

PSD2 (Directive (EU) 2015/2366)

PSD2 is an EU directive that strengthens security, transparency, and consumer protection for electronic payments and third-party providers.



European
Union

What it is

EU PSD2 — Payment Services Directive (Directive (EU) 2015/2366) is a European Union regulation that strengthens security, transparency, and consumer protection for electronic payments and payment services. The directive establishes requirements for strong customer authentication, reduces fraud, and fosters innovation and competition in the financial technology sector.

Published by the European Parliament and Council, PSD2 applies to banks, payment service providers, and fintech organizations operating within the European Economic Area. It addresses cybersecurity, data protection, operational risk management, and regulatory compliance by mandating secure access to payments infrastructure and setting rules for third-party providers.

At a glance

PUBLISHER European Commission	TYPE Regulation	VERSION Directive (EU) 2015/2366
EFFECTIVE January 13, 2018	DOMAIN Financial Services Regulation	FAMILY Other
REGION European Union	INDUSTRY Payment & FinTech	ADOPTION MODEL Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/payment-services-directive_en

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 PSD2

Authentication and SCA Controls

Track SCA requirements, MFA controls, and authentication evidence for payment flows.

API and Interface Security Governance

Manage control requirements and testing evidence for regulated interfaces.

Fraud and Transaction Monitoring Workflows

Track monitoring controls, alerts, investigations, and improvements.

Incident Response and Reporting Discipline

Run incident workflows with timelines, escalations, and documentation.

Critical Provider Contract and Monitoring Management

Manage critical provider contracts, reviews, and ongoing monitoring evidence.

Compliance Reporting

Report control status, testing coverage, and open issues for stakeholders.

Common framework mappings

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

Official resources

Payment Services Directive (PSD2) Text

Defines the legal framework and requirements for the Payment Services Directive.

eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

PSD2 Implementation Guidelines

Provides guidelines for implementing PSD2 requirements across financial institutions.

eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money

EBA Regulatory Technical Standards for PSD2

Describes the technical standards for strong customer authentication and secure communication.

eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/payment-services-and-electronic-money-0

PSD2 Compliance and Risk Management Overview

Outlines compliance requirements and risk management processes for PSD2 adherence.

ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html

Frequently asked questions

What is EU PSD2 used for?

EU PSD2 is a regulatory framework designed to enhance security, transparency, and consumer protection for electronic payments and payment services within the European Economic Area. It standardizes requirements for secure payment processing, facilitates safe third-party access to banking data, and aims to reduce fraud and encourage innovation in financial technology.

Is EU PSD2 mandatory for payment service providers?

Yes, compliance with PSD2 is mandatory for banks, payment institutions, and other payment service providers operating in the EU and EEA. Organizations are legally required to implement PSD2 provisions to maintain authorization and continue offering payment services.

Who does EU PSD2 apply to?

PSD2 applies to all financial institutions, including traditional banks, fintech companies, and third-party payment providers (TPPs) that process or access payment data of individuals and businesses within the EU and EEA. This applies regardless of the location of the service provider if the transaction involves parties in the EU.

What are key requirements and controls under EU PSD2?

Organizations must implement Strong Customer Authentication (SCA), secure communication protocols, risk management policies, and access controls for third-party providers. Key deliverables include multi-factor authentication, transaction monitoring, secure APIs, and audit trails for payment data access.

How is EU PSD2 typically implemented in practice?

Implementation involves deploying technical solutions for SCA, mapping roles and permissions for data access, and setting up continuous monitoring of payment transactions. Organizations must update internal policies, perform regular risk assessments, and train staff to recognize and address PSD2-related risks.

How does EU PSD2 relate to other compliance frameworks like GDPR?

PSD2 and GDPR have overlapping requirements around data protection, privacy, and incident response. Organizations frequently align their PSD2 compliance program with GDPR by harmonizing data management practices, breach notification processes, and security controls to satisfy both sets of requirements.

What are the ongoing compliance responsibilities under EU PSD2?

Continuous compliance requires regular security testing, risk assessments, monitoring third-party access, and maintaining up-to-date incident response plans. Firms are also expected to keep detailed records, respond to regulatory audits, and update procedures as regulatory interpretations evolve.

How would SmartSuite support EU PSD2?

SmartSuite enables organizations to manage EU PSD2 compliance by centralizing risk tracking, managing control libraries aligned with directive requirements, and facilitating evidence collection for audits. The platform provides dashboards for real-time compliance monitoring, supports audit readiness, and orchestrates remediation workflows to address gaps or findings efficiently.

License included / downloadable: Yes PSD2 is European Union legislation and is publicly available through official EU regulatory publications.

Full framework page and mappings: smartsuite.com/frameworks/eu-psd2-payment-services-directive-directive-eu-2015-2366