1. INTRODUCTION TO PERSONAL DATA PROTECTION: KEY CONCEPTS, REGULATORY FRAMEWORK AND SCOPE

What is personal data? A person's email address? Your phone number? The identification number? An image of a person captured by a camera? A person's wallet that has been stolen? A person that has filed a complaint or claim with a City Council? All of them are personal data. An important idea is that a person's identification data is personal data, but not just the mentioned cases.

Personal data is any information relating to an identified or identifiable individual. And when is an individual identified? When a name and surname appear, a mobile phone number, an identity document number, or any other data that identifies a person.

Personal data is also information that refers to an unidentified person, but that can be identified, that is, that is identifiable. And when is a person identifiable? When an identity can be determined from any element, such as an identification code or an employee number, or a job of a single person, such as a city council secretary or auditor.

Other **key concepts** in the field of data protection are:

- Processing of personal data: it is any operation on personal data, whether by automated procedures or not. Therefore, it is also a treatment when a person submits a paper instance. The collection of personal data is considered its capture, but also its consultation, use or dissemination, including its destruction, so when personal data is deleted, it must be done securely. In short, a treatment is any action that is carried out with personal data.

- Data Controller: it is the person, company or entity that decides the purposes and means of the treatment. Thus, the person in charge is the one who decides to initiate the collection and processing of personal data to consider them necessary for certain purposes.

- Data Processor: is the person, company or entity that processes personal data on behalf of the controller.

- Special categories of data: these are the types of personal data to which the data protection regulations grant maximum protection. This group includes data related to ethnic or racial origin, political opinions, religion, trade union membership, genetic or biometric data, health data or data related to sexual life or sexual orientation. In relation to these special categories of data, there is a general prohibition of processing, and it is only possible to process them in very specific cases.

- Pseudonymization, which is not the same as anonymization. Pseudonymization is the process of treating data in such a way that it can no longer be attributed to a person without the use of additional information, which must be stored separately and with very strict security measures. For example, police officers are not identified by name, but by a code.

- Anonymous data: are those in which the common thread between the information and a natural person has been broken, so it is not possible to re-identify it. Data protection regulations don’t apply to this, unlike pseudonymised data, to which it does.

The right to the protection of personal data is governed by **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC**, also known as **the General Data Protection Regulation (GDPR**). The GDPR has been mandatory in all states of the European Union since May 2018.

In relation to the **scope of application**, the GDPR applies to the totally or partially automated processing of personal data; and also, to non-automated processing of personal data contained in a file or intended to be included in it. An automated data processing is one that is carried out through electronic means. This would be the case for digital documents that a person saves on their computer. In contrast, non-automated processing is done on paper.

However, this rule **does not apply** in the following cases:

- Activities not covered by EU Law, such as national security or foreign policy.
- Treatments carried out by an individual in the exercise of exclusively personal or domestic activities (for example, when sending a WhatsApp to a friend).
- The processing of data related to deceased persons.

Apart from these exclusions, the regulations on personal data protection do not also apply to the processing of data relating to legal persons. Therefore, a City Council, a company or a neighbourhood association does not have the Right of Personal Data protection.

From a **territorial scope**, the GDPR establishes that it applies to the following processing of personal data:

1. Those carried out in the activities the processor or controller established in the EU, even if the processing takes place outside the Union.
2. Those related to interested parties who are located in the EU, carried out by a non-EU processor or controller, if the processing is related to the supply of goods or services to EU stakeholders or if the processing is linked to the control of the behaviour of persons who are in the EU, whether such behaviour takes place in the Union.
3. And the last case is related to the processing of data carried out by a person not established in the EU, but in a place where the law of EU member states applies.