G

# GDPR: Principles, Rights, Roles, and Breach Duties

The GDPR governs processing of personal data in the EU and EEA. Learn its principles, lawful bases, individual rights, roles, and breach duties.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

## In this guide

01 What does the GDPR cover?

02 The seven GDPR principles

03 Lawful bases: consent is only one

04 Controller, processor, and data protection officer

05 Rights of individuals

06 Personal data breach duties

07 Practical compliance checklist

**Quick answer:** The General Data Protection Regulation (GDPR) is the EU law governing the processing of personal data. It requires a lawful, fair, transparent, and accountable purpose for processing—not consent in every case—and gives individuals enforceable rights. Organizations must know their role, minimize data, secure it, document decisions,

and assess personal data breaches promptly.

*This article is a general explanation, not legal advice. Apply the regulation and national rules to the facts of your organization.*

## 01 What does the GDPR cover?

The GDPR applies to processing of personal data: information relating to an identified or identifiable person. It covers automated processing and many structured manual records. Examples include names, identifiers, location data, online identifiers, employee files, customer records, and data that identifies a person when combined with other information.

It applies to organizations established in the European Economic Area and can also apply outside it when an organization offers goods or services to people in the EU or monitors their behavior there. Pseudonymized data remains personal data when it can be linked back with additional information. Truly anonymous data falls outside the GDPR, but anonymization must be effective, not merely the removal of names.

## 02 The seven GDPR principles

- **Lawfulness, fairness, and transparency:** have a valid basis and explain processing clearly.
- **Purpose limitation:** collect data for specified, explicit, and legitimate purposes.
- **Data minimization:** use only what is adequate, relevant, and necessary.
- **Accuracy:** keep personal data accurate and correct errors.
- **Storage limitation:** retain identifiable data no longer than needed.
- **Integrity and confidentiality:** use appropriate technical and organizational security measures.
- **Accountability:** comply and be able to demonstrate compliance.

## 03 Lawful bases: consent is only one

Processing needs a lawful basis. The six bases are consent, contract, legal obligation, vital interests, public task, and legitimate interests. The correct basis depends on the purpose and relationship; an organization should not choose consent merely because it seems convenient. Valid consent must be freely given, specific, informed, unambiguous, and as easy to withdraw as to give. Additional conditions apply to special-category data.

## 04 Controller, processor, and data protection officer

A controller determines why and how personal data is processed. A processor handles data on the controller's behalf under documented instructions. Joint controllers determine purposes and means together. Contracts, security responsibilities, assistance with rights requests, and subprocessors should reflect the real arrangement, not just a label.

A data protection officer is required in certain cases, including some public-authority processing and certain large-scale regular monitoring or processing of special-category data. Not every business must appoint one, although assigning clear privacy responsibility remains important.

## 05 Rights of individuals

Depending on the circumstances and lawful basis, people may have rights to information, access, rectification, erasure, restriction, data portability, objection, and safeguards concerning solely automated decisions. These rights are not absolute in every case. Organizations need an identity-verification and response process that does not collect excessive new data or disclose someone else's information.

## 06 Personal data breach duties

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. It therefore includes some availability and integrity incidents, not only theft.

The controller must document breaches and assess risk to people's rights and freedoms. If a breach is likely to create such a risk, the controller must notify the competent supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware. If the risk is high, affected individuals may also need clear communication without undue delay. These are risk-based duties: “72 hours” is not a rule that every security event must be publicly announced.

## 07 Practical compliance checklist

1. Map personal data, purposes, systems, recipients, locations, retention, and lawful bases.
2. Provide concise privacy information and maintain records of processing where required.
3. Minimize collection and access; set and enforce retention and deletion schedules.
4. Use risk-appropriate security, privacy by design and by default, vendor controls, and staff training.
5. Prepare procedures for rights requests, incidents, breach assessment, and regulatory notification.
6. Assess high-risk processing with a data protection impact assessment when required.
7. Use an appropriate legal mechanism and safeguards for restricted international transfers.


**NEED MORE HELP?**

### We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

**Open this guide online at support.gridinsoft.com**