



DATA PROTECTION FOR PROCESSORS

What is *personal data*?

Personal data is more than a first name, surname, date of birth or address. It extends to online identifiers and **all types of data that, directly or indirectly, make it possible to determine a person's identity**. For example, IP address, SIM card IMSI, or the identifier of your terminal.

Pseudonymised data also form part of the concept of personal data, i.e. data that could be attributed to a natural person through the use of additional information.

Biometric data (e.g. a person's image, voice or fingerprint) and personal data publicly accessible on the internet or social networks would also be subject to the regulation.

Examples of personal data include:

Location — Physical attributes — Economic
Cultural or social information — Online identification — IPS



Processing of personal data

Processing is considered to be any **operation** carried out on personal data, whether manual or automated. For example: registration for a **service**, mere **access** or consultation of a database, **destruction or deletion** of documents containing personal data, **modification** of data, **transfer** of data to third parties, restriction of access, among others.

Principles relating to processing of **personal data**

Any processing of personal data must respect the principles of data protection.



LAWFULNESS, FAIRNESS AND TRANSPARENCY

The processing must be based on a legitimate basis, have a specified purpose and be faithful to that commitment to inform.



PURPOSE LIMITATION

Commitment to process the information exclusively for the informed purpose.



DATA MINIMISATION

Only the data necessary for the purpose for which it is processed will be used



ACCURACY

Personal data must be accurate and up to date.



STORAGE LIMITATION

The information must be kept for the time necessary for the purposes defined.



INTEGRITY AND CONFIDENTIALITY (SECURITY)

Protect personal data from any risk by maintaining Integrity, availability and confidentiality.



ACCOUNTABILITY

Maintain privacy awareness and culture by complying with the detail of the above principles.

Suppliers *Responsabilities*

The provider must be aware of its responsibilities in the processing of information in order to guarantee the privacy of the individuals whose data will be processed. The terms of the service provided are set out in a contractual document called Data Protection Agreement (DPA). This document contains, among others, the following commitments:



- To process the data according to the **instructions** of the data controller
- **Duty of confidentiality** of all persons accessing the data
- To ensure compliance with **security measures**
- In cases where the provider **hires sub-processors**, the authorisation of the data controller could be required
- **Assisting** the controller in the fulfilment of certain obligations, provided that they apply to the service provided, such as support in the exercise of rights or communication in relation to security incidents in relation to the service provided
- **At the end of the provision of the service**, the return or destruction of data (at the choice of the controller)

