Data Protection and Privacy Laws

Data Security and Privacy @ uninsubria

Roberto Vicario

2024/2025

Contents

1 EU Legislations

The concept of *privacy* in the European Union emerged with Article 8 of the European Convention on Human Rights (1950), which affirms the right to respect for private and family life. Any interference by public authorities must be lawful and necessary in a democratic society.

1.1 Data Protection Directive (1995)

> **Definition:** *Directive 95/46/CE* was introduced in 1995 to regulate the processing of personal data across EU member states.

- Enforced in national laws by 1998 (e.g., Italy: 1996).
- Emphasized **ownership of personal data** by individuals, not by data controllers.

1.1.1 Key Concepts

Term	Description
Personal Data	Any information that identifies an individual.
Sensitive Data	Includes health, political opinions, religious beliefs, etc.
Consent	Required for data processing and disclosure.
Purpose Limitation	Data must only be used for stated purposes.
Data Subject Rights	Individuals can access and correct their data.

1.2 Italian Data Protection Code

> **Enacted:** *January 1, 2004* — unified existing privacy regulations.

- **Art. 1**: Recognizes the right to personal data protection.
- **Art. 2**: Requires that processing respects freedoms and dignity.
- Introduced the principle of **Data Minimization**: use anonymous data when possible.

1.3 General Data Protection Regulation (GDPR)

> **Effective Date:** *May 25, 2018* (Approved: April 14, 2016)

- Applies to any entity processing EU citizens' data, regardless of location.
- Replaced previous directive and harmonized EU-wide data protection.

1.3.1 Core Principles

Principle	Description
Lawfulness, Fairness & Transparency	Processing must be clear and legal.
Purpose Limitation	Data collected for specific purposes only.
Data Minimization	Only necessary data should be processed.
Accuracy	Data must be accurate and updated.
Storage Limitation	Retain data only as long as needed.
Integrity & Confidentiality	Secure data against unauthorized access.

1.3.2 Key Roles

Role	Description
Data Subject	The individual whose data is being processed.
Data Controller	Determines the purposes and means of processing.
Data Processor	Processes data on behalf of the controller.

1.3.3 Data Subject Rights

Right	Description
Access	Know what data is being processed.
Rectification	Correct inaccurate or incomplete data.
Erasure ("Right to be Forgotten")	Request deletion under specific conditions.
Portability	Transfer data to another service.

Right	Description
Restriction & Objection	Limit or oppose certain processing activities.

1.3.4 Transparency & Consent

- Consent must be **freely given**, **specific**, **informed**, and **unambiguous**.
- Controllers/processors must inform data subjects clearly about processing activities.

1.3.5 Privacy by Design & Default

> Organizations must integrate data protection into system design and default settings.

1.3.6 Data Protection Officer (DPO)

- Required for:
  - Public authorities.
  - Entities conducting large-scale monitoring.
  - Processors of sensitive data.

DPO Responsibilities
Monitor compliance with GDPR
Advise on data protection impact assessments
Liaise with regulatory authorities

1.3.7 Data Breach Notification

- Notify supervisory authority **within 72 hours** of detection.
- Inform data subjects **if high risk** to their rights is present.

1.3.8 Penalties

- Up to **4% of global annual turnover** for major violations.
- Both **controllers** and **processors** are liable.

2 US Legislations

Unlike the EU, the U.S. lacks a centralized privacy framework. Instead, laws are **sector-specific** and **fragmented**.

2.1 Key Federal Laws

Law	Scope
HIPAA	Protects medical information.
COPPA	Regulates data collection from children under 13.
GLBA	Requires financial institutions to disclose privacy practices.
Privacy Act	Governs data held by federal agencies.
FOIA	Allows public access to federal agency records, with exceptions.

- **Private sector data** is typically regulated through **contracts and privacy policies**.

2.2 EU–US Data Transfer Frameworks

2.2.1 Safe Harbor (2000–2015)

> Allowed U.S. companies to self-certify compliance with EU data standards.

Principles
Notice
Choice
Onward Transfer

Principles
Security
Data Integrity
Access
Enforcement

- Invalidated in **2015** by the Court of Justice of the EU (CJEU) due to U.S. surveillance concerns.

2.2.2 Privacy Shield (2016–2020)

> Replaced Safe Harbor; aimed to restore trust in transatlantic data flows.

- Also invalidated in **July 2020** (Schrems II decision).
- Main concerns: lack of protections against U.S. intelligence access (e.g., FISA, CLOUD Act).

2.2.3 Data Privacy Framework (DPF)

> **Announced:** March 2022 — **Effective:** July 2023

- Restricts U.S. government data access to what is **necessary** and **proportionate**.
- Introduces an **independent redress mechanism** for EU citizens.
