2. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

The principles relating to the processing of personal data are set out in Article 5 of the European Regulation and are as follows:

- The **principle of lawfulness** implies that personal data can only be processed if there is at least one legal basis allowing the processing. This will be addressed in the next section.

- The **principle of fairness** prohibits the collection of personal data by fraudulent, unfair or illegal means. An example of unfair data collection would be a user satisfaction survey on the quality of the selective collection service, which ensures that it is done anonymously, but it turns out that this is not true, and that they can link the responses to the person conducting the survey.

- The **principle of transparency** requires that data subjects be informed of what will be done with their data when it is collected.

- The **principle of purpose limitation** implies that data should be collected for specific, explicit and legitimate purposes, and that they should not be further processed in a manner incompatible with those purposes. That is, data collected for a purpose, cannot be used for anything else. However, the further processing of personal data is not considered incompatible with archiving purposes in the public interest, scientific and historical research or statistics.

- The **principle of data minimisation** requires that the personal data processed be adequate, relevant and limited to the purposes for which it is processed. In other words, only data that is necessary for the corresponding purpose should be collected and processed, and therefore it is necessary to avoid the processing of data that would be disproportionate.

- The **principle of accuracy** requires the processing of personal data that is accurate and up-to-date. It is also necessary to delete or rectify without delay personal data that is inaccurate or obsolete.

- The **principle of storage limitation** means that the retention of data in such a way that individuals can be identified, should only be maintained for the time necessary for the purposes pursued. After this period, they can only be kept for research, statistical or archival purposes of public interest.

- The **principle of integrity and confidentiality** obliges to guarantee adequate security, through the application of appropriate technical or organizational measures, in order to prevent data from being known to unauthorized persons, or from being lost. In relation to this principle, a duty of confidentiality is imposed on all staff.

- The **principle of proactive responsibility or *accountability*** requires the controller to be aware, diligent and proactive in relation to all processing of personal data. Therefore, the controller has the duty to ensure that all duties imposed by data protection regulations are met. And not only must comply, but must have the capacity to prove it.