.S. Privacy Shield programs.

To be assured of Privacy Shield benefits, an organization must self-certify annually to the Department of Commerce (via its website) 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 can be found in the *"How to Join Privacy Shield"* on the Department of Commerce's website at https://www.privacyshield.gov.

Key New Requirements

- 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. When selecting the ICDR/AAA as your independent recourse mechanism the link would be: http://go.adr.org/privacyshield.html.
- 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.

Ensure that Your Organization's Privacy Policy Conforms to the Privacy Shield Principles

Make specific reference in the Privacy Policy to your organization's Privacy Shield Compliance. In addition, the privacy policy must include a hyperlink to the Privacy Shield website (https://www.privacyshield.gov/).

Identify in the Privacy Policy Your Organization's Independent Recourse Mechanism

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.

The ICDR serves as the independent recourse mechanism for U.S. companies across the country. When designating the ICDR (the international division of the American Arbitration Association) please use the following hyperlink: http://go.adr.org/privacyshield.html.

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.

What are the Differences Between the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks?

The Principles under the two frameworks align, with a few exceptions, including:

- The Swiss Federal Data Protection and Information Commissioner's authority substitutes for that of the EU DPAs' authority throughout the Swiss-U.S. Privacy Shield compared to the EU-U.S. Privacy Shield. For instance, under the Swiss-U.S. Privacy Shield, an organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the Swiss Federal Data Protection and Information

Commissioner. When covering HR data received from Switzerland for use in the context of the employment relationship, organizations must commit to cooperate with and comply with the advice of the Commissioner. Under the EU-U.S. Privacy Shield, the comparable commitment is to cooperate with the EU DPAs.

- The definition of sensitive data under the Choice Principle is modified slightly under the Swiss-U.S. Privacy Shield, including ideological views or activities, information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

Benefits to Using the ICDR/AAA

- The ICDR/AAA is the largest international ADR provider.
- ICDR/AAA arbitrators and mediators are drawn from a pool of professionals with privacy expertise and language capabilities from many different countries.
- Disputes will be determined pursuant to the ICDR International Arbitration Rules, based on documents only and as modified by the Privacy Shield procedures and fee schedule for this program.
- In-person hearings will not be provided for these cases unless they are requested and agreed to by the parties.
- Arbitrations will be conducted on an expedited basis.

ICDR/AAA Registration Fee Schedule

The Fee Schedule for selecting the ICDR/AAA as the administrator for your company/organization's independent recourse mechanism is as follows and will apply on an annual basis from the date of your registration.

Effective immediately for any registrations received, the ICDR/AAA will charge the fees below that will cover a 12-month period. New invoices will be sent on the 11th month from the date of your initial registration. The new invoice will reflect the fees for the following 12-month period of your designating the ICDR/AAA as your EU-U.S. and/or Swiss – U.S. Privacy Shield independent recourse mechanism.

The fee schedule will be based on a company's total annual sales, as follows:

- Up to and including 1 million USD: $300.00.
- Over 1 million USD: $500.00.

The fees are for *registration only* and do not include the fees for the administration of the arbitrations if any cases are filed with the ICDR/AAA. The fees will cover the registration for the EU-U.S and/or Swiss-U.S. Privacy Shield programs. Upon registering with the ICDR/AAA U.S. companies must advise if they are selecting one or both Privacy Shield programs as that will be reflected in the registry. See below for the fee schedule for the arbitrations, along with additional information on the program and the applicable rules (available in several languages).

ICDR/AAA Fee Schedule for Arbitrations

The fee schedule for the arbitrations can be found in *ICDR/AAA Fees for EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield* at http://go.adr.org/privacyshield.html and on the ICDR website www.icdr.org.

ICDR/AAA Privacy Shield Procedures

Additional information on the program can be found in *ICDR/AAA EU-U.S. and Swiss-U.S. Privacy Shield Administrative Procedures* at http://go.adr.org/privacyshield.html and on www.icdr.org.

ICDR Dispute Resolution Procedures

The applicable rules are available in several languages and can be found at http://go.adr.org/privacyshield.html or at www.icdr.org.

To Register for the ICDR/AAA EU-U.S. and/or Swiss-U.S. Privacy Shield Program

Companies can register with the ICDR/AAA by regular mail or by email.

By Email. Please send an email to Ms. Alyssa Montano at MontanoA@adr.org

By Mail. Please send a letter to:
Ms. Alyssa Montano
ICDR/AAA Privacy Shield Program
120 Broadway, 21st floor
New York, NY 10271

In the letter or the email,

- Reference the ICDR/AAA EU-U.S. and/or Swiss-U.S. Privacy Shield program and request that your company be listed on the ICDR/AAA's EU-U.S. and/or Swiss-U.S. Privacy Shield website, thereby certifying that you have selected the ICDR/AAA *as your independent recourse mechanism for Privacy Shield privacy complaints.*
- Please include your complete contact information for all notices and billing, along with your annual sales and the appropriate filing fee.
- Checks should be made payable to the American Arbitration Association. If registering by email, Ms. Montano will send a credit card authorization form and will process the registration electronically.

Upon receipt of the above, the ICDR/AAA will send a letter of confirmation. *Your company then must create or modify its privacy notice,* ensuring that it is available to the public, that it is in compliance with the EU-U.S. and/or Swiss-U.S. Privacy Shield programs and referencing the ICDR/AAA as your independent recourse mechanism.

To be assured of Privacy Shield benefits, an organization **must** self-certify annually to the Department of Commerce (via its website for one or both programs) 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 can be found in the *"How to Join Privacy Shield"* on the Department of Commerce's website at https://www.privacyshield.gov.

For further information on the ICDR/AAA Privacy Shield Program, please call or email Mr. Luis Martinez at MartinezL@adr.org or at +1.212.716.5833 or Ms. Alyssa Montano at MontanoA@adr.org +1.212.484.3281.