SmartSuite

Framework / Privacy / Other

Data Privacy Framework (DPF) Program: EU-U.S. DPF, UK Extension to the EU-U.S. DPF and Swiss-U.S. DPF

The U.S. Data Privacy Framework is the Commerce Department self-certification program for EU, UK and Swiss personal data transfers under the adequacy decision of July 10, 2023.



What it is

The U.S. Data Privacy Framework (DPF) program is the U.S. Department of Commerce mechanism, administered by the International Trade Administration (ITA), under which U.S. organizations self-certify their adherence to the DPF Principles. That self-certification lets personal data be transferred to them from the European Union under the European Commission's adequacy decision of July 10, 2023. It also covers transfers from the United Kingdom under the UK Extension to the EU-U.S. DPF (in force October 12, 2023) and from Switzerland under the Swiss-U.S. DPF (from September 15, 2024). Joining is voluntary; once an organization self-certifies, compliance with the Principles is compulsory and enforceable by the Federal Trade Commission under Section 5 of the FTC Act or by the Department of Transportation under 49 U.S.C. 41712.

At a glance

PUBLISHER
U.S. Department of Commerce, International Trade Administration (program and Principles); European Commission (adequacy decision)

TYPE
Framework

VERSION
EU-U.S. DPF Principles (adequacy decision of July 10, 2023); UK Extension (in force October 12, 2023); Swiss-U.S. DPF (from September 15, 2024)

EFFECTIVE
July 10, 2023 (EU adequacy decision); UK Extension October 12, 2023; Swiss-U.S. DPF September 15, 2024

DOMAIN
Privacy

FAMILY
Other

REGION
United States

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
Medium

Source: dataprivacyframework.gov/

Why it matters

- **One certification, three jurisdictions** The Department of Commerce notice of March 30, 2023 covers the EU-U.S. DPF, the UK Extension and the Swiss-U.S. DPF in one program; an organization chooses which parts it certifies to, and UK participation requires EU-U.S. participation.
- **Government safeguards apply to every transfer** The Commission notes that the EO 14086 limits and the redress mechanism apply to all GDPR transfers to the United States, whatever the mechanism, so they also support standard contractual clauses and binding corporate rules.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports US DPF

Principles Requirement Library

Load the seven Principles, the Supplemental Principles and Annex I as requirements with the policy clause, control, owner and evidence that satisfy each, and the jurisdictions (EU, UK, Switzerland) each certification covers.

Data Inventory and Purpose Register

Record the personal data received from the EU, UK and Switzerland, its purposes and retention, to evidence Data Integrity and Purpose Limitation (Principle 5) and Notice (Principle 1).

Onward Transfer Agreements

Track agents and third parties receiving DPF data, their contracts and compliance evidence under Accountability for Onward Transfer (Principle 3) in Third Party Risk Management.

Access, Choice and Complaint Handling

Log access and opt-out requests and complaints with deadlines and outcomes, and the referrals to the independent recourse mechanism (Principles 2, 6 and 7).

Annual Re-certification and Verification

Keep the self-certification record, the verification method and its evidence, the privacy policy version and the re-certification calendar the ITA requires.

Enforcement and List Status Reporting

Report List status, open complaints, overdue requests and policy changes so the organization can show the FTC, the DOT or an exporter that its public commitments match its practice.

Common framework mappings

CCPA/CPRA · GDPR · FedRAMP Rev. 5 · HIPAA · ISO 27001:2022 · ISO 27701 · NIST CSF 2.0 · NIST Privacy Framework v1.0 · PCI DSS 4.0.1 · SOC 2

Official resources

Data Privacy Framework Program (U.S. Department of Commerce)

The program site run by the International Trade Administration: the DPF Principles, the self-certification list and participant obligations.

dataprivacyframework.gov

Executive Order 14086 (87 FR 62283, October 14, 2022)

Enhancing Safeguards for United States Signals Intelligence Activities: the necessity and proportionality standard and the redress mechanism behind the DPF.

federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

European Commission: EU-US data transfers

The Commission's page on the EU-U.S. Data Privacy Framework adequacy decision of 10 July 2023 and its review.

commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

Frequently asked questions

Is participation in the Data Privacy Framework mandatory?

No. The Principles document says that the decision to self-certify is entirely voluntary, but effective compliance is compulsory: an organization that self-certifies to the Department of Commerce and publicly declares its commitment must comply fully with the Principles. Non-compliance is enforceable by the FTC under Section 5 of the FTC Act, by the DOT under 49 U.S.C. 41712, and by removal from the Data Privacy Framework List with a public record of the removal.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the seven DPF Principles?

Part II of the Principles lists Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability. The last requires readily available independent recourse mechanisms and, as a last resort, binding arbitration under Annex I. Part III adds Supplemental Principles, including self-certification, verification, dispute resolution and enforcement and human resources data.

Who can join, and how does an organization stay on the List?

An organization must be subject to the investigatory and enforcement powers of the FTC, the DOT or another recognized statutory body, publicly declare its commitment to the Principles, publish a privacy policy in line with them and implement them (Federal Register notice of March 30, 2023). It self-certifies to the ITA, naming its recourse mechanism and verification method, and must re-certify at least annually; organizations that withdraw, miss re-certification or persistently fail to comply are removed and listed in a public removal record.

What did Executive Order 14086 change?

Section 2 limits U.S. signals intelligence to legitimate objectives pursued only when necessary and proportionate. Section 3 creates a redress mechanism: a complaint from an individual in a qualifying state goes through that state's public authority to the ODNI Civil Liberties Protection Officer, whose determination can be reviewed by a three-judge Data Protection Review Court panel, established by Attorney General regulation at 28 CFR Part 201, with a special advocate for the complainant and binding remediation. The Commission cites these safeguards as the basis of its July 10, 2023 adequacy decision.

Does the DPF cover transfers from the United Kingdom and Switzerland?

Yes, for organizations that certify to those parts. The UK Extension took effect through the Data Protection (Adequacy) (United States of America) Regulations 2023 (SI 2023/1028), in force October 12, 2023, after the U.S. Attorney General designated the UK a qualifying state on September 18, 2023; UK participation requires EU-U.S. participation. The Swiss Federal Data Protection and Information Commissioner recorded that certified U.S. companies ensure adequate protection from September 15, 2024 under the Swiss-U.S. DPF.

License included / downloadable: Yes The DPF Principles, the Data Privacy Framework List and the program guidance are published free by the U.S. Department of Commerce at dataprivacyframework.gov; the Commission's adequacy decision, Executive Order 14086 and the UK Regulations are public legal texts. This page describes the program and is not a statement of any organization's participation in it.

Full framework page and mappings: smartsuite.com/frameworks/us-data-privacy-framework-dpf-cross-border-personal-data-transfer