UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Master's Degree in Computer Science

Academic year 2024/2025

LAW AND DATA

Prof. Fiorella Dal Monte

Written by Michael Amista'

A course offered by the School of Science –
Master's Degree in Data Science

Table of contents

1. Laws, legal systems and sources of law

A **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.

A **legal order** is a collection of general and specific norms that regulate human behaviour, setting expectations for how individuals ought to act. These norms are guidelines that can function as commands, permissions, or authorizations. The concepts of a norm and a "ought" coincide.
A **plurality of norms** is an order if they constitute a unity, meaning they share a common foundation of validity.
If the law is **positive law**, the norms of a legal order are "posited" or "created" through human acts → the norm is the subjective meaning of the act.

The **legal system** includes *rules*, *procedures* and *institutions* by which activities, both public and private, can be carried out through legitimate means. A legal system is a system for interpreting and enforcing the laws. Plurality of legal systems considering several and different social groups.

Examples of what legal systems can be / where legal systems can be found:

- STATES (e.g. Italy, France, USA, India, China, etc.)
- EUROPEAN UNION (Legal system encompassing 27 Member States)
- COUNCIL of EUROPE (Legal system including 46 Member States)
- INTERNATIONAL LEGAL ORDER (Special legal system – independent from States)

Note: European Union is a huge legal system that deals with other 27 legal systems.

Legal systems are organized based on modern theory of **separation of power**. In legal systems the power is divided into three branches: legislative branch is responsible for making laws; executive for implementing and enforcing these laws; judicial for interpreting them.
This structure ensures that power is not concentrated in one branch, **promoting legal certainty** (the law should be easily understandable, making clear what an individual can do or not), **impartiality**, and **equality before the law** (everyone should be treated equally before the law). Every power should be checked by the other powers, in a way it cannot overcome the others, reaching so a balance.

The system of **checks & balances** limits the power of a single individual/entity/body of government to ensure balanced and harmonious and relationships and co-existence.

There are two branches of law, and each legal system needs to manage this separation: **public law** and **private law**. Branches of law is universally accepted, meaning every law belongs to one of those two branches, there cannot be a third branch.

Public law governs the relationship between individuals and the state, ensuring the regulation of public affairs and the protection of individual rights through administrative, constitutional, and criminal law.
Private law, on the other hand, manages relationships between private individuals and entities, encompassing areas such as contract law, property law, family law, and tort law.

Privacy law is unique because it fits into both public and private law:

- **Public Law**: privacy law controls how government bodies handle personal information, protecting individuals from government overreach. For example, laws may limit how much data the government can collect on citizens.
- **Private Law**: privacy law also applies to interactions between private individuals or companies. For instance, it regulates how businesses can collect and use customer data or allows someone to sue someone else for invading their privacy.

Privacy law overlaps with both public and private law because it protects people's rights both against the government and in private relationships.

There are two primary types of legal systems used by countries worldwide:

- **Civil Law**:
  - Based on written laws or codes (like statutes and regulations) that are applied and interpreted by judges.
  - Judges play a limited role in creating law; they focus mainly on applying the existing laws to cases.
  - Legal decisions generally do not set binding precedents for future cases.
- **Common Law**:
  - Based on precedents, or past judicial decisions, alongside written statutes.
  - Judges have a more active role in shaping the law because their decisions can set precedents for future cases.
  - This system relies heavily on the principle of *stare decisis*, which means that courts follow the rulings of previous similar cases to maintain consistency.

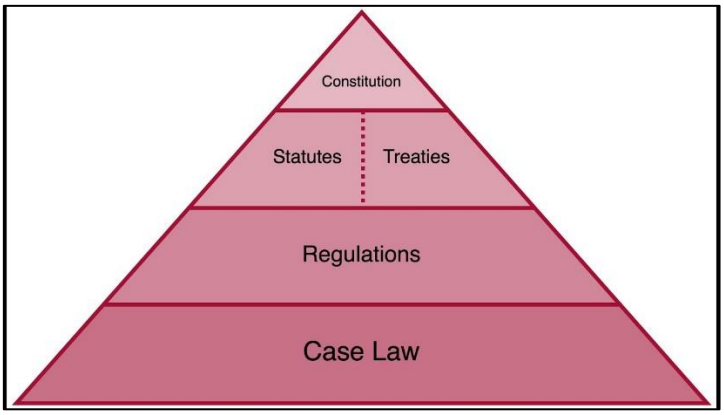
Sources of law are the origins from which laws derive their authority and content. They include the foundational rules and principles that govern a legal system, such as constitutions, statutes, regulations, case law, and customary practices. These sources establish legal standards, rights, and obligations and guide the judiciary, legislators, and public in the application and interpretation of law.

Sources of law can be classified as:

- **Hard law** consists of binding legal rules that can be enforced in a court of law (e.g., European Convention of human rights). Examples include constitutions, statutes, regulations, and treaties, which impose clear obligations and specify consequences for non-compliance. Hard law provides the legal certainty and authority necessary to govern conduct, protect rights, and ensure accountability within society.

- **Soft law** includes non-binding guidelines, principles, and agreements, such as codes of conduct (e.g., Universal Declaration of human rights). Soft law can be used by a judge to interpret hard law. Many rights and obligations regarding data protection originates from soft law provision.

Sources of law are hierarchical, meaning that lower sources of law cannot contradict higher sources of law. This hierarchy determines which laws take precedence in case of conflict. To have an idea consider the following source of law pyramid, keeping in mind every country has its own one that may differ from this.



Note: Case Law refers to law established by judicial decisions rather than through legislative statutes. Case law is generally considered a form of hard law. It is legally binding within the jurisdiction of the court and must be followed by lower courts in the same hierarchy. For example, a ruling by the U.S. Supreme Court becomes binding precedent for all federal and state courts in the United States.

2. European Union (EU)

The European Union is a legal system, composed by rules (defined by legislators), procedures (set up by rules) and institutions. It is an example of legal system composed by other 27 states (other legal systems) and due to that is one of the most complex.

In Europe there are also international organizations (legal systems) that deal with states that belong to EU and not, in general with European states. It is important to talk about them since these organizations are involved in data protection policies.

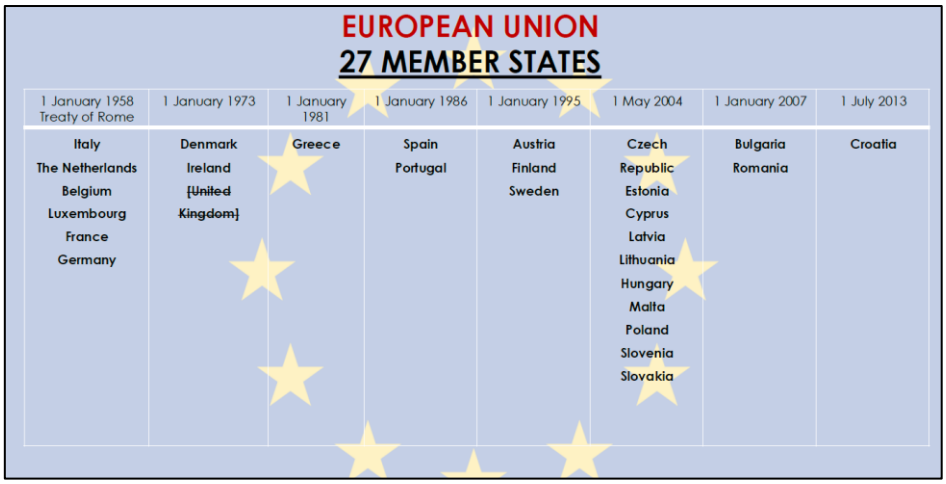
- The **Council of Europe (CoE)** operates with the goal of sustain human rights, democracy and the rule of law in Europe (compliance to existing legal systems). Composed by 46 member states. The most important institution is the European Court of Human Rights.
- The **European Free Trade Association (EFTA)** is an intergovernmental organisation established in 1960 by the EFTA Convention, that promotes free trade and economic integration between its members, within Europe and globally.
- The **European Economic Area (EEA)** includes EU and EFTA members (excluding Switzerland) under an international agreement from 1994, ensuring the application of EU single market rules across a defined geographic area.

What we need to understand how the rules of each legal system of interest are applied in data protection, asking ourselves which is the legal boundary in which we can operate when talking about personal data.

Members of the different international organizations

- EFTA -	- EEA -		- SCHENGEN -	
Iceland	Austria	Italy	Austria	**Liechtenstein**
Liechtenstein	Belgium	Latvia	Belgium	Lithuania
Norway	Bulgaria	**Liechtenstein**	Croatia	Luxembourg
Switzerland	Croatia	Lithuania	Czech Republic	Malta
	Cyprus	Luxembourg	Denmark	Netherlands
	Czech Republic	Malta	Estonia	**Norway**
	Denmark	Netherlands	Finland	Poland
	Estonia	**Norway**	France	Portugal
	Finland	Poland	Germany	Slovakia
	France	Portugal	Greece	Slovenia
	Germany	Romania	Hungary	Spain
	Greece	Slovakia	**Iceland**	Sweden
	Hungary	Slovenia	Italy	**Switzerland**
	Iceland	Spain	Latvia	
	Ireland	Sweden		
			NO Bulgaria, Cyprus, Ireland, Romania	

Schengen Area is a group of 27 European countries that have abolished most of their internal borders to allow free and unrestricted movement of people across member states. This means that within the Schengen Area, people can travel from one country to another without going through passport checks or border controls, much like moving between states within a single country.



European Union was born to prevent conflicts of any type between the member states (e.g., wars). Now EU counts 27 members states (28 before UK left).

*"The Community constitutes a **NEW LEGAL ORDER** OF INTERNATIONAL LAW for the benefit of which the states have limited their sovereign rights"*.

In the *Costa v. ENEL* case, the European Court of Justice (ECJ) ruled that the European Community (now the EU) established a new legal order, distinct from international law and above the individual laws of member states. This new legal system requires that **member states cede some aspects of their sovereignty to the EU**, meaning that EU law takes precedence in areas governed by EU treaties.

*"its own legal system which, on the entry into force of the Treaty, became an **integral part of the legal systems of the Member States** and which their courts are bound to apply (...)"*.

In *Van Gend en Loos*, the ECJ established that EU law is directly applicable in member states and forms an integral part of their national legal systems. This principle means that EU law can create rights and obligations for individuals and entities within member states that national courts must enforce.

APPLICATION FOR 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

*«any European State which respects the **values referred to in Article 2** and **is committed to promoting them** may apply to become a member of the Union. 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** by all the contracting States in accordance with their respective constitutional requirements»*

Article 2 sets the foundational values for EU membership, while **Article 49** defines the structured, consensus-driven process by which eligible countries can join the EU. These articles reinforce the EU as a **values-based union** with strict entry requirements to maintain cohesion among its member states. In general, both articles set the basis for the respect of the fundamental human rights which is also related to data protection.

The **Copenhagen Criteria** defines the different kind of requirements for a country to join EU:

- **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 and market forces, protecting so the consumers' rights (freely able to purchase what they want).
- **Administrative and institutional capacity**: to effectively implement the *acquis communautaire*** and ability to take on the obligations of EU membership.

* rule of law: all public powers must operate within the limits established by law.

- LAW-MAKING PROCESS: transparent, accountable, democratic and pluralistic.
- JUDICIAL PROTECTION: 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 of basic political and civil rights, civil liberties.

** *acquis communautaire*: body of common rights and obligations binding upon EU member states.

2.1 Hierarchy of sources of law in EU

The hierarchy of sources in European Union law establishes the order of legal authority among various types of legislation within the EU framework.

1. At the top is **Primary Law**, which includes foundational treaties such as the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). These treaties form the constitutional basis of EU law and set out the structure, powers, and principles guiding the EU.
2. Below primary law there are **International Agreements**, which are treaties and agreements that the EU makes with non-EU countries or international organizations. These agreements are binding and integrate into EU law, influencing member states' legal systems.
3. **Secondary Law** follows, comprising regulations, directives, decisions, recommendations, and opinions issued by EU institutions to implement and apply primary law.

4. Lastly, **Supplementary Law** fills in gaps through case law from the Court of Justice of the European Union and unwritten principles that ensure consistent interpretation and application of EU law across member states.

2.1.1 Primary Law

Primary law includes **Treaties**, the **Charter of Fundamental Rights**, and **General Principles** established by the Court of Justice of the European Union.

Treaties are the core legal documents that founded and continue to shape the European Union:

- **Founding Treaties**: treaties established the European Communities, which evolved into the European Union. The key founding treaties laid the groundwork for European integration and cooperation.
- **Amending Treaties**: over time, various treaties have been amended to adapt to changing political and economic conditions.
- **Protocols annexed to treaties**: protocols attached to the treaties clarify or specify certain aspects of EU law.
- **Accession Treaties**: these treaties enable new countries to join the EU, setting terms for their membership and adapting the EU structure to accommodate new members.

The **Charter of Fundamental Rights** guarantees key rights and freedoms to individuals within the EU, such as dignity, freedoms, equality, solidarity, citizens' rights, and justice. The Charter reflects the EU's commitment to human rights.

The **General Principles**, established by the European Court of Justice (ECJ), ensure fairness and coherence in the interpretation and application of EU law. These principles include proportionality, legal certainty and protection of fundamental rights.

As mentioned before, primary law also consists in two treaties that shaped the basis of EU:

- **Treaty on the European Union (TEU)** sets out the EU's main objectives, principles, and values, such as promoting peace, democracy, and the well-being of its community. It also defines the core institutions of the EU (e.g., European Parliament, European Commission, Council of the EU) and describes their functions and relationships. The TEU essentially acts as a "constitutional" document for the EU, outlining its purpose and values.
- **Treaty on the Functioning of the European Union (TFEU)** provides detailed organizational and operational rules to implement the objectives established in the TEU. It includes the procedures, competencies, and responsibilities of the EU institutions, helping to structure the day-to-day functions and powers of the EU.

Together, these treaties form the legal foundation of the EU, setting both broad principles and specific mechanisms for how the EU functions and interacts with its member states and citizens.

Article 16(1) of TFEU establishes the right to **personal data protection** as a fundamental aspect of human rights within the EU. This provision underscores that individuals have a right to privacy concerning their personal data, ensuring their control over how personal information is used, stored, and shared. This article laid the groundwork for the General Data Protection Regulation (GDPR).

2.1.2 Secondary Law

Secondary Law in the EU refers to legal acts established based on the EU Treaties, and it is governed by **Article 288 of the TFEU**. These acts are defined as **typical and atypical acts**.

Typical Acts (TFEU Art. 288 TFEU) include:

- **Regulations**, **Directives**, and **Decisions**: these are binding forms of law (hard law provision). They have legal force and are mandatory in specific ways, depending on the type.
- **Opinions** and **Recommendations**: these are non-binding (soft law provision) and serve as guidance without enforceable power.

How much is each typical act binding?

- A **regulation** is binding in its entirety and is directly applicable in all EU Member States. This means that once it is adopted, it automatically becomes part of national law without the need for transposition. Member States are required to apply it as it is, ensuring consistent application across the EU.
- A **directive** is binding regarding the result it seeks to achieve but allows Member States flexibility in how they implement it. National authorities are responsible for choosing the form and methods to reach the directive's objectives. This process requires transposition, where each Member State adapts the directive into its own legal system, while still achieving the intended EU-wide goal.
- A **decision** is fully binding in its entirety. It can be *general*, applying to all within the EU, or *individual*, targeting specific entities or individuals. When a decision is individual in scope, it is only binding on the parties to whom it is addressed, making it a tailored instrument for specific cases.

Atypical Acts, instead, include documents like communications, resolutions, white papers (proposals for EU actions), and green papers (used to stimulate debate on a specific topic). They are not explicitly mentioned in Art. 288 TFEU and generally lack binding force, often used to express ideas, intentions, or proposals from EU institutions.

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 harmonised rules on artificial intelligence – ***Artificial Intelligence Act***

2.2 EU institutions

Article 13 of the Treaty on European Union (TEU) establishes the main institutions of the European Union which are:

- European Parliament
- European Council
- Council of the EU (Council)
- European Commission
- Court of Justice of the EU
- European Central Bank
- Court of Auditors

2.2.1 European Parliament

The European Parliament serves as a cornerstone of **democratic representation** within the European Union. It consists of a maximum of 750 MEPs (Members of the European Parliament), though currently, there are 705 members. Each Member State (MS) is allocated a number of MEPs proportional to its population. Since 1979, EU citizens have directly elected MEPs every five years to represent their interests rather than those of their respective MS. The Parliament's members organize themselves into **political groups based on shared ideologies**, rather than national affiliations. It operates across three primary locations: Strasbourg, Brussels, and Luxembourg.

The **functions of the European Parliament** span legislative, budgetary, supervisory, and elective domains.

- As one of the EU's two **legislative** chambers, it collaborates with the Council of the European Union in shaping laws.

- In its **budgetary** role, the Parliament oversees EU expenditures.
- It also exercises **supervisory** authority, holding other EU institutions accountable through general reports, questioning the European Commission, and conducting inquiries via temporary committees. Furthermore, the Parliament provides a platform for EU citizens to submit petitions and elects the EU Ombudsman, a civil mediator addressing maladministration.
- Its **elective** responsibilities include approving the President of the European Commission, proposed by the European Council, and the team of EU Commissioners, proposed by the Commission's President.

2.2.2 European Council

The European Council is the **EU's strategic decision-making body**, comprising the 27 Heads of State or Government from each Member State. Its role is to set the EU's overall political direction, though it holds no formal legislative power. The European Council **provides guidelines on key areas** such as the Common Foreign and Security Policy (CFSP), external actions, and broad economic strategies. While its primary function is advisory, it can intervene in specific matters outlined by EU treaties. Led by a President elected for a 2.5-year term.

2.2.3 Council of the EU (Council)

The Council of the European Union, often referred to simply as the Council, **represents the governments of the EU Member States**. Each Member State sends a representative, typically a minister, empowered to commit their government and cast votes on its behalf. The Council operates in various configurations, depending on the policy area under discussion, such as General Affairs, Foreign Affairs, Economic and Financial Affairs, Environment, or Justice and Home Affairs. As one of the EU's legislative chambers, the Council **shares responsibility with the European Parliament for adopting legislation**. Additionally, it performs supervisory functions, ensuring that other EU institutions align with the agreed policies and objectives, thus maintaining accountability within the Union's governance structure.

2.2.4 European Commission

The European Commission is the EU's executive body, composed of 27 Commissioners who serve five-year terms and are collectively approved by the European Parliament. Commissioners are appointed through a collaborative process involving the European Parliament, the President of the Commission, and the Member States. However, once in office, they **act independently from Member States**, prioritizing the interests of the EU rather than those of their home countries. The Commission is organized into specialized Directorates-General, each handling specific policy areas. Its primary functions include **proposing new legislation, enforcing EU law, managing the EU budget, and supervising compliance by Member States and private entities**.

2.2.5 Court of Justice of the EU (ECJ)

The European Court of Justice, together with the General Court of the EU, serves as the **judicial branch of the European Union**, ensuring the uniform interpretation and application of EU law. It comprises **Judges** and **Advocates General**, with the number typically corresponding to the number of Member States (one per MS). Judges and Advocates General are appointed for renewable six-year terms, with appointments staggered every three years to maintain continuity. They are selected among individuals qualified for the highest judicial offices in their respective countries or recognized legal experts of high competence. Despite their national origins, these officials act with complete independence from their home countries, prioritizing the principles and laws of the EU.

The ECJ's functions span several key areas. Its **jurisdictional role** involves handling litigation cases. In its **interpretative role**, the ECJ provides preliminary rulings ("decisions") when national courts request clarification on EU law (not litigation). Additionally, its **advisory and consultative function** enables the court to offer non-binding guidance on legal matters (not litigation).

The **Litigation Proceedings** before the ECJ can be summarized into three main categories:

- **Direct Appeals** (Article 263 TFEU): appeals can be filed against acts adopted by EU institutions.
    - Public Initiatives: Filed by Member States or other EU institutions.
    - Private Initiatives: Filed by individuals or legal entities if the act directly and individually concerns them or relates to a regulatory act without implementing measures. Grounds for appeals include lack of competence, invalidity, voidness, or misuse of powers. There is a strict time limit of 2 months and 10 days for filing.
- **Failure to Act** (Article 265 TFEU): if an EU institution fails to act when legally required, a process is initiated:
    - Prelitigation: A formal notice is sent, providing the institution 2 months to respond or act.
    - If non-performance persists, the matter proceeds to litigation before the ECJ.
- **Compensation for Damages** (Article 340(2) TFEU): individuals, legal entities, or Member States can seek compensation for damages caused by unlawful, serious, and certain actions or omissions of EU institutions.

The **Non-Litigation Proceedings** before the ECJ focus on Preliminary Rulings (Article 267 TFEU):

- **Initiative:** any jurisdiction in a Member State (MS), regardless of its nature or instance, can request a preliminary ruling, often at the request of the parties involved.
- **Object:**
    - Interpretation of any EU law provision.
    - Validity of acts adopted by EU institutions.

- **Development Process:**
    - A case begins in the national court of an MS.
    - The national judge refers questions regarding EU law to the ECJ.
    - Typically, national proceedings are suspended while awaiting the ECJ's decision.
    - The ECJ delivers a binding judgment or order, which the national judge must follow.

2.2.6 Bodies of the EU

The bodies of the EU consist of specialized institutions and agencies that support the functioning of the Union by addressing specific areas of expertise. Here we list the bodies focused on data protection and fundamental rights:

- **European Data Protection Supervisor (EDPS)**: an independent body that ensures EU institutions and bodies respect individuals' right to privacy when processing personal data. EDPS can receive complaints from individuals and determine possible data breaches caused by EU institutions. If data breaches are not caused by EU institutions (for example by other individuals/businesses) individuals must report it to the relative national supervisory authority (as defined by the GDPR).
- **European Data Protection Board (EDPB)**: an independent body that ensures the consistent application of data protection rules across the EU and promotes cooperation among national data protection authorities. Especially involved when data is exchanged between different States → EDPB, if involved, can decide which national supervisory authority is responsible for that data exchange.
- **Agencies of the European Commission**:
    - Decentralized bodies within the EU, distinct from its main institutions.
    - Created to perform specific tasks and responsibilities.
- **Fundamental Rights Agency (FRA)**: focused on providing expert advice and data on fundamental rights to help ensure these rights are respected across the EU.

3. Privacy and Personal Data Protection

Over the time the notion of privacy was subject to many interpretations and declinations. Initially privacy was associated to a **negative** connotation which deals with the need to prevent intrusions from the external space. Nowadays, instead, privacy is represented by a **positive** connotation which refers to the possibility/right of making free choices by ourselves, no more avoiding external intrusions in our personal space but rather **deciding who can have access to our personal space**. Exclusion became something individuals can decide, not avoid.

The **distinction between what is private from what is public**, rooted in common law, forms the basis of privacy rights. Common law recognizes certain aspects of life, such as reputation, family matters, and personal information, as private, offering legal protection from interference or exposure. In contrast, public matters, such as actions in the public sphere or information voluntarily shared with the public, receive less legal protection.

The **distinction between the Common Law and Civil Law traditions in privacy** highlights different approaches to individual rights. In the Common Law tradition, privacy is often linked to the **right to liberty**, emphasizing personal freedom and protection from interference in private matters. In contrast, the Civil Law tradition emphasizes the **right to dignity**. Here, privacy is more closely tied to ensure that a person's dignity is respected and preserved in all aspects of life.

Article 8(1) of the Charter of Fundamental Rights (CFR) specifically states: "*Everyone has the right to the protection of personal data concerning him or her*".

Personal data is any information relating to an identified or identifiable natural person. 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 (Art. 4(1) GDPR).

Note: the concept of personal data does not derive from common law, it belongs to civil law development of the notion of privacy. **The right to protect personal data is seen as part of the individual's dignity and autonomy**, ensuring that their personal information is handled with care and respect.

The right to privacy and the right to personal data protection are closely related but distinct concepts that aim to safeguard human rights. Both rights are **intertwined and often overlap**, as they aim to safeguard individual autonomy and dignity. Privacy protects a person's private life, home, communications, and freedom from undue interference, while personal data protection focuses on controlling the use and processing of personal information to prevent misuse or harm. Despite their differences, both rights **work together to ensure individuals are treated with respect and fairness**, transcending boundaries of race, sex, nationality, ethnicity, religion, or any other status, as they belong to all individuals inherently as human beings.

3.1 Right to Privacy

The **Nice Charter (2009)** and the **EU Charter of Fundamental Rights (2009)** are crucial because they provide a codified set of rights that are legally binding on the European Union and its member states. The transition from the Nice Charter to the EU Charter of Fundamental Rights marked a significant evolution in the EU's commitment to protect fundamental human rights. Here we list some of the most significant articles from the CFR:

- **Article 7 – Respect for private and family life (RIGHT TO PRIVACY)**: this right protects individuals' private lives, homes, and communications. It emphasizes that no interference by public authorities is allowed unless it is lawful, necessary, and proportional in a democratic society. Exceptions are limited to legitimate objectives such as national security, public safety, economic well-being, crime prevention, health, or the protection of others' rights and freedoms.
- **Article 8 – Protection of personal data (RIGHT TO PRIVACY → PERSONAL DATA PROTECTION)**: it guarantees that individuals have the right to ensure their data is processed fairly, for specified purposes, and with their consent or under another legitimate legal basis. Additionally, individuals have the right to access their data and request rectification of inaccuracies. Compliance with these rules must be overseen by an independent authority, ensuring transparency and accountability.
- **Article 52 – Scope and interpretation**: while these rights are fundamental, Article 52 of the EU Charter outlines conditions under which they may be limited. Such limitations must:
    - Be provided by law and respect the essence of the right.
    - Be necessary, proportional, and aimed at achieving objectives of general interest recognized by the EU or protecting others' rights and freedoms.

3.2 Right to Personal Data Protection

One significant milestone in the development of global standards for data protection is the **OECD Privacy Guidelines** (1980), which introduced a set of soft law universal standards. These principles continue to influence national and international data protection frameworks today. The key principles are:

- **Collection limitation**: there should be limits to the collection of personal data, which must be obtained by lawful and fair means.
- **Data quality**: personal data should be relevant to the purposes for which they are used, and be accurate, complete, and up to date.
- **Purpose specification**: the purposes for which personal data are collected should be specified at the time of data collection.
- **Use limitation**: personal data should not be disclosed, made available, or otherwise used for purposes other than those specified except with the consent of the subject or by the authority of law.

- **Security safeguards**: personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
- **Openness**: there should be a general policy of openness about developments, practices, and policies with respect to personal data.
- **Individual participation**: an individual should have the right to obtain data about themselves, and to have data corrected or erased if it is inaccurate, incomplete, outdated, or processed unlawfully.
- **Accountability**: data controllers should be accountable for complying with measures that give effect to the principles stated above.

The Council of Europe Convention 108, adopted on 28 January 1981 (now celebrated as Data Privacy Day), was the **first legally binding international instrument on data protection**. Officially titled the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, it established universal standards for protecting individuals' personal information in an increasingly automated world. Convention 108 set a global precedent for regulating data processing, ensuring respect for privacy, and safeguarding individuals' rights. Its modernized version, Convention 108+, adopted on 18 May 2018, updates these standards to address challenges posed by new technologies, strengthening accountability, transparency, and international cooperation in the digital age.

The applicable EU legislations (primary law) to protect the right to personal data protection are following reported:

- **TEU - Article 39**
  In accordance with Article16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph2 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 - Article 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.

3.3 EU Personal Data Protection directives

A **directive** is a legislative act that sets out a goal that EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the EU single-use plastics directive, which reduces the impact of certain single-use plastics on the environment, for example by reducing or even banning the use of single-use plastics such as plates, straws and cups for beverages.

The evolution of data protection laws in the European Union began with **Directive 95/46/EC**, which focused on protecting individuals regarding the processing of personal data and the free movement of such data. However, its limited harmonization led to the development of the **General Data Protection Regulation (GDPR)**. Another key milestone was **Directive 2006/24/EC (Data Retention Directive)**, which regulated the retention of data generated or processed in electronic communication services. This directive was repealed by the European Court of Justice (ECJ) in the landmark case of Digital Rights Ireland (*C-293/12 + C-594/12*).

Applicable EU Data Protection Directives are the following:

- **Directive 2002/58/EC (E-Privacy Directive)**
  This directive aims at safeguard the privacy and the processing of personal data within public electronic communication services.
- **Directive 2016/680/EU (Data Protection Law Enforcement Directive)**
  This directive ensures the protection of personal data processed by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offenses.

DIRECTIVE 2002/58/EC (E-PRIVACY DIRECTIVE)

Some definitions:

- **User**: any natural person using publicly available electronic communications services, whether for private or business purposes, without necessarily subscribing to the service (**subscriber**).
- **Traffic Data**: data processed for communication conveyance on electronic networks or for billing purposes.
- **Location Data**: data indicating the geographic position of a user's terminal equipment in an electronic communication network.
- **Communication**: information exchanged between a finite number of parties via publicly available electronic communications services, excluding broadcasting unless identifiable by subscribers or users.

Scope of application: covers the application and processing of personal data (PD) in connection with public communication networks.

Service Provider: service providers must implement appropriate technical and organizational measures to ensure data security.

Objective: Member States must guarantee the confidentiality of communications and related data (e.g., traffic data).

Key scenarios addressed by the directive:

- **Automatic Call Forwarding**: prohibited unless stopped by the user.
- **Directories of Subscribers**: permitted only with explicit or implied consent.
- **Unsolicited Communications (spam)**: allowed only with prior, clear, and distinct consent. Users must have an easy and free way to object.

Directive 2018/1972 (European Electronic Communications Code – "Recast directive")

This directive provides a harmonized framework for regulating electronic communications services, networks, and associated facilities across the EU. Although it does not focus directly on personal data processing, it contributes to the broader data protection landscape by:

- Promoting an internal market in electronic communications.
- Ensuring fair competition and equitable access to services.
- Expanding connectivity across the EU.

Directive 2016/680/EU (Data Protection Law Enforcement Directive)

This directive ensures the protection of personal data processed by competent authorities for law enforcement purposes, filling the gap left by the repealed Data Retention Directive. It has been adopted in parallel with GDPR as part of the new "**Personal Data Protection Package**".

Key provisions include:

- **Data Protection by Design and Default**: systems must integrate privacy measures from the outset.
- **Data Security and Breach Notifications**: organizations are required to maintain security and notify breaches promptly.
- **Data Protection Officers (DPOs)**: appointment of DPOs is mandated for oversight.

Key restriction: **decisions based solely on automated processing (including profiling) are prohibited in principle**. The use of sensitive data for such decisions is strictly forbidden. Processing must not result in any form of discrimination.

Beyond directives, there are also **applicable EU data protection regulations**, such as:

- The **General Data Protection Regulation (Regulation 2016/679/EU)**, widely known as the GDPR, provides a robust framework for the protection of personal data, ensuring individuals' rights and harmonizing standards across EU.
- Complementing this, **Regulation 2018/1725/EU** outlines specific data protection rules for European Union institutions, bodies, offices, and agencies, aligning their practices with the principles of the GDPR.
- Additionally, the evolving digital landscape is addressed through complementary regulations like the **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)**, which enhance transparency, accountability, and fair practices in online platforms and digital markets.

4. General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)** is a legal framework that sets guidelines for the collection, processing, and protection of personal data of individuals within the EU. It also applies to organizations outside the EU that handle the personal data of EU citizens, ensuring their privacy rights are safeguarded globally.

4.1 Data Subject

The term "Data Subject" refers to any individual who can be identified, directly or indirectly, by any related information such as a name, an identification number, location data, etc.

Main rights of the Data Subject:

- **Right to be informed of purposes**: individuals must be informed about the purposes for which their personal data is collected and processed, ensuring transparency.
- **Right to access**: data subjects have the right to access their personal data held by organizations and understand how it is being used.
- **Right to rectification, erasure (aka "right to be forgotten"), restriction**: individuals can request the correction of inaccurate data, deletion of their data under specific conditions (right to be forgotten), or restriction of data processing.
- **Right to data portability**: data subjects can request their personal data in a structured, commonly used, and machine-readable format to transfer it to another controller.
- **Right to object**: individuals have the right to object to data processing for specific purposes, such as direct marketing, profiling, or processing based on legitimate interests.

4.2 Controller

GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**". When two or more entities jointly determine the purposes and means of processing, they are considered **joint controllers**.

Controllers have some obligations: as a general rule, it is responsible and liable for any processing of personal data carried out by itself and on its behalf. The main obligations are:

- Adoption of appropriate TOMs (Technical & Organizational Measures) to implement data protection principles.
- Record of processing activities
- Cooperation with Data Subjects
- Cooperation with Supervisory Authorities

A **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 objective it to achieve compliance with GDPR, by adopting appropriate TOMs.

4.3 Processor

GDPR defines a processor as "a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**".

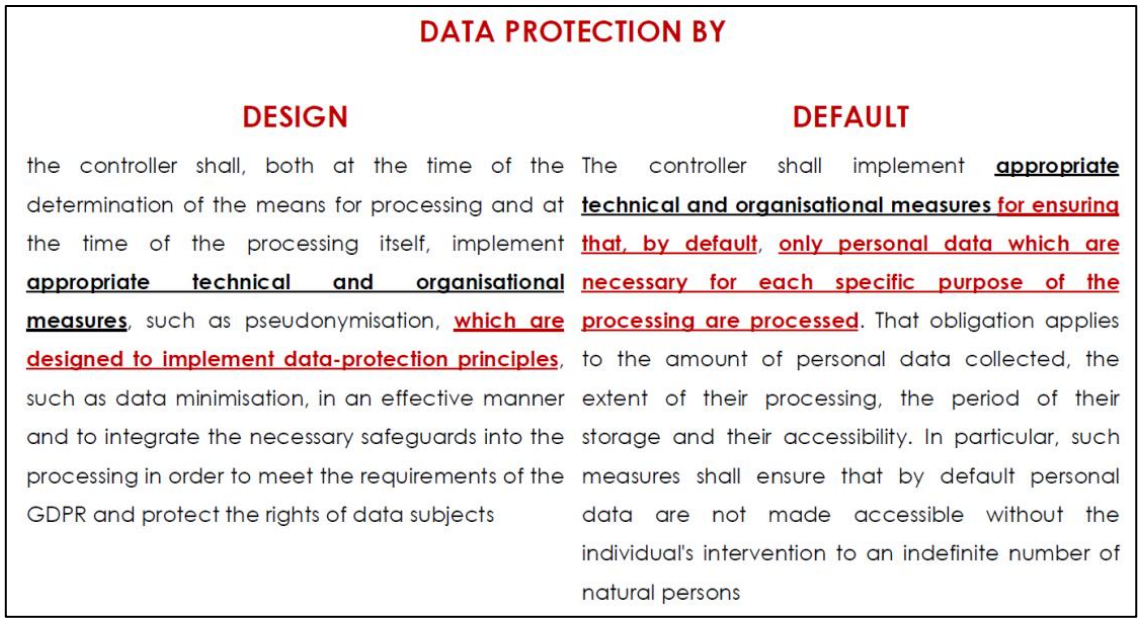
With "processing personal data" (**PD processing**) we refer to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Main obligations of the Processor:

- Act upon instructions of the Controller
- Implement TOMs
- Appoint a Representative within the EU
- Maintain a record of processing activities
- Cooperate with Supervisory Authorities
- Designate a Data Protection Officer (where required)

Contents of the RECORD

CONTROLLER	PROCESSOR
Name and contact details of the (joint) controller(s), the representative(s) and DPO(s)	Name and contact details of the processor(s) and (joint) controller(s), the representative(s) and DPO(s)
Purposes	Categories of processing
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 organisation and documentation of suitable safeguards	Transfer to third countries/international organisation and documentation of suitable safeguards
Envisaged time-limits for erasure of the different categories of data	--
General description of TOSMs	General description of TOSMs



4.4 Data Protection Officer (DPO)

According to GDPR, the Data Protection Officer is a "person who advises on compliance with 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 consist 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.

4.5 Supervisory Authority

Supervisory Authority is an "independent public authority which is established by each Member State pursuant to Article 51".

Supervisory Authorities have different responsibilities, such as:

- Data subjects' complaints.
- Be responsible for monitoring the application of the GDPR, 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.
- Contribute to the consistent application of the GDPR throughout the Union and collaboration with the EU Commission.

4.6 Main notions

This section provides some interesting notions used by GDPR to implement data protection regulations.

PERSONAL DATA: 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

SENSITIVE DATA: a special category of personal data that reveals racial or ethnic origin, political opinions, religious 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, the processing of sensitive data is considered prohibited. However, there are few exceptions:

- Explicit consent (specified purposes)
- Employment law / social security and social protection law
- Protection of vital interests
- Legitimate activities of foundations, associations, non-profit bodies – members or former members
- Manifestly made public by DS
- Legal claims
- Substantial public interest
- Preventive / occupational medicine
- Health - public interest
- Scientific and historical research – public interest

PURPOSES: GDPR does not define explicitly the purposes, but they can be generally described as “aims for which data are collected and processed”.

CONSENT (of the Data Subject): any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

DATA PROTECTION IMPACT ASSESSMENT (DPIA): assessment of the impact of the processing operations on the protection of personal data, helping identify/minimize data protection risks of a project (particularly, determining "whether processing likely result in high risk"). The data controller, responsible for determining the purpose and means of processing personal data, works closely with the DPO, who serves as an independent advisor ensuring that data protection principles are upheld.

DPIA is mandatory only in the following 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 (e.g., monitoring traffic).

DPIA assessment includes:

- Systematic description of the specific 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.
- An assessment of the risks 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.

Note: DPIA differs from DPMS, which is primarily an IT security framework that organizations use to monitor and manage their compliance with personal data processing requirements. In contrast, a DPIA focuses on assessing specific data processing activities to identify potential risks to individuals' rights and freedoms. It enables organizations to evaluate the potential impact of such activities and determine the measures necessary to mitigate or minimize the identified risks.

4.7 Main principles for PD processing

GDPR defines the main principles for personal data processing. The principles are:

- Lawfulness and Fairness
- Transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and Confidentiality
- Accountability

Lawfulness and Fairness are based on legal permission given from the Data Subject. Legal permission is necessary for:

- Performing a contract
- Complying with a legal obligation
- Protecting vital interests
- Performance of a task of public interest
- Legitimate interests of the controller/third party

Transparency describes how personal data is collected, used, consulted or otherwise disclosed. The information that should be in plain is:

- on the identity of the controller;
- on the purposes of the processing;
- on the DS rights / to obtain confirmation and communication of processing activities;
- on risks, rules, safeguards and rights in relation to processing activities.

Purpose limitation principle requires that personal data should be processed only for specified, explicit, and legitimate purposes. The key aspects are the following:

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

Data minimization principle ensures 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 should be adopted.

Accuracy principle ensures personal data shall be accurate and kept up to date. If inaccurate, erasure or rectification must be made. Personal data shall reflect the reality of any given situation. Inaccuracy may imply legal consequences even for the subjects involved.

Storage limitation ensures personal data shall be kept in a form that permits identification of data subjects for no longer than necessary for the processing purposes, basically the bare/strict minimum.

Integrity and Confidentiality principles ensure personal data shall be processed in a manner that ensures their appropriate security. This is necessary to avoid:

- Unauthorised/unlawful processing.
- Unauthorised/unlawful access.
- Accidental loss, destruction, damage.

The principle of **accountability** focuses on focusing on two key roles: Controller and Processor. Both controllers and processors must take responsibility for their handling of personal data.

A **privacy policy** is a crucial document for any organization handling personal data and some templates on how to write a policy. The topics asked are the following:

- What data do we collect?
- How do we collect your data?
- How will we use your data?
- How do we store your data?
- Marketing
- What are your data protection rights?
- How to contact us
- How to contact the appropriate authorities
- How do we use cookies and what types of cookies do we use?
- How to manage your cookies
- Privacy policies of other websites
- Changes to our privacy policy

5. European Data Strategy

Synthetic data can be defined as "artificial data generated from original data and a model that is trained to reproduce the characteristics and structure of the original data". Synthetic data and original data should deliver very similar results when undergoing the same statistical analysis (generation process = SYNTHESIS).

Big data can be defined as "great volume, velocity and variety of (personal and non-personal) data and technological ability to collect, process and extract new and predictive knowledge".

The **European Data Strategy** focuses on creating a connected and efficient system for sharing data across the European Union. It promotes the **free flow of personal and non-personal data**, allowing individuals and businesses to access and use data more easily while protecting privacy and security. The goal is to build a **single market for data**, where data can move freely between sectors and countries. This helps support innovation, economic growth, and new technologies, while ensuring that people's rights are protected.

The EU Data Strategy, initiated in 2020, is a comprehensive framework aimed at making the European Union a global leader in the data-driven economy. It encompasses various regulations and acts designed to ensure a balanced, fair, and innovative digital environment.

- **Regulation 2018/1807 (Free Flow of Non-Personal Data)**: eliminates data localization restrictions within the EU and promotes data portability and interoperability.
- **Data Governance Act (DGA) (2022)**: establishes a framework to facilitate a safe data-sharing setting out conditions for their re-use and intermediation services.
- **Digital Services Act (DSA) + Digital Markets Act (DMA) (2022)**: complementary legislative measures to shape a safer digital space where individuals' rights are protected.
- **Data Act (2023)**: guarantees cross-sectoral fair access to and use of data, establishing clear rules that must be followed within the EU.
- **AI Act (2024)**: creates a legal framework for AI systems based on their risk level, ensuring safety, transparency, and fundamental rights.

Regulation 2018/1807

It has the purpose of ensuring free flow of data other than personal data laying down rules relating to data localization requirements. Scope of the application is the following:

- Applies to the processing of electronic data other than personal data.
- Includes data processing provided as a service to users within the EU or carried out by a person within the EU.
- Limited application to sets of data that contain both personal and non-personal data, where non-personal data provisions apply to the non-personal data part.

Data localization requirements: obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law.

In principle, data localization requirements are prohibited. This means that Member States cannot enforce rules that require data to be processed or stored within their territory, nor can they hinder the processing of data in another member state.
There are obligations upon the Member States to repeal any legal provision setting out data localization requirements. The goals are the following:

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

The **Data Governance Act (DGA)** is a key component of the EU's data strategy, aiming to establish a robust 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 entities
- Citizens

Data = 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.

EU Digital Services Act (DSA) and **EU Digital Market Act (DMA)** are complementary legislative measures under the EU's digital strategy to regulate digital space with the aim of:

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

The aim of the **Data Act** is to guarantee fair access to and use of data (fair distribution of the value of data by establishing clear and fair rules for accessing and using data within the European data economy), having so principles and guidelines applying to all sectors (cross-sectoral).

- Increasing legal certainty for companies and consumers.
- Mitigating 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) purpose is to establish a harmonised framework on artificial intelligence for respecting fundamental rights. The Act enhances the capabilities of AI systems improving predictions, optimizing operations and personalizing service delivery. It also gives the following advantages:

- Support socially and environmentally beneficial outcomes.
- Key competitive advantages to companies and the EU economy.