ORRADATA

# European Union's General Data Protection Regulation (GDPR)

**Simplified Explanation**

A concise overview of principles, rights, and compliance requirements

www.orradata.com

**Summary:**

The **General Data Protection Regulation (GDPR)** is a comprehensive privacy and security law passed by the European Union (EU) that imposes strict obligations on organizations anywhere in the world, so long as they target or collect data related to people in the EU. Enforceable since **May 25, 2018**, the regulation fundamentally shifted the ownership of personal data back to the individual (the "data subject"), granting them expansive rights such as the right to access, correct, and erase their data ("the right to be forgotten"). It mandates that organizations process data lawfully, transparently, and with specific purpose limitation, backed by a severe penalty structure where non-compliance can result in fines of up to **€20 million or 4% of global annual turnover**, establishing it as the global "gold standard" for data protection legislation.

## 1. Purpose and Scope (Articles 1–3)

- **What it does:** Sets rules for how personal data of people in the EU (and EEA) must be collected, stored, and used.
- **Who it applies to:**
  - Any organization inside the EU that processes personal data.
  - Organizations outside the EU if they offer goods/services to, or monitor, people in the EU.
- **Goal:** Protect individuals' fundamental rights and freedoms, particularly their right to privacy.

## 2. Key Definitions (Article 4)

- **Personal data:** Any information that can identify a person (e.g., name, email, ID number, location, IP address).
- **Processing:** Any action performed on data (collecting, storing, using, sharing, deleting, etc.).
- **Controller:** The entity that decides why and how personal data is processed.
- **Processor:** A party that processes data on behalf of a controller.

## 3. Main Principles (Article 5)

Organizations must process personal data in line with these principles:

1. **Lawfulness, fairness, transparency:** Data must be processed legally, fairly, and clearly explained to people.
2. **Purpose limitation:** Use data only for specific, stated purposes.
3. **Data minimization:** Collect only what is necessary.
4. **Accuracy:** Keep data correct and up to date.
5. **Storage limitation:** Do not keep data longer than needed.
6. **Integrity and confidentiality:** Protect data against unauthorized access, loss, or damage.
7. **Accountability:** Organizations must be able to prove compliance.

## 4. Legal Bases for Processing (Article 6)

To process personal data, organizations must have a valid reason, such as:

- Consent of the individual.
- Contract performance.
- Legal obligation.
- Protection of someone's vital interests (e.g., emergencies).
- Public interest or official authority tasks.
- Legitimate interests (if they do not override individuals' rights).

## 5. Special Categories of Data (Article 9)

Certain types of personal data (e.g., health, biometric, racial/ethnic origin, political opinions, religious beliefs) require extra protection and can only be processed in limited circumstances (e.g., explicit consent, public health reasons).

## 6. Rights of Individuals (Articles 12–23)

People (data subjects) have:

- **Right to be informed:** Know what is done with their data.
- **Right of access:** Request a copy of their data.
- **Right to rectification:** Correct inaccurate data.
- **Right to erasure ("right to be forgotten"):** Ask for data deletion under certain conditions.
- **Right to restrict processing:** Temporarily limit use of their data.
- **Right to data portability:** Receive their data in a usable format or transfer it to another provider.
- **Right to object:** Stop processing for marketing or certain other reasons.
- **Rights related to automated decision-making:** Protection against decisions made solely by algorithms that have legal or significant effects.

## 7. Accountability & Compliance (Articles 24–43)

Organizations must:

- Implement **appropriate technical and organizational measures** to ensure compliance.
- Maintain documentation on data processing activities.
- Conduct **Data Protection Impact Assessments (DPIAs)** when high risks are involved.
- Appoint a **Data Protection Officer (DPO)** in some cases (e.g., public bodies, large-scale monitoring, special data).
- Ensure processors follow GDPR rules through binding contracts.
- Notify **supervisory authorities** (within 72 hours) and individuals (when necessary) about personal data breaches.

## 8. Transfers Outside the EU (Chapter V)

Personal data can leave the EU only if:

- The destination country has an **adequacy decision** by the European Commission.
- Or appropriate safeguards exist (e.g., Standard Contractual Clauses, Binding Corporate Rules).
- Or specific exceptions apply (e.g., explicit consent).

## 9. Enforcement and Penalties (Articles 77–84)

- Individuals can file complaints with their national data protection authority.
- Supervisory authorities can investigate, order compliance, and impose fines.
- **Fines:**
    - Up to **€20 million or 4% of global annual turnover**, whichever is higher, for serious violations.
    - Lower tier fines for less serious breaches.

## 10. Key Bodies

- **Supervisory Authorities:** National agencies that enforce GDPR.
- **European Data Protection Board (EDPB):** Ensures consistent application across the EU.

## 11. Why does GDRP matter?

### For Individuals (Data Subjects)

- **Greater control:** People have the legal right to know who is collecting their data, why, and how it's used—and they can demand corrections, deletions, or stop certain uses.
- **Stronger privacy protections:** Companies must implement strict safeguards to prevent misuse, breaches, or unauthorized sharing of personal data.
- **Transparency:** Individuals get clearer information about data practices, reducing hidden or exploitative tracking.

### For Organizations

- **Legal obligation:** Any business operating in or targeting the EU must comply—or face significant penalties.
- **Global standard:** GDPR has influenced privacy laws worldwide (e.g., Brazil's LGPD, California's CCPA), making it a benchmark for best practices.
- **Reputation and trust:** Compliance can build customer confidence, which is increasingly important in data-driven markets.

## For Society and Markets

- **Prevents abuse:** Reduces the risk of large-scale data exploitation, identity theft, and surveillance misuse.
- **Creates uniform rules:** Harmonizes data protection laws across EU member states, simplifying cross-border business operations.
- **Drives better security:** Forces organizations to adopt higher cybersecurity standards, indirectly protecting critical infrastructure.

***Disclaimer:***
*This document is provided for general informational purposes only. It offers a simplified overview of the General Data Protection Regulation (Regulation (EU) 2016/679) and does not constitute legal advice. Organizations and individuals should consult official regulatory texts or seek professional legal counsel for advice regarding their particular obligations under the GDPR.*