

U.S. Data Privacy Framework (DPF)

U.S. Data Privacy Framework governs transfers of personal data to the U.S., ensuring privacy safeguards and avenues for redress.



What it is

The U.S. Data Privacy Framework (DPF) is a cross-border personal data transfer framework that facilitates compliant transfers of personal data from the European Union, United Kingdom, and Switzerland to the United States, helping organizations meet international data protection and privacy requirements.

Published by the U.S. Department of Commerce in coordination with European and Swiss authorities, the DPF is used by U.S.-based organizations that receive personal data from abroad and need to demonstrate adequate privacy safeguards. The framework addresses areas such as privacy governance, data protection, and regulatory compliance, supporting the lawful transfer of personal information in line with global privacy regulations like the EU General Data Protection Regulation (GDPR).

At a glance

PUBLISHER U.S. Department of Commerce	TYPE Framework	VERSION 2023
EFFECTIVE July 11, 2023	DOMAIN Privacy	FAMILY APEC Privacy Framework
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

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

Why it matters

- **Enhance regulatory alignment** Support compliance with international privacy laws, such as GDPR, by adopting recognized cross-border data transfer mechanisms and privacy principles.
- **Strengthen data protection practices** Promote robust safeguards for personal data by requiring transparent policies and effective risk management in global operations.
- **Increase audit readiness** Demonstrate privacy controls and compliance measures to regulatory authorities through certification and ongoing oversight requirements.
- **Support business continuity** Reduce legal and operational risks associated with cross-border data transfers, enabling uninterrupted data-driven business activities.

How SmartSuite supports US DPF

Privacy Principle Control Library

Structure DPF privacy principles with mapped controls, ownership, and implementation tasks.

Data Processing and Transfer Records

Maintain records of personal data processing, transfer purposes, and data lifecycle governance.

International Data Transfer Tracking

Track international data transfers, safeguards, and contractual requirements supporting DPF compliance.

Data Subject Rights Management

Manage access, correction, and deletion requests while documenting response timelines and outcomes.

Vendor and Subprocessor Privacy Oversight

Track third-party data processors, privacy obligations, and compliance documentation.

DPF Privacy Compliance and Certification Reporting

Provide dashboards summarizing privacy control coverage, open issues, and readiness for DPF self-certification and regulatory review.

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

U.S. Data Privacy Framework Overview

Describes the structure and key elements of the U.S. Data Privacy Framework for personal data transfer.
commerce.gov/data-privacy-framework

Department of Commerce Data Privacy FAQs

Provides answers to frequently asked questions about the U.S. Data Privacy Framework.
commerce.gov/privacy-faq

Department of Commerce Guidance on Cross-Border Transfers

Outlines guidelines for transferring personal data under the U.S. Data Privacy Framework.
commerce.gov/guidance-cross-border-transfers

Frequently asked questions

What is the U.S. Data Privacy Framework (DPF) used for?

The U.S. Data Privacy Framework (DPF) facilitates lawful cross-border transfers of personal data from the European Union, United Kingdom, and Switzerland to the United States. Its main purpose is to ensure that U.S. organizations provide an adequate level of data protection that aligns with EU, UK, and Swiss privacy requirements.

Is the U.S. Data Privacy Framework (DPF) certification mandatory?

DPF certification is voluntary, but organizations wishing to import personal data from the EU, UK, or Switzerland and comply with data transfer requirements must self-certify to the DPF with the U.S. Department of Commerce. Certification is required for legal adequacy and to benefit from streamlined data transfer mechanisms.

Who does the U.S. Data Privacy Framework (DPF) apply to?

The DPF applies to U.S.-based organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) that process or receive personal data from the EU, UK, or Switzerland. It is most relevant to companies engaged in cross-border data transfers with partners or customers in those regions.

What are the key principles and requirements of the DPF?

DPF certified organizations must uphold principles such as notice, choice, accountability for onward transfer, security, data integrity, access, and recourse, enforcement, and liability. These principles guide how organizations collect, use, and protect personal data received under the DPF.

How does a company implement the U.S. Data Privacy Framework?

To implement the DPF, organizations must develop and publish a privacy policy reflecting DPF principles, conduct internal reviews of data handling practices, establish complaint handling procedures, and self-certify annually with the Department of Commerce. Regular training and compliance monitoring are also necessary.

How does the DPF relate to other international data transfer mechanisms?

The DPF functions similarly to previous frameworks like Privacy Shield or Standard Contractual Clauses (SCCs) but is specifically approved for adequacy by the European Commission and recognized by UK and Swiss authorities. Organizations may choose the DPF or alternative mechanisms depending on their data transfer needs.

What are the ongoing requirements for maintaining DPF compliance?

Organizations must annually re-certify with the Department of Commerce, maintain updated privacy notices, respond to data subject inquiries, address complaints, and ensure continued adherence to DPF principles. Non-compliance may result in enforcement actions by the FTC or DOT.

How would SmartSuite support U.S. Data Privacy Framework (DPF)?

SmartSuite can help organizations manage DPF compliance by centralizing risk tracking, documenting required controls, and streamlining evidence collection for annual self-certification. Its platform supports audit readiness through workflow management, task assignment, and real-time reporting to ensure continued alignment with DPF requirements.

License included / downloadable: Yes The U.S. Data Privacy Framework is publicly available for free on the Department of Commerce website.
License included with platform

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