LAW AND DATA – OPEN QUESTIONS OVER THE YEARS

1) Please describe any legal provision included in EU primary law sources setting out the right to personal data protection. (up to 8 pts)

Sources of law are defined as the origins from which a law takes its authority and content. In the hierarchy of the European Union (EU) the highest source of law is primary law which contains different types of documents that define the principles and the guidelines on which the EU is based on. In particular, primary law contains: Treaty on European Union (TEU), Treaty on the Functioning of the European Union (TFEU), Charter of Fundamental Rights (CFR) and General Principles.
These fundamental documents, beyond guiding the EU in its activities, set out the right to personal data protection through different Articles, such as:

- TEU Article 2 highlights the EU's values, such as promoting respect for human dignity, democracy, freedom, equality, rule of law and respect for human rights.
- TEU Article 3 sets out the protection of citizens and values described in Article 2.
- TFEU Article 16 establishes the protection of personal data as a fundamental right for individuals within the European Union.
- CFR Article 8 guarantees the personal data of individuals are processed fairly and with the individual consent or other legitimate legal basis. Individuals have also the right to access their data and request rectifications if necessary. CFR Article 7 also establishes the right to privacy by protecting the individuals' personal life from potential intrusions. Article 7, even if not directly associated with the right to personal data protection, has been fundamental to the development of the notion of personal data protection.
- Even if these rights are recognized as fundamental, CFR Article 52 may impose legal limitations under certain conditions in a way to find a balance with other rights and/or situations of public interest.

2) Please describe the difference between EU regulations and directives. (up to 6 pts)

The European Union regulations and directives are typical acts belonging to the secondary sources of law. The general aim of secondary law is to establish laws that implement and apply the principles and guidelines defined in primary law.
Regulations are binding in their entirety, meaning that they must be followed and implemented as they are in each Member State legal system. There is no need for transposition since the regulation should be applied as it is in a way to promote and ensure coherence among all the European Union.
Directives, instead, are binding only on the results the directive seeks to achieve. This means that directives need transposition by each Member State who can decide the methods and processes (laws) to achieve the goals outlined by the EU directive (e.g., reduction of plastic).

3) Please describe the legal status of EU regulations. (up to 6 pts)

The European Union regulations are typical acts belonging to the secondary sources of law. The general aim of secondary law is to establish laws that implement and apply the principles and guidelines defined in primary law.
EU regulations hold a binding legal status and are directly applicable in all Member States without requiring transposition into each Member State legal system. Established under Article 288 of the Treaty on the Functioning of the European Union (TFEU), they ensure uniformity by creating consistent legal standards across the EU. Unlike directives, which allow Member States flexibility in implementation, regulations are immediately enforceable as law once adopted. They take precedence over conflicting

national laws, ensuring their primacy in the legal hierarchy. Regulations aim to harmonize laws to facilitate the functioning of the internal market and maintain legal consistency within the EU.

4) Please describe how the right to privacy evolved into the right to personal data protection. (up to 6 pts)

Initially the right to privacy was associated with a negative connotation which deals with the need to prevent intrusions in personal space. Nowadays, privacy is associated with a positive connotation: individuals can decide who can have access to their personal space rather than preventing intrusions. Exclusion became something individuals can choose and not avoid.
The distinction between Common Law and Civil Law traditions highlights different approaches to protect privacy. Common Law is oriented to the right to liberty, emphasizing freedom and protection from interference in private matters. Civil Law, instead, is oriented to the right to dignity, ensuring individuals' dignity is respected in all life activities. The concept of personal data does not derive from Common Law, but it is seen as part of individuals' dignity. This highlights how the right to personal data protection is the result of Civil Law development of the right to privacy.
Article 8(1) of the Charter of Fundamental Rights marked the transition from the notion of privacy to personal data protection. The article defines the right to protect personal data, defining it as any information related to an identified or identifiable natural person.

5) Please, illustrate the EU personal data protection package adopted since 2016. (up to 6 pts)

The EU personal data protection package adopted since 2016 primarily consists of General Data Protection Regulation (GDPR) and Data Protection Law Enforcement Directive (2016/680/EU).
The GDPR establishes rules for personal data protection, ensuring transparency, accountability, and individual rights across all Member States. It applies to businesses within and outside the EU that process EU citizens' data.
The Data Protection Law Enforcement Directive, instead, focuses on protecting personal data when processed by competent authorities for law enforcement purposes. Data protection is ensured by design and default. 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.

6) Please, explain what personal data means according to the EU personal data protection legislation and the difference with sensitive personal data (up to 8 pts)

According to GDPR Article 4(1), personal data is any information related to an identified or identifiable natural person. An identifiable natural person is anyone who can be identified, directly or indirectly, by information related to him/her, such as a name, identification number, location data, etc. The processing of personal data should be conducted with respect to human dignity and rights and with the consent of the data subject. This process should always operate in the limit of law.
The concept of personal data has its origins in earlier legal frameworks, including Convention 108, which was the first binding international instrument on data protection, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, a set of soft law universal standards.
Sensitive data, instead, is a special category of personal data that can highlight sensitive personal information such as ethnic origin, religious or philosophical beliefs, data concerning health or sexual orientation. According to GDPR Article 9, the process of sensitive data is prohibited in principle since process should not result in any form of discrimination. Anyway, there are lawful reasons for processing personal and sensitive data such as: substantial public interests (health, crimes, etc.), explicit consent, protection of vital interests.

7) Please, describe which are the main rights recognized to a data subject by the GDPR. (up to 8 pts)

According to GDPR, data subject is any natural or legal person who can be identified, directly or indirectly, through information regarding him/her such as: name, identification number, location data, etc. GDPR recognizes data subject different rights regarding the protection of personal data, such as:

- Right to be informed about purposes for which his/her data is processed.
- Right to access personal data held by organizations and understand how it is used.
- Right to rectification in case of inaccurate data held by organizations.
- Right to erasure ("right to be forgotten"), ensuring that data subject can be identified only within a certain temporary limit, also defined by the processing purposes.
- Right to restriction of data processing.
- Right to data portability. Data subject can request his/her processed data in a machine-readable format in a way to transfer them to another data controller.
- Right to object. Data subjects have the right to object to the process of their data under certain conditions such as profiling activities or direct marketing.

8) Please, explain the main principles for personal data processing. (up to 6 pts)

GDPR defines the main principles for personal data processing as:

- Lawfulness and Fairness are based on legal permission given from the Data Subject. Legal permission is necessary for performing a contract, complying with legal obligations, protecting vital interests, performance of a task of public interest and legitimate interests of the controller/third party.
- Transparency describes how personal data is collected, used and processed. The information that should be in plain is: identity of the controller, purposes for which data is processed, data subject rights and potential risks of processing activities.
- Purpose limitation ensures that personal data is processed only in accordance with the specified purposes and within the limit of law.
- Data minimization ensures that data must be relevant, adequate and limited to what is necessary in relation to the purposes.
- Accuracy ensures that data must be accurate and kept up to date. If inaccurate, erasure should be performed. Personal data should reflect the reality of any given situation.
- Storage limitation ensures that personal data shall be kept in a form that permits the identification of data subjects for no longer than necessary (processing purposes).
- Integrity and Confidentiality ensure that personal data shall be processed in a way to guarantee the security of such data.
- Accountability focuses on two key roles: Controller and Processor. Both entities must take responsibility for their handling of personal data.

9) Please describe a Data Protection Impact Assessment and its aims. (up to 8 pts)

The Data Protection Impact Assessment (DPIA) is a risk management system used by organizations to assess the impact of personal data processing activities on the protection of personal data, helping to identify/minimize the risks of a project. The controller, responsible for determining the purposes and means of personal data processing, works closely with the Data Protection Officer (DPO), an independent authority that ensures compliance with data protection legislation.

DPIA is mandatory only for specific scenarios, such as: automated processing activities (including profiling), large-scale processing of special categories of data and when monitoring data of public areas (e.g., traffic monitoring).
The contents of a DPIA are: systematic description of processing activities, purposes and legitimate interests of the controller (if any); assessment of the necessity and proportionality of processing activities in relation to the purposes; an assessment of the risks of such activities; the measures to mitigate such risks.
Also consider that DPIA is different from DPMS (Data Protection Management System) which is an IT framework to guarantee compliance with data protection legislation. DPIA instead provides a systematic assessment of processing activities, highlighting risks and countermeasures.

10) Please describe the main subjects involved in personal data processing activities and their rights and obligations according to the GDPR. (up to 8 pts)

According to GDPR, the main subjects involved in personal data processing activities are:

- Data Subject is any natural person that can be identified, directly or indirectly, through information regarding him/her such as name, identification number, location data, etc. GDPR recognizes data subject different rights: right to be informed about purposes, right to access, right to rectification, erasure, restriction, right to data portability and right to object.
- Controller is the natural or legal person, public authority or body that establishes the purposes and means by which personal data is processed. Controller has some obligations, in general it is responsible for any processing activity conducted by itself or on its behalf. It has also to adopt TOMs (Technical and Organizational Measures) to implement data protection principles, record processing activities and cooperate with data subjects and supervisory authorities.
- Processor is the natural or legal person, public authority or body that processes data on the behalf of the controller. Processor must act on the behalf of the controller, implement TOMs, maintain a record of processing activities, cooperate with the supervisory authority and designate a DPO where required.
- Data Protection Officer (DPO) is a person who advertises on compliance with data protection legislation.
- Supervisory Authority is an independent public authority which is established by each Member State pursuant to GDPR Article 51. Supervisory Authorities are responsible to handle data subjects' complaints, as well as monitoring and ensuring consistency in the application of GDPR.

11) Please describe the 2020 European Data Strategy conceived by the European Union. (up to 8 pts)

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): facilitate safe data-sharing setting out conditions for their re-use and intermediation services.
- Digital Services Act (DSA) and 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 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 respect for fundamental rights.