Law & Data

Davide Volpi

February 1, 2025

Contents

1 Introduction

1.1 What is Law

Is a **set of conditions** under which the **choices** of each **person** can be united with the choices of **others** under a universal law of **freedom**.

1.2 The Legal System

There is a plurality of legal systems and they include **rules, procedures and institutions** by which activities, both public and private, can be carried out through legitimate means. It is a system for **interpreting and enforcing the laws**.

1.2.1 Branches of Law

This branches are **fundamental**, **universally accepted** and **exhaustive**.

- **Public law:** public interests (citizen vs state).
- **Private law:** private purposes.

1.2.2 Type of State Legal Systems

The main difference is between:

- **Civil law:** written laws.
- **Common law:** judicial decisions.

1.3 Sources of Law

- **Hard law: Binding** legal provisions which can be legally enforced before court (Global convention of human rights).
- **Soft law:** Contents (agreements, principles, declarations, statements...) which are **not legally binding**, usually cannot be enforced by a party before a court, but can be used by a judge to interpret hard law.

There are some examples of sources of law such as conventions, legislation, case-law, public and private policies, doctrine, fundamental and general principles of law, customary law (overtime the law become binding).

1.3.1 Hierarchy of the Sources of Law

It can be seen as a reverse pyramid where the lower elements can't contradict the upper elements and the higher you go, the more the legal provisions are important and should be general. There is a different hierarchy for each legal system with different elements and principles.

1.4 Modern Theory of Separation Powers

In every legal system there are 3 main powers:

- **Legislative:** Make
- **Executive:** Implement and enforce
- **Judicial:** Interpret

Separate and independent bodies so to ensure legal certainly, impartiality, equality before the law.
There is a **System of Checks and Balances** (exercised by judges) to limit the power of a single individual/entity/body of government to ensure **balanced** and **harmonious** and **relationship** and **co-existence**.

2 The European Union

2.1 Different Organizations of the European Union

- **Council of Europe (CoE):** Continental level association with 46 states and his own institutions (the most important is the European Court of Human Rights).
- **European Free Trade Association (EFTA):** Regional trade organization with a free trade area (Iceland, Norway, Liechtenstein, Switzerland). Participation in the Schengen Area = no controls.
- **European Economic Area (EEA):** Between EU + EFTA - Switzerland. Defined by an international agreement within which the EU single market basic rules apply.

This organizations are involved when we talk about the personal data protection and GDPR.

2.2 A Case of Study for European Union

To EU citizens data apply GDPR also from non EU companies/states which want to manage that data. We can find two different cases of EU Law:

- *Costa vs ENEL:* The Community constitutes a **New Legal Order** of international law for the benefit of which the states have limited their sovereign rights.
  - **Violated Law:** Articles 102 and 93 of the Treaty of Rome, regarding anti-competitive practices and state aid
  - **Principle of Primacy of EU Law:** states that EU law cannot be overwritten by national provisions.
- *Van Gend en Loos:* Its own legal system which, on the entry into force of the Treaty, became an **integral part of the legal system of the Member States** and which their courts are bound to apply.
  - **Violated Law:** Article 12 of the Treaty of Rome, prohibiting customs duty increases.
  - **Principle of Direct Effect:** any natural/legal person could enforce the rights stemming from the EU legal system before national judges of the MS.

2.3 Application to EU Membership

- **ART. 2 TEU:** any European state which **respects the common values of the Member States** and undertake to promote them may apply to become a member of the Union. These **values** include **human dignity, freedom, democracy, equality, the rule of law and respect for human rights**, including the rights of persons belonging to minorities.
- **ART. 49 TEU:** The state **must respect the ART 2**. The European Parliament and national Parliaments shall be notified of this application. The applicant State shall **address its application to the Council**, which shall act unanimously after consulting the Commission and after receiving the consent of the European Parliament, which shall act by a majority of its component members. The conditions of eligibility agreed upon by the European Council shall be taken into account. The conditions of admission and the adjustments to the Treaties on which the Union is founded, which such admission entails, shall be the **subject of an agreement between the Member States and the applicant State**. This agreement shall be submitted for ratification (the state approve the international agreement by his own legal system) by all the contracting States in accordance with their respective constitutional requirements.

2.4 Copenaghen Criteria for EU Accession

- **Political:** stability of institutions guaranteeing democracy, the **rule of law, human rights** and respect for and protection of minorities.
- **Economic:** a functioning market economy and the capacity to cope with competition (aim to protect consumers rights → fundamental right) and market forces.
- **Administrative and institutional capacity:** to effectively implement the **acquis communautaire** and ability to take on the obligations of EU membership.

The Rule of Law

- **Law-Making process:** all public powers must act within the constrains set out by law. They must be transparent, accountable, democratic and pluralistic.
- **Judicial Protection:** Not only protection set by law but we need law enforced by judges. Must be effective → access to justice, independent and impartial courts, separation of powers.
- **Equal Protection:** everyone enjoys equal protection under the law and prevents the arbitrary use of power by governments.
- **Political and Civil Rights:** protection, grant and guarantee of basic political and civil rights, civil liberties.

Acquis Communautaire

Represents the body of common rights and obligations binding upon EU member states. We have both soft and hard law.

2.5 Hierarchy of Sources of European Union Law

It is always a reverse pyramid build as follow:

1. **Primary Law**
   - Treaties
   - Charter of Fundamentals Rights
   - General Principles of EU Law Established by the Court of Justice
2. **International Agreements**
3. **Secondary Law**
4. **Supplementary Law**

2.6 Primary Law

2.6.1 Treaties

- **Founding treaties:**
  1. **Treaty of Paris:** regulate the industrial production of coal and steal (Establishment of European Coal and Steal).
  2. **Treaty of Rome:** create a common market and custom unions, and to promote economic integration in Europe (European Economic community and European Atomic Energy Community).
  3. **Single European Act:** reform EU institutions and lay to the groundwork for the establishment of the Single Market.

4. **Maastricht Treaty:** formally establish the EU, introduce EU citizenship, and pave the way for the creation of the euro.
5. **Treaty of Amsterdam:** reform EU institutions, increase the role of the European Parliament, and enhance cooperation in foreign and security policy.
6. **Treaty of Nice:** reform the EU industrial structure in preparation for the enlargement.
7. **Treaty of Lisbon:** streamline EU governance, enhance the role of the EU Parliament, and create positions like the President of the EU Council.

- **Amending treaties**
- **Protocols annexed to treaties**
- **Accession treaties**

2.6.2 Treaty on the European Union (TEU)

States objectives and principles of the EU and also lists the institutions of the EU.

- **Art. 2:** The Union is founded on the values of respect for **the rule of law and respect for human rights, including the rights** of persons belonging to minorities. This values are common on the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.
- **Art. 3:** Set some objectives to be pursued by the EU members. Is divided in sections:
  1. Promote **peace**, its values and the **well-being of its peoples**.
  2. Ensure the **free movement of persons** (also free movement of data).
  3. Establish an **international market** for the **sustainable development** (the approach of fulfilling current needs without harming future generations' ability to meet theirs), protecting the **environment** and promote **scientific and technological advice**
  4. **Economic and monetary union** whose currency is euro.
  5. In its relations with the wider world, the Union shall **uphold and promote its values and interests** and contribute to the **protection of its citizens**.
  6. The Union shall pursue its objectives by **appropriate means** commensurate with the competences conferred upon it in the Treaties.

The **Brussels effect** is the process of unilateral regulatory globalization caused by the European Union who de facto externalizes its laws outside its borders through market mechanisms.

2.6.3 Treaty on the Functioning of the European Union (TFEU)

States the organizational part and the functional provisions to reach the EU objectives. Also states the procedures for the functioning of EU institutions.

- **Art. 16:** Everyone has the right to the **protection of personal data** concerning them.

2.6.4 EU Charter of Fundamental Rights (CFR)

After the Lisbon Treaty this Charter became hard law, with the same value as treaties.

- **Art. 6:** The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted at Strasburg, on 12 December 2007, which shall have the same legal value as the Treaties. Is divided in 7 chapters:
  1. **Dignity:** Human dignity is inviolable, must be respected and protected
  2. **Freedoms:** Respect for private and family life, protection of personal data.
  3. **Equality**
  4. **Solidarity**
  5. **Citizens' Rights**
  6. **Justice**
  7. **General Provisions:** includes a safeguard clause.

The Safeguard Clause

- **Art. 52(1) CFR:** Scope and interpretation of rights and principles. Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for law and respect the essence of those rights and freedoms. Subject to the **principle of proportionality**, limitations may be made only if they are **necessary and genuinely meet objectives of general interest** recognized by the Union or the need to protect the rights and freedoms of others.

2.6.5 General Principles of EU Law Established by the Court of Justice

Are legal principles developed by the Court of Justice over time. Is a no exhaustive list under constant development. Starting from constitutional traditions of EU Member States. The Art.6(3) TEU is an example.

2.7 Agreements

2.7.1 International Agreements

Are agreements concluded by the European Union and third countries within the sphere of competence of the EU.

- **Art. 216 TFEU:** The Union may conclude an agreement with one or more third countries or international organizations where the Treaties so provide or where the conclusion of an agreement is necessary **in order to achieve**, within the framework of the Union's policies, **one of the objectives referred to in the Treaties**, or is provided for in a legally binding Union act or is likely to affect common rules or alter their scope. Agreements concluded by the Union are binding upon the institutions of the Union and on its Member States.
- **Art. 217 TFEU:** The Union may conclude with one or more third countries or international organizations agreements **establishing an association involving reciprocal rights and obligation**s, common action and special procedure.
- **Art. 218 TFEU:** Procedure for negotiating and concluding international agreements, involving Council, European Parliament (possibly, the ECJ).

Some examples are:

- **Training cooperation agreement** between EU and UK) after the Brexit.
- **EU US PNR (passenger name records) agreement** between EU and US for the exchange of data of passengers in flights.
- **Sweeft agreement** between EU and US for the secure exchange of personal data.

2.8 Secondary Law

- **Typical Acts - Art. 288 TFEU**
  - **Regulations:** binding in its entirety and directly applicable in all Member States
  - **Directive:** binding as to the result to be achieved. The implementation in Member States is the choice of form and methods to achieve the result lies with the national authorities. Also the deadline is binding.
  - **Decisions:** binding in its entirely and is general/individual.
  - **Opinions and recommendations:** not binding.
- **Atypical Acts**
  - Communications, resolutions, white papers (report with detailed information), green papers (preliminary report) (soft law)

Examples of EU Secondary Legislation on Data

- **Directive 95/46/EC** on the protection of individuals with regard to the processing of personal data and on the free movement of such data - **Data Protection Directive**
- Regulation (EU) 2016/679 on the protection individuals with regard to the processing of personal data and on the free movement of those data, known as the GDPR - **General Data Protection Regulation**.
- **Directive (EU) 2016/680** on protecting individuals when personal data are used by law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties - **Data Protection Law Enforcement Directive**.
- **Regulation (EU) 2018/1725** laying down rules for protecting individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of those data.
- **Directive 2002/58/EC** on the processing of personal data and the protection of privacy in the electronic communications sector - **E-communications Directive**.
- **Regulation (EU) 2024/1689** of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence - **Artificial Intelligence Act**.

2.9 Institutions of the EU

Are established by the Art. 13 TEU :

2.9.1 European Parliament

Is composed of max 750 members(MEPs), has 5 years term and since 1979 is directly elected by EU citizens. These groups are formed according to affinities in political parties. Has a few **functions**:

- **Legislative:** one of the two legislative chambers of the EU.
- **Budgetary:** monitoring on the expenditures (not manage).
- **Supervisory:** on the activities of the other EU institutions (general reports):
  - Question the Commission
  - Investigate (temporary committees of inquiry)
  - Receive petitions by EU citizens
  - Election of Ombudsman (civil mediator)
- **Elective:** president of the EU commission (suggested by the Council) and EU commissioners (proposed by the Commission's President).

2.9.2 European Council

Composed by 27 Heads of State and Governments and the president is elected for a 2.5 years' term. It has no legislative function, but **guideline function:**

- Objectives in CFSP + EU external action.
- Abroad guidelines of economic policies.

It can intervene in some areas foreseen by treaties.

2.9.3 Council of the European Union

One representative for each MS, able to commit the government of that state and cast its vote and make the **interests of the governments**.

- **Different Configurations**: General affairs, FA, Economic and financial, Environment...
- **Legislative Function:** is the second legislative chamber with the European Parliament.
- **Supervisory Functions** on other institutions.

2.9.4 European Commission

Composed by 27 commissioners approved by the EP with a 5 years' term, but is **independent from the MS**, appointed with a procedure involving the EP, President of the Commission and MS.
Is divided into **Directorates General** and represents the **interests of the EU as a whole** all over the world. It has a few **functions**:

- **Legislative:** initiative.
- **Executive and Administrative:** enforcement of EU law.
- **Budgetary:** management of the EU budget.
- **Supervisory:** on MS (possible breaches of EU law) and on private entities (competition law).

2.9.5 European Court of Justice

Is composed by two courts: the **European Court of Justice** and the **General Court of the EU**. Is formed by **judges** and **advocates general** whose number depends on the number of MS. They have a 6 years' term, renewable every three years.
Appointed among individuals possessing qualifications required for appointment to the highest judicial offices in their respective countries or jureconsults of recognized competence but **independent from their MS**. They have a few **functions:**

- **Jurisdictional:** litigation → legal process of resolving disputes through the court system, involves one part suing another (is the only institution with this power).
- **Interpretative/Preliminary rulings:** not litigation → resolving disputes outside the court.
- **Advisory/Consultative:** not litigation.

Litigation Proceedings before the ECJ

There are three types of litigation:

- **Direct Appeals:** Art. 263 TFEU, appeal of acts adopted by EU institutions
  - **Public initiative:** MS, other EU institutions
  - **Private initiative:** any natural or legal person against an act addressed to that person or which is of direct and individual concern to them, and against a regulatory act which is of direct concern to them and does not entail implementing measures.
  - They have some vices such as lack of competence, invalidity, voidness, misuse of powers; they also have a time limit of 2 months and 10 days.
- **Failure to Act:** Art. 265 TFEU, is a pre-litigation, with a letter of formal notice, then have 2 moths for acting. This can lead to a **litigation before the ECJ**.
- **Compensation for Damages:** Art. 340(2) TFEU, initiative by individuals, legal persons, and MS. The damage must be proved as unlawful, serious and certain.

Non litigation Proceedings before the ECJ

- **Preliminary Rulings:** ECJ + General Court, Art. 267 TFEU
  - **Initiative:** by any jurisdiction of any MS.
  - **Object:**
    - **Interpretation** of any EU law provision.
    - **Validity** of acts of EU institutions.
  - **Development:**
    1. MS National proceedings.
    2. The national judges refer the preliminary rulings to the ECJ.
    3. (usually) Suspension of the national proceedings.
    4. ECJ decision (judgment / order) which is **compulsory** for the national judge.

2.9.6 European Central Bank

2.9.7 Court of Auditors

2.10 Bodies of the EU

2.10.1 European Data Protection Supervisor (EDPS)

Is the EU's independent body ensuring that EU institutions comply with data privacy laws. It supervises data processing, advises on privacy policies, and collaborates with EU data protection authorities for consistency.

2.10.2 European Data Protection Board (EDPB)

Is an independent body that ensures the consistent application of data protection rules throughout the EU, promoting cooperation between national data protection authorities in the EU.

2.10.3 Agencies of the European Commission

Decentralized bodies distinct from institutions with specific tasks (**fundamental rights agency**).

3 Privacy

3.1 What is Privacy

- **Negative:** need to prevent intrusions of private space.
- **Positive:** right to make free choices and to choose who to exclude from my personal space.

Is the most comprehensive of rights and the right most valued by civilized men: right to reputation, to honour and moral integrity, to one's own image, to private/family life, to non-interference personhood / protection of identity and dignity ...
Has an **origin in common law**, with a distinction between what is private from what is public.

- **Common Law Tradition:** created a definition of privacy which dealt with the right to liberty.
- **Civil Law Tradition:** privacy was rather meant from the origin as the right to dignity.

The **right to human dignity** is equal to saying that all the other rights are respected.
The **right of self-determination** is the ability to make their own choices and control aspects of their lives and futures without external interference. This includes making personal decisions, especially regarding one's body, identity, and personal information.

3.2 Right to Personal Data

- **Art. 8(1) CFR:** Everyone has the right to protect personal data concerning him or her.

We can define **personal data** as:

- **Art.4(1)(1) GDPR:** Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Has a **civil law origin**.

3.3 Right to Privacy and Personal Data

These are **human rights**, rights belonging to individuals as human beings regardless of race, sex, nationality, ethnicity, language, religion or any other status.

3.3.1 History of the Right to Privacy

UN Universal Declaration of Human Rights (1948)

- **Article 12:** No one shall be subjected to **arbitrary interference** with his privacy, family, home or correspondence, nor to attacks upon his **honour and reputation**. Everyone has the right to the protection of the law against such interference or attacks (in China, the right to personal data is not considered a right).

International Covenant on Civil and Political Rights (1966)

- **Article 17**

  1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
  2. Everyone has the right to the protection of the law against such interference or attacks.

UN Convention of the Rights of the Child (1989)

- **Article 16**
  - **No child** shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.
  - **The child** has the right to the protection of the law against such interference or attacks.

European Convention of Human Rights (1950)

- **Article 8 - Right to respect for private and family life**
  - Everyone has the right to respect for his private and family private life, his home and his correspondence.
  - **There shall be no interference by a public authority** with the exercise of this right **except** such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorders or crime, for the protection of health or morals, or for the protection of the right and freedom of others.

Nice Charter (2001) - EU Charter of Fundamental Rights (2009)

They are the same charter but the Nice Charter was based on soft law, than it becomes binding and becomes the EU Charter of Fundamental Rights, that has the same value of the fundamental treaties.

- **Article 7 - Respect for private and family life**
  - Everyone has the right to respect for his or her private and family life, home and communications.
  - **There shall be no interference by a public authority** with the exercise of this right **except** such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety of the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- **Article 8 - Protection of Personal Data**
  - Everyone has the right to protection of personal data concerning him or her.
  - Such data must be processed **fairly** for **specified purpose** and on the basis of the **consent** of the person concerned or some **other legitimate basis** laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it **rectified**.
  - Compliance with these rules shall be subject to control by an **independent authority**.
- **Article 52 - Scope and Interpretation**
  - **Any limitation** on the exercise of the rights and freedoms recognized by this Charter must be **proved for by law** and respect the essence at those rights and freedoms. Subject to the principle of **proportionality**, limitations may be made only if they are **necessary** and genuinely meet objectives of general interests recognized by the Union or the **need to protect the rights and freedoms of others**.
  - Rights recognized by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

3.4 Right to Personal Data Protection

- **OECD Privacy Guidelines (1980):** soft law universal standards. The main **principles** are:
  - **Collection Limitation Principle:** Limit personal data collection, ensure consent.
  - **Data Quality Principle:** Ensure accuracy, relevance, and timeliness of data.
  - **Purpose Specification Principle:** Specify data use purpose at collection.
  - **Use Limitation Principle:** Restrict use to specified, legitimate purposes.
  - **Security Safeguards Principle:** Protect data from unauthorized access or loss.
  - **Openness Principle:** Maintain transparency about data practices and policies.
  - **Individual Participation Principle:** Allow individuals to access and correct data.
  - **Accountability Principle:** Ensure compliance and responsibility for data practices.
- **CoE Convention 108 (28 January 1981 - Data Privacy Day):** convention for the protection of individuals with regard to automated processing of personal data. Was the first legally binding instrument at the international level on data protection. Set universal standards for processing data. The main **principles** are:
  - Protection of the individuals against PD abuses
  - Regulation of transborder data flows
  - Fair and lawful collection
  - Legitimate purposes
  - Processing for the same purposes for which data were collected
  - Storage duration (no longer than necessary)
  - Quality of data: adequate, relevant not excessive (proportionality)
  - Sensitive data (special categories of data)
  - Right to know information stored and to have it rectified
  - Possible overriding interests for different processing activities
- **CoE Convention 108+ (adopted on 18 May 2018):** upgrade of the convention 108. Set evolved standards in line with the technological events. GDPR are aligned with this convention.

3.4.1 Applicable EU Legislation (Primary Law)

- **TEU - Art.39:** In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the **Council** shall adopt a **decision laying down the rules** relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which **fall within the scope of this Chapter**, and the rules relating to the **free movement** of such data. Compliance with these rules shall be subject to the control of independent authorities.
- **TFEU - Art.16:**
  1. Everyone has the right to the protection of personal data concerning them.
  2. **The European Parliament and the Council**, acting in accordance with the ordinary legislative procedure, **shall lay down the rules** relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free **movement of such data**. Compliance with these rules shall be subject to the control of **independent authorities**.
  3. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

3.5 History of EU Data Protection Directives

- **Directive 1995/46/EC:** on the protection of individuals with regard to the process of personal data and on the free movement of such data. To give higher level of legislative harmonization was replaced by the GDPR.
- **Directive 2006/24/EC - Data Retention Directive:** on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (replaced in 2016 because it was rebuild by the ECJ in Digital Rights Ireland).
  - The Court of Justice of the European Union (CJEU) declared the Data Retention Directive invalid, ruling it violated fundamental rights to privacy and data protection. The directive required telecom companies to retain user metadata for potential law enforcement use. The court found it disproportionate, lacking safeguards against misuse and failing to limit retention to strictly necessary purposes. This decision marked a significant affirmation of privacy rights in the EU.

  Due to some public safety problems and for prevention of terrorist attacks, but his directive gave the chance to public authorities to abuse of their power

3.6 Applicable EU Data Protection Directives

3.6.1 Directive 2002/58/EC - E Privacy Directive

Directive on privacy and electronic communications. Aim to protect the private electronic life. Refers also to data in general, not only to personal data, but is really outdated.
The main subjects of this directive are:

- **User:** any natural person using a publicly available electronic communications service, for private or business purpose, without necessarily having subscribed to this service (**subscriber**).
- **Traffic Data:** any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.
- **Location Data:** any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.
- **Communication:** any information exchanged of conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communication network except to the extent that information can be related to the identifiable subscriber or user receiving the information.

Now we can define what are:

- **Scope of application:** services concerned are those involving in processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks within the EU.
- **Service Provider:** required to take appropriate technical (costs) and organizational measures (principle of proportion) to ensure security of its services.
- **Objectives:** require to ensure confidentiality of communications and related personal data processed through public communication networks/publicly available electronic communications services.

Some examples of this general principles are:

- **Automatic call forwarding** by third parties to the subscriber's terminal, unless stopped.
- **Directories of subscribers** possible, but based on consent.

- **Unsolicited communications** as automated calling systems without human intervention or fax or email or direct marketing is possible, but with clear, distinct and prior consent possibility to object free of charge and easily.

3.6.2 Directive 2016/680/EU - Data Protection Law Enforcement Directive

On the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
Repealing Council Framework Decision 2008/977/JHA. The main difference from the one of 2006 is that this directive sets the subjects (criminal offenders). Filled the void of Data Retention Directive.
Is adopted in parallel with GDPR, to a new **PDP (private data protection) Package**.
The underlying principles are:

- Data protection by design or by default
- Data security
- Data breach notifications
- Appointment of Data Protection Officers
- Emerging tech challenges
- **NO decisions based solely on automated processing (including profiling)** in principle
  - **MUST NO** be based on sensitive data.
  - **MUST NOT LEAD** to any discrimination against any person.

3.6.3 Directive 2018/1972 - European Electronic Communications Code

Is a recast directive for the no processing of personal data. Is an harmonised framework for the regulation of electronic communications networks, electronic communications services, associated facilities and services, and some aspects of the terminal equipment. Integrates and complements the E-Privacy Directive because it deals with specific electronic networks. The **goals** are:

- Implement an international market in electronic communications.
- Promote a fair competition between companies (competition law).
- Ensure equal and fair access to these services.
- Promote connectivity all across EU.

3.6.4 Regulation 2016/679/EU - General Data Protection Regulation

3.6.5 Regulation 2018/1725/EU

Setting forth the rules applicable to the processing of personal data by EU institutions, bodies, offices and agencies.

3.6.6 Digital Services Act - DSA

3.6.7 Digital Markets Act - DMA

3.6.8 Artificial Intelligence Act - IAA

4 General Data Protection Regulation

4.1 Data Subjects

Identified or identifiable person (individual) to which any information may relate. An individual because has the fundamental right of personal data protection. An individual is a data subject also when is possible to connect personal data indirectly.
A **consumer** is an individual who purchases goods or services for personal use, not for resale or business purposes. So, I could be a consumer and a data subject at the same time by the GDPR.
The **main rights** of the Data Subject are:

- **Right to transparency of communication:** Ensures clear and accessible information about data processing.
- **Right to be informed of purposes:** Guarantees knowledge of why personal data is being collected and used.
- **Right to access:** Allows individuals to view and obtain a copy of their personal data.
- **Right to rectification, erasure (right to be forgotten), restriction:** Permits correcting errors, deleting data, or limiting processing under specific conditions.
  - The **Google Spain v. AEPD and Mario Costeja González case (2014)** established the "right to be forgotten" in the European Union. The European Court of Justice ruled that individuals can request search engines like Google to remove links to personal information that is outdated, irrelevant, or excessive, provided it doesn't conflict with public interest. This landmark decision reinforced privacy rights under the EU Data Protection Directive (now GDPR) while balancing freedom of information.
- **Right to data portability:** Enables transfer of personal data between organizations in a usable format.
- **Right to object:** Allows individuals to oppose processing of their data, especially for marketing or profiling purposes.

4.2 Controller

Is the natural or legal person, public authority, agency or other body which, alone or jointly (joint controllers) with others, **determines the purpose and means** of the processing of personal data.
In case of joint controllers one controller must identify the other for his reliability. In every case the data subject must be protected by both the controllers.
A **processor** is an entity that processes personal data on behalf of a controller, following the controller's instructions, and is not responsible for determining the purposes or means of processing.
Data subject can make questions and receive answers to the controller.
Obligations of the Controller: as a general rule, it is responsible and liable for any processing of personal data carried by itself or on its behalf (article 38-GDPR).
The main obligations of the controller are:

- Adoption of appropriate technical and organizational measures (TOM's)
- Adopt additional protection policies
- Keep a record of processing activities (not mandatory only well recommended)
  - **Data Protection Management System (DPMS):** Is a risk-based internal compliance system, typically consisting in an IT security concept that introduces and monitors technical and organisational conduct of data processing activities, and records/documents processing activities to achieve compliance with the GDPR. The **aim** is to achieve compliance with GDPR, by adopting appropriate TOM's.
- Cooperation with Data Subjects
- Cooperation with Supervisor Authorities

4.3 Processor

Is a natural or legal person, public authority, agency or other body which **processes personal data** on behalf of the controller. As with the controllers, it's possible to have more than one processor, in that case you have **joint processors**, but if a processor delegate the work of processing data to another processor, you have a **subprocessor**.
The **processing of personal data** is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
The **main obligations** of the Processor are:

- Act upon instructions of the Controller: what and how to do with the personal data.
- Implement TOMs: has to deal with the ones selected by the Controller and can implement others.
- Appoint a Representative within the EU: if they are based outside the EU but process personal data of individuals in the EU, to ensure GDPR compliance and act as a contact point for authorities and data subjects.
- Maintain a record of processing activities (only well recommended, not mandatory).
- Cooperate with Supervisor Authorities
- Designate a Data Protection Officer (where required)

4.4 Contents of the Record

Controller:

- Keep record of name and contact details of the (joint) controller(s), the representative(s) and DPO(s).
- Purposes
- Description of the categories of data subjects and categories of personal data.
- Categories of recipients to whom personal data are or will be disclosed (including outside EU and/or international organisations)
- Transfer to third countries/international organisations and documentation of suitable safeguards.
- Envisaged time-limits for erasure of the different categories of data.
- General description of TOSMs.

Processor:

- Keep record of name and contact details of the processor(s) and (joint) controller(s), the representative(s) and DPO(s).
- The categories of processing.
- Transfer to third countries/international organisation and documentation of suitable safeguards.
- General description of TOSMs.

4.5 Data Protection by Design

The controller shall, both at the time of the determination of the means for processing and at the time of processing itself, implement **appropriate technical and organisational measures**, such as pseudonymisation, **which are designed to implement data-protection principles**, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GPDR and protect the rights of data subjects.

4.6 Data Protection by Default

The controller shall implement **appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural purpose.

4.7 Data Protection Officer

Person who advises on compliance with a data protection rules in organisations undertaking data processing. **Voluntarily** appointed by controllers, unless:

- A public authority or body carries out the processing.
- The controller's or processor's core activities consists of processing operations requiring the regular and systematic monitoring of data subjects on a large scale.
- The core activities consist of large-scale processing of special categories of data or personal data relating to criminal convictions and offences.

4.8 Supervisory Authorities

Independent public authority which is established by each member state pursuant to article 51. They :

- Receive data subject's complaints.
- Are responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.
- Must contribute to the consistent application of the GDPR throughout the Union and collaboration with the EU Commission.
- Must be independent.

4.9 Main Notions

4.9.1 Personal Data

Any **information** relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can b identified, directly or indirectly, in particular by reference to an identifier of that natural person.

Synthetic Data

Data artificially generated from real data thanks to AI mechanisms. As they appear to be referred to a natural person, they are not since they are artificially created.
They are not protected by the GDPR, so can be used freely and exchanged without the risk of breaches.

Big Data

Great volume, velocity and variety of data and can be either personal and non personal. They are useful for their technological ability to collect, process and extract new and predictive knowledge.
They can be regulated by the AI Act in some specific cases.

Sensitive Data

Art 9 - GPDR: Personal data revealing racial or ethnic origin, political opinions, religions or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
In principle is prohibited but there are some strictly exceptions.

4.9.2 Purposes

Aims for which data are collected and processed (not expressly defined by GDPR).

4.9.3 Consent

Referred to data subject, is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to he/she.

4.9.4 Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

Transfer

Rules governing the movement of personal data to countries or organizations outside the EU.

Cross-Border Processing

Involves processing personal data across multiple EU or international jurisdictions. It requires coordination to comply with GDPR and respect local laws while safeguarding individuals' rights.

4.9.5 Data Protection Impact Assessment (DPIA)

Is an assessment of the impact of the envisaged processing operations on the protection of personal data. Can be useful to find risks and after design specific tools (by design/default) to prevent those risks.
May be mandatory in certain cases:

- Systematic/extensive evaluation of personal data based on automated processing, including profiling activities.
- Processing on a large scale of special categories of data.
- Systematic monitoring of a publicly accessible area on a large scale.

The main contents are:

- Systematic **description** of the envisaged processing operations, purposes and legitimate interest of the Controller (if any).
- Assessment of the **necessity and proportionality** of the processing operations in relation to the purposes.
- Assessment of the **risk** to the rights and freedoms of data subjects.
- The **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance.

The writing is made by the Controller and the DPO (when there is).

4.10 Main Principles for PD Processing

4.10.1 Lawfulness and Fairness

Data processing must be lawful and fair, in order to this there is the need of a legal permission (consent) from the data subject. Necessary for:

- Performing a contract Necessary to full fill a contractual obligation with the data subject.
- Complying with a legal obligation.
- Protecting vital interests.
- Performance of a task of public interest.
- Legitimate interests of the controller/third party.

4.10.2 Transparency

How PD are collected, used, consulted or otherwise dislocated.

4.10.3 Purpose Limitation

Processing for specified, explicit and legitimate purposes, guaranteeing:

- **Legitimacy:** accordance with existing applicable laws.
- **Detail of the purpose:** further processing operations need to be verified (if compatible with initial purposes).

4.10.4 Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Assessment on proportionality and TOMs.

4.10.5 Accuracy

Personal data shall be accurate and kept up to date. If inaccurate the must be erased or rectified. PD shall reflect the reality of any given situation, inaccuracy may imply legal consequences even for the subject involved.

4.10.6 Storage Limitation

PD shall be kept in a form that permits identification of DS for no longer than necessary for the processing purposes (strict minimum).

4.10.7 Integrity and Confidentiality

Personal data shall be processed in a manner that ensures their appropriate security. Is necessary to avoid unauthorised/unlawful processing/access, accidental loss, destruction or damage.

4.10.8 Accountability

Legal element allowing DS to exercise the PDP and allows Controller and Processor to act lawfully and legally without getting fined.

4.11 Privacy Policy

Transparency and informing the public about how their data are being used are two basic GDPR goals. A **privacy notice** is a public document from an organization that explains how that organization processes personal data and how it applies data protection principles.

4.12 European Data Strategy

The 3 main pillars are:

- **Free Flow of Personal Data:** EU PDP Package is a main key.
- **Free Flow of Non-Personal Data:** all that information that can not be related to any natural person.
- **Single Market for Data:** as a digital level market.

4.12.1 A Developing Package

Is a package under development, but all the act are set to became in function after 2 years, so is still under construction and they are fully applicable.

Regulation 2018

- Adopted to ensure free flow of data other than personal data laying down rules relating to **data localisation requirements**.
  - **Data Localisation Requirements:** is **imposing** the processing of data in the territory of a specific Ms or hindering such processing in another MS, **in principle prohibited**.
- Is for the processing of electronic data.
- The scope of application is limited within the EU and limited for a set of data including personal and non personal data.

This regulation is imposing obligations upon the Member States to repeal any legal provision setting out data localisation requirements.
The **goals** are:

- Encouraging the development and adoption of self regulatory codes of conduct.
- To contribute to a competitive data economy.

DGA - Data Governance Act 2022

Aim: crating a framework for facilitating a safe data-sharing setting out conditions for their re-use and intermediation services.
It covers data held by public bodies, private bodies, citizens both for commercial and not commercial purposes either the initial purposes they where collected was different.
Data in this case are any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording.

DSA - EU Digital Services Act and DMA - EU Digital Markets Act

1. Creating a safer digital space where users' fundamental rights are protected.
2. Establishing a level playing field to foster innovation, growth and competitiveness.

Adopted to prevent digital trade of illegal users and to ensure safety online.

Data Act

At beginning of 2024, with the aim of grant fair access to and use of data. Is a **cross sectorial** regulations, so its principles apply to all sectors (general). Its objectives are:

- Increasing **legal certainty** for companies and consumers.
- **Mitigate the abuse of contractual imbalances** that impede equitable data sharing.
- Rules enabling **public sector bodies** to access and use data held by the private sector for specific public interest purposes.
- New rules setting the framework for customers to effectively **switch between different providers** of data-processing services.

Artificial Intelligence Act - AI Act

The **aim** is an harmonised framework on artificial intelligence for respecting fundamental rights.
Is **improving prediction, optimising operations and resource allocation, and personalising service delivery**.
It support socially and environmentally beneficial outcomes and is the key competitive advantages to companies and the EU economy.