

EU GDPR — Regulation (EU) 2016/679

GDPR is an EU regulation that protects individuals' personal data and strengthens organizations' accountability for privacy.



What it is

The EU General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation that establishes requirements for how organizations collect, process, and safeguard personal data of individuals within the European Union. Its primary purpose is to strengthen data privacy rights and enhance organizational accountability in handling personal information.

Enforced and published by the European Union, the GDPR applies to all organizations—regardless of location—that offer goods or services to, or monitor the behavior of, individuals in the EU. The regulation covers areas such as data protection governance, risk management, breach notification, individual rights, and cross-border data transfers.

At a glance

PUBLISHER

European Commission

TYPE

Regulation

VERSION

Regulation (EU) 2016/679

EFFECTIVE

May 25, 2018

DOMAIN

Privacy

FAMILY

Global Privacy Regulations

REGION

European Union

ADOPTION MODEL

Regulatory Compliance

IMPLEMENTATION COMPLEXITY

Very High

Source: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

Why it matters

- **Strengthen data protection practices** Enable organizations to safeguard personal data through rigorous privacy controls, reducing the risk of unauthorized access or disclosure.
- **Enhance regulatory alignment** Support compliance with EU and global privacy laws, ensuring organizations meet mandatory legal requirements for data processing activities.
- **Promote individual rights and trust** Empower individuals with greater control over their personal information, thereby fostering customer trust and organizational transparency.
- **Reduce breach and enforcement risk** Implement requirements for incident detection, reporting, and risk assessments, lowering the threat of data breaches or regulatory penalties.

How SmartSuite supports GDPR

Records of Processing Activities

Maintain processing inventories with purposes, lawful bases, sharing, and retention.

DSAR Workflows and Deadlines

Manage access, deletion, correction, and objection requests with full audit trail.

DPIAs and Privacy Risk Management

Track high-risk processing assessments, mitigations, and approvals.

Processor and Subprocessor Oversight

Manage DPAs, vendor reviews, and ongoing monitoring evidence.

Breach Response and Documentation

Run incident workflows with timelines, decisions, and post-incident improvements.

Accountability Reporting

Report privacy posture, open actions, and readiness across the organization.

Common framework mappings

APEC PF

CCPA/CPRA

ISO 27001:2022

ISO 27002:2022

ISO 27701

NIST Privacy Framework v1.0

OECD Privacy Guidelines

UK DPA 2018

Official resources

EU GDPR Full Text

Provides the complete legal text of the General Data Protection Regulation.

eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Guidelines on GDPR Implementation and Compliance

Outlines practical guidance for implementing and complying with GDPR.

edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Data Protection Impact Assessment Guidelines

Describes requirements and procedures for conducting data protection impact assessments.

edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

GDPR Recitals

Provides the context and reasoning behind each GDPR requirement.

eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Frequently asked questions

What is the EU GDPR used for?

The EU GDPR is designed to protect personal data and privacy rights of individuals within the European Union. It establishes legal requirements for how organizations collect, process, store, and transfer personal data, ensuring data subjects' fundamental rights are respected.

Is the EU GDPR mandatory for organizations?

Yes, GDPR is a legally binding regulation that applies to all organizations offering goods or services to, or monitoring the behavior of, individuals in the EU, regardless of the organization's location. Non-compliance can result in significant administrative fines and enforcement actions.

Who does the EU GDPR apply to?

The GDPR applies to any data controllers or processors—whether established inside or outside the EU—that handle the personal data of individuals located within the EU. This includes companies, non-profits, and public authorities that process EU personal information.

What are the key concepts and required artifacts under GDPR?

Key GDPR concepts include lawfulness, transparency, data minimization, purpose limitation, and accountability. Required artifacts include Records of Processing Activities (ROPAs), Data Protection Impact Assessments (DPIAs), privacy notices, and evidence of consent and security controls.

How do organizations implement GDPR requirements?

Organizations implement GDPR by mapping data flows, determining lawful bases for processing, conducting DPIAs, establishing data protection policies, managing vendor relationships with Data Processing Agreements (DPAs), and training staff on compliance responsibilities.

How does the EU GDPR relate to other privacy frameworks?

GDPR can intersect with frameworks such as ISO 27701 and the NIST Privacy Framework, often serving as a baseline for privacy program development. Aligning GDPR with these or local requirements streamlines global compliance and harmonizes privacy risk management.

What are ongoing compliance obligations under GDPR?

Maintaining GDPR compliance requires continuous monitoring of processing activities, updating policies and records, periodic staff training, regular security assessments, management of data subject rights requests, and prompt breach notification to supervisory authorities when required.

How would SmartSuite support EU GDPR?

SmartSuite supports GDPR management by providing tools for risk tracking, control implementation, evidence collection, and records management. It enables organizations to operationalize DPIAs, automate compliance workflows, prepare for audits, manage incident tracking, and generate reports to demonstrate compliance.

License included / downloadable: Yes The General Data Protection Regulation is European Union legislation and is publicly available through official EU regulatory publications.

Full framework page and mappings: smartsuite.com/frameworks/eu-gdpr-general-data-protection-regulation