SmartSuite

Framework / Privacy / Global Privacy Regulations

EU GDPR — Regulation (EU) 2016/679

The GDPR (Regulation (EU) 2016/679) sets principles, lawful bases, individual rights and accountability duties for personal data, with fines up to EUR 20 million or 4 percent of turnover.



What it is

The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) governs the processing of personal data of people in the European Union: it sets seven principles, six lawful bases and a set of individual rights, requires controllers to demonstrate compliance, and allows fines of up to EUR 20 million or 4 percent of worldwide annual turnover. It was adopted on April 27, 2016, entered into force on May 24, 2016 and has applied since May 25, 2018.

The European Parliament and the Council adopted it, and independent national supervisory authorities enforce it, coordinated by the European Data Protection Board. It applies to controllers and processors established in the Union and to those outside it that offer goods or services to people in the Union or monitor their behavior there (Article 3). Member States add national rules where the Regulation leaves choices open.

At a glance

PUBLISHER European Parliament and Council of the European Union	TYPE Regulation	VERSION Regulation (EU) 2016/679
EFFECTIVE May 25, 2018 (entered into force May 24, 2016)	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION European Union	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

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

Why it matters

- **Accountability is the test** The controller is responsible for, and must be able to demonstrate, compliance with the principles (Article 5(2)).
- **Rights people can use** Access, rectification, erasure, restriction, portability, objection and protection from solely automated decisions (Articles 15 to 22), with a response due within one month (Article 12(3)).
- **Breach notification clock** A personal data breach that risks people's rights is notified to the supervisory authority within 72 hours of becoming aware of it (Article 33).
- **Controlled transfers** Personal data leaves the Union only on an adequacy decision, appropriate safeguards or a listed derogation (Articles 44 to 49).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports GDPR

Records of Processing

Keep a record of each processing activity with purpose, categories, recipients, transfers and retention (Article 30).

Lawful Basis and Consent Register

Record the Article 6 basis, any Article 9 condition and consent evidence for each purpose (Articles 6, 7 and 9).

Rights Request Workflow

Run access, erasure and other requests with the one-month deadline, identity checks and an audit trail (Articles 12 to 22).

Impact Assessment Tracker

Hold DPIAs, risk ratings, mitigation actions and prior consultation records (Articles 35 and 36).

Breach Notification Workflow

Time each breach against the 72-hour rule and record notices to the authority and affected people (Articles 33 and 34).

Processor and Transfer Oversight

Track processor contracts, sub-processors and the transfer mechanism for each flow outside the Union (Articles 28 and 44 to 49).

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

Who must comply with the GDPR?

Controllers and processors established in the Union, and those outside it that offer goods or services to people in the Union or monitor their behavior there (Article 3). It covers the processing of personal data by automated means and non-automated processing in a filing system (Article 2).

What are the six lawful bases for processing?

Consent, contract, legal obligation, vital interests, public task and legitimate interests (Article 6(1)). Special categories of data need an additional condition under Article 9.

How quickly must a data breach be reported?

The controller notifies the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of a breach that is likely to result in a risk to people's rights and freedoms (Article 33). People are told without undue delay when the risk is high (Article 34).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How long does a controller have to answer a rights request?

One month from receipt, which can be extended by two further months for complex or numerous requests with notice to the person (Article 12(3)). Information is provided free of charge in principle.

What are the maximum fines?

Up to EUR 20 million or 4 percent of total worldwide annual turnover, whichever is higher, for infringements of the principles, data subject rights, transfer rules and orders. Up to EUR 10 million or 2 percent applies to other listed provisions such as controller and processor duties (Article 83(4) to (6)).

License included / downloadable: Yes The Regulation is EU law published in the Official Journal and is included with the platform for reference.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.