Summary of the General Data Protection Regulation (EU 2016/679)

Abdellahi El Moustapha

March 31, 2025

Introduction

The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union that took effect on May 25, 2018, replacing the 1995 Data Protection Directive. GDPR applies globally to organizations that process personal data of individuals in the EU. It strengthens privacy rights and imposes strict obligations on data controllers and processors, with significant penalties for non-compliance. Key actors under GDPR include data subjects (individuals), data controllers (entities determining purposes and means of processing personal data), data processors (entities processing data on behalf of a controller), and supervisory authorities (national regulators enforcing GDPR).

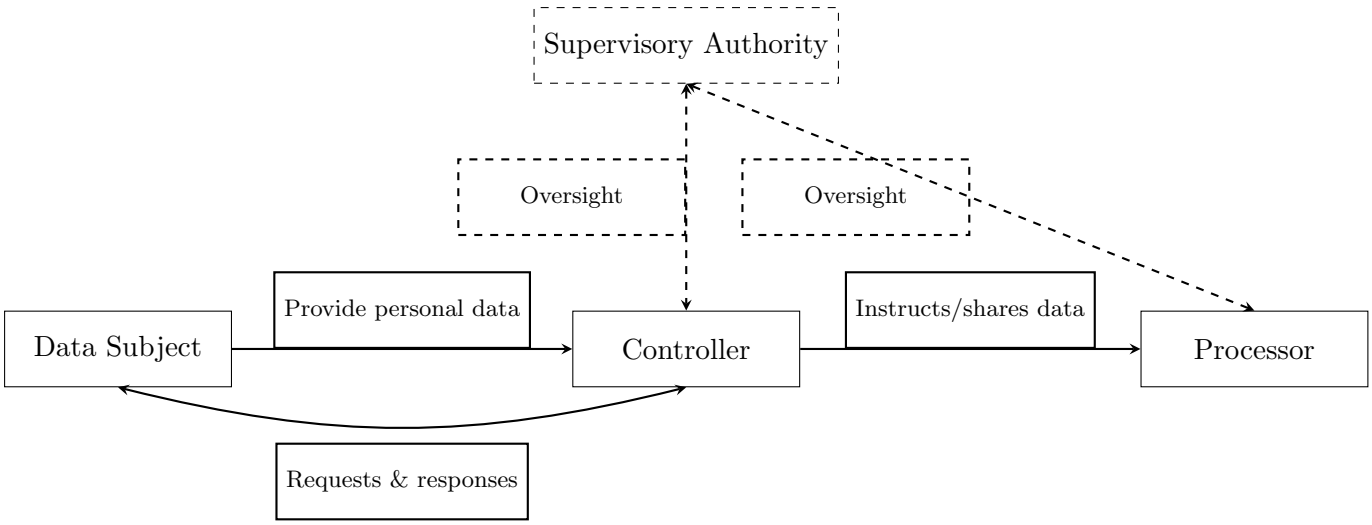

Figure 1: Key GDPR roles and interactions. Data flows from the data subject to the controller (which may engage a processor). The supervisory authority oversees compliance. Data subjects exercise rights with controllers.

Principles

GDPR Article 5 outlines core data protection principles that govern all personal data processing:

Lawfulness, Fairness & Transparency: Process data lawfully (on a valid legal basis), fairly, and transparently, with clear information provided to the data subject.

Purpose Limitation: Collect data for specific, explicit and legitimate purposes and do not further process it in ways incompatible with those purposes.

Data Minimization: Only process personal data that is adequate, relevant, and necessary for the stated purposes.

Accuracy: Keep personal data accurate and up to date. Inaccurate data should be corrected or deleted without delay.

Storage Limitation: Do not keep personal data (in identifiable form) longer than necessary for the purposes. (Longer retention is allowed only for specific purposes like archiving in the public interest, with safeguards.)

Integrity & Confidentiality: Ensure appropriate security of personal data, protecting against unauthorized processing or accidental loss, destruction, or damage.

Accountability: The controller is responsible for compliance with all these principles and must be able to demonstrate such compliance.

Legal Bases for Processing

Under GDPR, processing of personal data is lawful only if at least one of the following applies: (Note: Additional conditions apply for special categories of data, such as health or religious

Legal Basis	Description
Consent	Data subject has given clear, explicit consent for processing a specific purpose.
Contract	Necessary to perform a contract with the data subject, or to take steps at the data subject's request before entering a contract.
Legal Obligation	Necessary to comply with a legal obligation to which the controller is subject.
Vital Interests	Necessary to protect an individual's life or vital interests.
Public Interest	Necessary for a task in the public interest or under official authority.
Legitimate Interests	Necessary for the legitimate interests of the controller or a third party, unless overridden by the data subject's interests or fundamental rights (especially for children).

Table 1: Legal Bases for Processing (GDPR Article 6).

data, under Article 9, generally requiring explicit consent or other specific justifications.)

Data Subject Rights

GDPR grants individuals several rights over their personal data (Articles 12–22):

Right to be Informed: Individuals have the right to clear information about who is processing their data, what data, and why (typically provided via privacy notices).

Right of Access: Individuals can request access to their personal data held by a controller and obtain a copy, along with relevant details on how it is used.

Right to Rectification: Individuals can have inaccurate personal data corrected or incomplete data completed.

Right to Erasure: Individuals can request deletion of their personal data in certain cases ("right to be forgotten"), e.g. when data is no longer needed or was processed unlawfully.

Right to Restrict Processing: Individuals can request that their data be stored but not otherwise processed in certain circumstances (for example, during a dispute over data accuracy).

Right to Data Portability: Individuals can receive their personal data in a structured, commonly used, machine-readable format and have the right to transmit that data to another controller where technically feasible (applies to data processed by consent or contract).

Right to Object: Individuals can object to certain processing. They have an absolute right to object to direct marketing; otherwise, processing must stop unless the controller demonstrates compelling legitimate grounds.

Automated Decision-Making: Individuals have the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects, except in limited cases allowed by law. They are entitled to human review or other safeguards for such decisions.

Controllers must facilitate these rights and respond to requests within one month (extendable to two months for complex cases).

Controller and Processor Responsibilities

GDPR imposes detailed obligations on both data controllers and data processors to ensure accountability and security in data handling.

Controller Responsibilities

- **Accountability:** Implement appropriate technical and organizational measures to ensure and demonstrate GDPR compliance (Article 24). This includes keeping documentation (records of processing activities, Article 30) and performing internal audits.
- **Data Protection by Design & Default:** Integrate data protection principles into processing activities and systems from the start, and ensure default settings are privacy-friendly (Article 25).
- **Contracts with Processors:** Use only processors that provide sufficient guarantees of compliance, and have a binding contract or Data Processing Agreement in place outlining the processor's obligations (Article 28).
- **Security:** Ensure appropriate data security (confidentiality, integrity, availability) through technical and organizational measures (Article 32), e.g. encryption, access controls, and staff training.
- **Breach Notification:** If a personal data breach occurs, notify the supervisory authority within 72 hours of becoming aware (Article 33). If the breach likely poses a high risk to individuals, also inform affected data subjects without undue delay (Article 34).
- **Data Protection Impact Assessment:** Conduct Data Protection Impact Assessments (DPIAs) for processing likely to result in high risk to individuals' rights (Article 35), such as large-scale use of sensitive data or systematic monitoring.
- **Data Protection Officer (DPO):** Appoint a DPO if required by law (Article 37) — for example, public authorities or organizations engaging in large-scale monitoring of sensitive data. The DPO advises on compliance and serves as a liaison to regulators.

Processor Responsibilities

- **Act Only on Instructions:** Process personal data only on the documented instructions of the controller (Article 29), and assist the controller in meeting GDPR obligations.
- **Security Measures:** Implement appropriate security measures and maintain confidentiality. Processors are directly obligated to ensure data security (Article 32) through measures like staff training and access controls.
- **Breach Reporting:** Inform the controller without undue delay after becoming aware of a data breach (Article 33(2)), so the controller can fulfill notification duties.
- **Sub-processor Approval:** Do not engage sub-processors without the controller's prior authorization, and ensure any approved sub-processor is bound by the same data protection obligations (Article 28).
- **Record-Keeping:** Maintain records of processing activities carried out on behalf of each controller (Article 30), and cooperate with supervisory authorities as needed.

Governance and Oversight

GDPR establishes a regulatory framework to monitor and enforce compliance:

- **Supervisory Authorities (SAs):** Each EU Member State has an independent data protection authority responsible for enforcing GDPR, handling complaints, and providing guidance. SAs have investigative and corrective powers (audits, warnings, orders, fines).
- **Cooperation and Consistency:** For cross-border processing (affecting data subjects in multiple countries), the "one-stop-shop" mechanism designates a lead supervisory authority (usually where the controller's main EU establishment is located) to coordinate enforcement with other concerned SAs. National authorities cooperate through mutual assistance and joint operations for consistent GDPR application.
- **European Data Protection Board (EDPB):** The EDPB, composed of representatives of all SAs and the European Data Protection Supervisor (EDPS), ensures consistent application of GDPR across the EU. It issues guidelines, recommendations, and binding decisions to resolve disputes between SAs.

Organizations may also adopt approved **Codes of Conduct** or **Certification mechanisms** (Articles 40–42) to help demonstrate compliance, under oversight by SAs or accredited bodies.

International Data Transfers

Chapter V of the GDPR regulates transfers of personal data to countries outside the European Economic Area (EEA):

- **Adequacy Decisions:** Transfers can occur to third countries or international organizations that the European Commission has deemed to have an "adequate" level of data protection. Examples include countries like Japan, Switzerland, and others with adequacy findings.
- **Appropriate Safeguards:** Without an adequacy decision, transfers are allowed if the controller or processor ensures appropriate safeguards. Key safeguards include Standard Contractual Clauses (SCCs) adopted by the Commission, Binding Corporate Rules (BCRs) for intra-group transfers, or approved codes of conduct/certification with binding

commitments. (These mechanisms typically require additional measures after the Schrems II ruling to ensure effectiveness.)

- **Derogations:** GDPR provides narrow exceptions for specific situations, such as explicit consent of the data subject for the transfer, transfers necessary to perform a contract with or in the interest of the data subject, important reasons of public interest, establishment or exercise of legal claims, or to protect vital interests when the person cannot consent.

Penalties and Enforcement

GDPR enforcement is backed by significant penalties and remedies:

- **Administrative Fines:** Regulators can impose fines up to **€20 million** or **4% of worldwide annual turnover** of the prior financial year, whichever is higher, for the most serious violations. Lesser violations can incur fines up to **€10 million** or **2% of global turnover** (Article 83).
- **Corrective Actions:** Supervisory authorities can issue warnings, reprimands, and orders to bring processing into compliance (e.g. order data deletion or suspend data flows), in addition to or instead of fines.
- **Liability and Compensation:** Data subjects have the right to claim compensation for material or non-material damage resulting from GDPR violations (Article 82). Controllers or processors in breach may be liable for those damages.
- **Criminal Penalties:** Member States may enact additional criminal penalties for certain GDPR infringements (Article 84), and related laws (like ePrivacy rules) can also impose further sanctions.