

EU-US Data Privacy Framework (DPF)

The EU-US Data Privacy Framework enables lawful transfers of EU personal data to US organizations by requiring adequate privacy protections.



What it is

The EU-US Data Privacy Framework (DPF) is a transatlantic data protection framework that facilitates lawful transfers of personal data from the European Union (EU) to the United States (US) in compliance with EU data protection requirements. Its primary purpose is to ensure that participating US organizations provide adequate privacy protections for personal data originating in the EU.

Developed and administered by the US Department of Commerce in collaboration with the European Commission, the DPF sets out privacy principles covering notice, choice, accountability for onward transfer, security, data integrity, access, and recourse. It is primarily used by US-based organizations receiving EU personal data, as well as by EU companies and their compliance teams seeking to validate data transfer mechanisms under the General Data Protection Regulation (GDPR).

At a glance

PUBLISHER U.S. Department of Commerce	TYPE Framework	VERSION EU-US Data Privacy Framework (DPF)
EFFECTIVE July 10, 2023	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.dataprivacyframework.gov/s/>

Why it matters

- **Support cross-border data transfers** Facilitate compliant movement of personal data between the EU and US while reducing operational barriers.
- **Enhance regulatory alignment** Demonstrate adherence to GDPR and European data protection standards, improving trust with regulators and customers.
- **Strengthen data protection practices** Institute robust procedures and controls for protecting EU-origin personal data within US-based organizations.
- **Increase audit readiness** Maintain documentation and safeguards required for external reviews, investigations, or compliance audits.

How SmartSuite supports EU-US DPF

EU Data Processing Inventory

Document EU data categories, purposes, sharing, and safeguards with traceability.

Policy Commitments and Accountability

Track required privacy commitments, policy reviews, and proof that practices align.

Access and Correction Request Management

Manage access/correction requests and complaints with deadlines and an audit trail.

Vendor and Onward Transfer Oversight

Track vendor contracts, safeguards, and monitoring for onward data transfers.

Incident Response and Documentation

Run breach workflows with timelines, decisions, and corrective actions.

Compliance Program Status and Evidence Reporting

Report program status, open gaps, and evidence coverage for ongoing compliance.

Common framework mappings

- CCPA/CPRA
- EU SCCs (2021)
- GDPR
- ISO 27701

Official resources

EU-US Data Privacy Framework Overview

Provides a detailed overview of the framework principles and requirements for data protection.

dataprivacyframework.gov/s/framework

EU-US Privacy Shield Framework Documents

Describes the updates and documents related to the framework and participant guidance.

dataprivacyframework.gov/s/docs

EU-US Data Privacy Program Rules

Outlines the rules and processes for participation in the Data Privacy Framework.

dataprivacyframework.gov/s/program-rules

Frequently asked questions

What is the EU-US Data Privacy Framework (DPF) used for?

The EU-US Data Privacy Framework (DPF) facilitates the lawful transfer of personal data from the EU to the US, ensuring that US organizations provide privacy protections aligned with EU requirements. It helps businesses comply with the General Data Protection Regulation (GDPR) when handling cross-border data transfers.

Is the EU-US Data Privacy Framework required or mandatory?

The DPF is not mandatory but is a voluntary self-certification program for US-based organizations seeking to receive EU personal data under GDPR-compliant conditions. Organizations choosing not to participate must use alternative EU-approved data transfer mechanisms.

Who does the EU-US Data Privacy Framework apply to?

The DPF primarily applies to US organizations that receive personal data from the EU and wish to demonstrate GDPR-equivalent data protection via self-certification. It is also relevant for EU entities and their compliance teams seeking validated mechanisms for cross-border data transfers.

What key principles or controls are required by the DPF?

The DPF sets out seven core privacy principles: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability. Organizations must implement policies and procedures to meet these requirements and ensure data subject rights are protected.

How do organizations implement the EU-US Data Privacy Framework?

To implement the DPF, organizations must develop and publicly post compliant privacy policies, conduct risk assessments on data transfers, establish security controls, and maintain processes for handling complaints and regulatory inquiries. Formal self-certification with the US Department of Commerce is required annually.

How does the DPF relate to other regulatory frameworks like GDPR?

The DPF is designed to align with GDPR data protection standards, providing a recognized mechanism for EU-to-US data transfers. While it complements GDPR and other international frameworks, organizations must ensure DPF participation is in conjunction with internal privacy compliance and other legal obligations.

What are the ongoing compliance requirements under the DPF?

Ongoing compliance includes annual re-certification, maintaining up-to-date privacy notices, internal monitoring of data handling practices, regular staff training, and responsive complaint and inquiry management. Documentation and evidence of compliance activities must be available for regulatory review.

How would SmartSuite support the EU-US Data Privacy Framework?

SmartSuite helps organizations manage DPF compliance by centralizing privacy control libraries, tracking risks, and supporting policy and process governance. The platform enables evidence collection, automates compliance monitoring, facilitates audit readiness, and delivers reporting to demonstrate adherence to DPF principles.

License included / downloadable: Yes The EU-US Data Privacy Framework documentation and program requirements are publicly available through official U.S. Department of Commerce and European Commission resources.

Full framework page and mappings: smartsuite.com/frameworks/eu-us-data-privacy-framework-dpf