

# 2023 Annual Report on Privacy Shield and Data Privacy Framework Cases

## JAMS- Executive Summary

This annual report is submitted by JAMS, for the reporting period of Aug. 1, 2022 through July 31, 2023, as an Independent Recourse Mechanism supporting the EU-U.S. Privacy Shield, Swiss-U.S. Privacy Shield frameworks, EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).<sup>1</sup>

## Organizations

JAMS served as an Independent Recourse Mechanism provider under the EU-U.S. Privacy Shield program and also under the Swiss-U.S. Privacy Shield program and now the Data Privacy Frameworks. The following is an overview of information related to the JAMS Privacy Shield Services and the Data Privacy Framework Services.

The number of organizations enrolled in the Privacy Shield program is 1991 (including active and inactive).

There are currently no organizations enrolled in DPF.

JAMS does not provide a Privacy-Shield or Data Privacy Framework related verification service.

## Guidance

JAMS provides information located on its website for any organizations or participants that wish to register. JAMS also provides a designated point of contact to answer questions regarding registration, and a General Fee Schedule should a mediation case need to be opened.

A link to the information/registration can be found here:

<https://www.jamsadr.com/dpf-registration-page>

---

<sup>1</sup> The EU-U.S. Data Privacy Framework (EU-U.S. DPF) amends the privacy principles that organizations adhered to under the EU-U.S. Privacy Shield Framework as the “EU-U.S. Data Privacy Framework Principles” (EU-U.S. DPF Principles); and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) amends the privacy principles that organizations adhered to under the Swiss-U.S. Privacy Shield Framework as the “Swiss-U.S. Data Privacy Framework Principles” (Swiss-U.S. DPF Principles). The EU-U.S. DPF Principles, which entered into effect on July 10, 2023, lay out a set of requirements for participating organizations’ use and treatment of personal data received in reliance on the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF. Effective as of July 17, 2023, eligible organizations in the United States that wish to self-certify their compliance pursuant to the UK Extension to the EU-U.S. DPF may do so. The Swiss-U.S. DPF Principles, which entered into effect July 17, 2023, lay out a set of requirements for participating organizations’ use and treatment of personal data received in reliance on the Swiss-U.S. DPF. Neither the EU-U.S. DPF nor the Swiss-U.S. DPF create new substantive obligations for organizations with regards to protecting EU and Swiss personal data (*i.e.*, the privacy principles, including provisions concerning independent recourse mechanisms remain substantively the same). The Privacy Shield Program administered by the U.S. Department of Commerce’s International Trade Administration (ITA) has been updated and renamed as the Data Privacy Framework (DPF) Program.

## Compliance Activities

JAMS provides daily reports of registrations to the Department of Commerce. JAMS also advises organizations of lapses or changes in self-certifications based on notifications from the US Department of Commerce which may affect compliance.

## Data Privacy Framework “DPF” Complaint Handling

A DPF complaint can be filed with JAMS by submission through its “File a Claim with JAMS” hyperlink on its website. <https://www.jamsadr.com/file-a-dpf-claim> JAMS then reviews any complaint for validity, and eligibility under the frameworks.

The Eligibility Requirements are as follows:

### ***Eligibility***

- a. *You are the subject of personal data collected in the European Union / European Economic Area, UK, and / or Switzerland; or*
- b. *You are the parent or legal guardian of that data subject in the case of personal data collected from a child under the age of 13. Please note, if JAMS cannot verify your identity, JAMS may choose not to open a case.*

### ***To be accepted your complaint must:***

- a. *Be filed by an eligible Complainant (either the subject of the alleged data protection breach, or the parent/legal guardian of a child under the age of 13 who is of the subject of the alleged data protection breach).*
- b. *Be made against an entity in the United States that (1) has self-certified its compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF); and the Swiss-U.S. Data Privacy Framework, or the UK Extension as applicable, to the U.S. Department of Commerce, whichever applies, and (2) has designated JAMS as its ADR provider for disputes under the DPF Frameworks.*
- c. *Allege that the Respondent failed to comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF); and the Swiss-U.S. Data Privacy Framework, or the UK Extension as applicable, in relation to the Complainant’s covered personal data.*
- d. *Include credible documentation to support the Complainant’s allegations.*
- e. *Provide evidence that you have completed a good faith effort to resolve the Complaint in accordance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF); and the Swiss-U.S. Data Privacy Framework, or the UK Extension as applicable, whichever applies.*
- f. *Have not been previously resolved by negotiation, court action, arbitration, or any other form of dispute settlement; and*
  - g. *Unless agreed by both Parties to the case, not be the subject of current litigation or any other adjudicatory process (including claims submitted for resolution through binding arbitration).*

### ***Information submitted with your claim:***

*Information submitted by a Complainant must be sufficiently complete to permit both JAMS and the Respondent to evaluate and understand the Complaint adequately, and to enable the Respondent to respond to the Complaint. JAMS has sole authority to determine whether the information submitted is sufficiently complete to open a case.*

*Please note that all complaint materials should be submitted in English.*

If eligible, JAMS will seek to coordinate and facilitate a resolution of the complaint typically within 30-45 days through communication with the organization and complainant. If these efforts are unsuccessful, JAMS will officially open a case wherein a mediator will be selected by the parties to address applicable or appropriate remedies/sanctions based upon the parties' specific circumstances (i.e. data removal, compensation for individual losses etc.). If this is unsuccessful, JAMS will refer the case to the Department of Commerce as appropriate.

### **Statistics**

Total Eligible Claims received under the Privacy Shield Frameworks: **1**

**Total Eligible Claims received under the DPF: 0**

Type of Claim Received-1 request to have personal information/data protected and accessible to complainant

Total Claims resolved or otherwise disposed (i.e. closed) of under the Privacy Shield Frameworks: **1**

**Total Claims resolved or otherwise disposed (i.e. closed) of under DPF: 0**

Quality measures and outcomes: Complaint settled with organization to Complainant's satisfaction in mediation.

JAMS processed complaint within 6 days of receipt from Complainant and organization responded to Complainant within one week. Resolution by the parties was achieved 90 days after initially processed by JAMS.

There are no sanctions to report.