

Release of the Code of Best Practices in Data Protection for Big Data Projects

Big Data is extremely important today as it provides multiple benefits to both businesses and data subjects. In this sense, and due to its rapid growth in recent years, it represents a new challenge as a new way of processing personal data.

Referencing GDPR, the SDPA and ISMS Forum Spain have jointly drafted a Code of Best Practices in Data Protection for Big Data Projects (hereinafter, "The Code").

The Code is structured as follows:

Firstly, it gives an overview of what Big Data is and the applicable legal framework: the Organic Law 15/1999, of December 13 on Data Protection and the GDPR.

Secondly, it defines the roles of data processors and data controllers in big data, and focuses on the implications of data processing. These include the origin of the data, its quality and retention, transparency before the data subject, necessity of obtaining data subject's consent or, when appropriate, relying on a different legitimation.

The Code mentions how privacy shall be taken into account from the outset of a data protection project: describing certain principles and procedures to ensure compliance such as privacy by design, accountability, data protection, impact assessment and the use of dissociated data.

The Code provides practical advice and summarises measures to improve privacy and security in big data projects, such as:

- **Minimisation:** The amount of personal data in big data projects should be limited as much as possible (minimisation of data).
- **Aggregation:** Personal data must be processed at the highest possible level of aggregation and with the least amount of detail.
- **Hide:** Personal data and its interrelationships must be protected in a way that makes them invisible to users.
- **Separate:** Personal data must be processed separately and distributed as so.
- **Inform:** Data subject should be adequately informed when their personal data will be processed (clarity).
- **Control:** The data subjects must be able to exercise their rights and know the processing of their data at all times.
- **Comply:** It must be enforced with a privacy policy compatible with legal requirements.
- **Demonstration:** You must be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

As a conclusion, the Code states that the trust of the data subjects is crucial for ensuring that all parties benefit from big data projects. Compliance with the Code and its measures and principles will guarantee this mutual trust.