edgeGRC

Guide | European Union

EU GDPR: practical compliance guide

The core obligations of the General Data Protection Regulation, organised as the work a privacy team actually does: principles, lawful bases, rights, records, assessments, processors, transfers and accountability.

Last reviewed: 27 November 2026

General information only. Not legal advice, a legal opinion or a certification of compliance.

1 At a glance

The General Data Protection Regulation (Regulation (EU) 2016/679, the GDPR) has applied across the European Union since 25 May 2018, and in the wider European Economic Area. It is enforced by national supervisory authorities, coordinated through the European Data Protection Board (EDPB).

Proposed changes: the "Digital Omnibus"

In November 2025 the European Commission proposed targeted amendments to the GDPR as part of a wider digital simplification package. At the review date of this guide, the proposal was still going through the legislative process. The Council had agreed a negotiating position, but the European Parliament had not adopted its position. **None of the proposed GDPR changes apply yet.** Plan against the current text and watch the final outcome.

2 Scope

- **Material scope:** processing of personal data wholly or partly by automated means, and manual processing of data that forms part of a filing system.
- **Territorial scope (Article 3):** organisations established in the EU, whether or not processing happens in the EU. It also covers organisations outside the EU that offer goods or services to individuals in the EU, or monitor their behaviour in the EU.
- Non-EU organisations caught by Article 3(2) generally need to appoint a **representative in the EU** (Article 27).

Roles

Role	What it means in practice
Controller	Decides why and how personal data is processed, and carries primary responsibility.
Joint controllers	Decide purposes and means together, and must agree a transparent arrangement on responsibilities (Article 26).
Processor	Processes on behalf of a controller, under a contract with mandatory terms (Article 28).

3 The principles (Article 5)

Principle	Question to ask
Lawfulness, fairness and transparency	Do we have a lawful basis, and have we told people clearly what we do?
Purpose limitation	Are purposes specified up front, and is any further use compatible with them?

Principle	Question to ask
Data minimisation	Do we collect only what is adequate, relevant and necessary?
Accuracy	Can we keep data up to date and correct errors?
Storage limitation	Do we have retention periods and actually delete or anonymise?
Integrity and confidentiality	Are security measures appropriate to the risk?
Accountability	Can we **demonstrate** compliance with all of the above?

Accountability is the principle that shapes the whole programme. The GDPR expects documented decisions, policies, records and evidence, not only good intentions.

4 Lawful bases (Article 6)

Every processing activity needs one of six lawful bases, chosen and documented before processing starts:

1. **Consent:** freely given, specific, informed and unambiguous, and as easy to withdraw as to give.
2. **Contract:** necessary to perform a contract with the individual, or to take steps at their request before entering one.
3. **Legal obligation:** necessary to comply with EU or Member State law.
4. **Vital interests:** necessary to protect someone's life.
5. **Public task:** necessary for a task in the public interest or official authority.
6. **Legitimate interests:** necessary for legitimate interests, unless overridden by the individual's interests or rights. Record the balancing assessment.

Special category data (Article 9) needs a lawful basis *and* one of the Article 9 conditions. This covers health, genetic and biometric data used for identification, racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sex life or sexual orientation. Data about criminal convictions and offences has its own rules (Article 10).

5 Transparency and individuals' rights

Individuals must receive concise, intelligible information about the processing (Articles 13 and 14). This includes the controller's identity, purposes and lawful bases, recipients, transfers, retention, rights and the right to complain to a supervisory authority.

Right	Article	Note
Access	15	A copy of the data and supporting information.
Rectification	16	Correct inaccurate or complete incomplete data.
Erasure	17	Applies in defined circumstances; not absolute.

Right	Article	Note
Restriction	18	Limit processing while a dispute is resolved.
Data portability	20	For data provided by the individual, processed by automated means on consent or contract.
Objection	21	Including an absolute right to object to direct marketing.
Automated decisions	22	Safeguards against solely automated decisions with legal or similarly significant effects.

Timing: respond without undue delay and within **one month**. You can extend by two further months for complex or numerous requests, if you tell the individual within the first month.

6 Records, security and breaches

Records of processing activities (Article 30)

Controllers and processors must keep written records of processing. For controllers these cover the purposes, the categories of individuals and data, recipients, transfers, retention periods and a general description of security measures. A limited exemption exists for organisations with fewer than 250 employees, but it does not cover processing that is regular, risky or involves special category data. In practice most organisations keep records.

Security (Article 32)

Measures must be appropriate to the risk. Take into account the state of the art, costs, and the nature, scope, context and purposes of processing. Examples named in the Regulation include pseudonymisation and encryption, ongoing confidentiality, integrity and resilience, timely restoration after an incident, and regular testing.

Personal data breaches (Articles 33 and 34)

- Notify the competent supervisory authority **without undue delay and, where feasible, within 72 hours** of becoming aware. This is required unless the breach is unlikely to result in a risk to individuals.
- Tell affected individuals without undue delay when the breach is likely to result in a **high risk** to them.
- Document every breach, including those you do not notify: the facts, effects and remedial action.
- Processors must notify their controller without undue delay.

7 Assessments, DPOs and privacy by design

- **Data protection by design and by default (Article 25):** build data protection into systems and processes from the start, and default to the minimum data necessary.
- **Data protection impact assessment (Article 35):** required before processing that is likely to result in a high risk. See our separate guide, *Running a DPIA from screening to sign-off*.

- **Prior consultation (Article 36):** consult the supervisory authority before processing if a DPIA shows high residual risk that you cannot mitigate.
- **Data Protection Officer (Articles 37 to 39):** mandatory for public authorities, and for organisations whose core activities involve large-scale regular and systematic monitoring, or large-scale processing of special category or criminal offence data. The DPO must be independent, adequately resourced and involved in all data protection issues.

8 Processors

Use only processors that provide sufficient guarantees. The Article 28 contract must cover, among other things:

- processing only on documented instructions;
- confidentiality of people authorised to process;
- appropriate security;
- conditions for engaging sub-processors (prior authorisation, with flow-down of obligations);
- assistance with rights requests, security, breaches and DPIAs;
- deletion or return of data at the end of the service;
- audits and information to demonstrate compliance.

9 International transfers (Chapter V)

Transfers of personal data to countries outside the EEA need one of the following:

1. an **adequacy decision** by the European Commission for the destination;
2. **appropriate safeguards**, most commonly the Commission's Standard Contractual Clauses, or Binding Corporate Rules for intra-group transfers;
3. a **derogation** for specific situations (Article 49), interpreted narrowly.

When relying on safeguards such as Standard Contractual Clauses, regulators expect you to assess whether the law and practice of the destination country could undermine them. Add supplementary measures where needed, following the EDPB's recommendations on supplementary measures.

10 Enforcement

Supervisory authorities have investigative and corrective powers, including orders to stop processing. Administrative fines (Article 83) have two tiers:

Tier	Maximum	Examples
Lower	€10 million or 2% of total worldwide annual turnover, whichever is higher	Obligations of controllers and processors such as records, security, breach notification, DPIAs and DPOs.
Higher	€20 million or 4% of total worldwide annual turnover, whichever is higher	Principles, lawful bases, consent conditions, special category data, individuals' rights and transfers.

Individuals can also complain to a supervisory authority and seek compensation for material or non-material damage (Article 82).

11 Programme checklist

Foundations

- [ ] Confirm which entities are in scope under Article 3, and appoint an EU representative if needed.
- [ ] Decide whether a DPO is mandatory; if appointing one voluntarily, the same rules apply.
- [ ] Assign owners for each processing activity and a route for decisions to senior management.

Records and lawful bases

- [ ] Maintain the Article 30 record, and keep it current when systems, vendors or purposes change.
- [ ] Document the lawful basis for each purpose, plus the Article 9 condition and a legitimate interests assessment where relevant.
- [ ] Set and apply retention periods.

People-facing processes

- [ ] Publish clear privacy information at the points where data is collected.
- [ ] Run a rights-request process that meets the one-month deadline, with identity checks proportionate to the risk.

Risk and third parties

- [ ] Screen new or changed processing for DPIA requirements, and complete DPIAs before launch.
- [ ] Hold Article 28 contracts with every processor, and track sub-processor changes.
- [ ] Map international transfers, the transfer mechanism for each, and any transfer assessments.

Security and incidents

- [ ] Align security measures to risk, and test them regularly.
- [ ] Keep a breach log and a tested process for the 72-hour notification window.

Accountability

- [ ] Keep policies, training records, assessments and approvals as evidence you can produce to a regulator.
- [ ] Review the programme at least annually, and when the law or guidance changes.

12 Official sources

- Regulation (EU) 2016/679 (General Data Protection Regulation): EUR-Lex, eur-lex.europa.eu/eli/reg/2016/679/oj
- European Data Protection Board guidelines and recommendations: edpb.europa.eu
- European Commission, data protection and adequacy decisions: commission.europa.eu

About this guide

This guide summarises publicly available legislation and regulator guidance in our own words, as of the review date above. Laws, rules and regulator guidance change; always check the current official text and obtain advice appropriate to your organisation's circumstances.

EdgeGRC and Cyber Intelligence Private Limited is an Indian technology company focused on developing software platforms for enterprise privacy management and AI governance. Questions about this guide: **info@edgegrc.com** · edgegrc.com