

# **INTERNAL INFORMATION SYSTEM POLICY**

November 2023

## 1. Purpose

The purpose of this Policy is to establish principles, strategy and characteristics of the Internal Information System (hereinafter IIS) of the companies that are part of the FINSOLUTIA GROUP.

The Policy is applicable to any natural or legal person who has a relationship with any company in FINSOLUTIA group and reports a breach or irregularity, illicit or criminal act, as well as any actions or omissions that may constitute breaches of European Union Law, as indicated in Law 2/2023, Law 93/2021, of 20 December and the Directive. Therefore, it is applicable to all its directors, managers, and employees of all group companies, as well as to its clients, suppliers, brokers, collaborators and other third parties with whom business relations are maintained, as well as to persons with an employment or statutory relationship that has already ended, in addition to all the persons indicated in the aforementioned Law.

## 2. Principles of IIS

The principles of the Internal Information System implemented by FINSOLUTIA are as follows:

- Presumption of innocence.
- Contradiction.
- Confidentiality.
- Possibility of anonymous reporting.
- Non-reprisals against the Reporting Party, this concept encompassing the conduct described in article 36 of Law 2/2023 of 20 February and article 21 of Law 93/2021 of 20 December, regulating the protection of persons who report regulatory infringements and the fight against corruption.
- Right of information to data subjects.

The Internal Reporting System implemented by FINSOLUTIA has been duly consulted with employees and guarantees confidentiality of the identity of the Reporting Party, the reported Party, as well as the third parties to whom the reports refer. Furthermore, it is guaranteed that there will be no retaliation or negative consequences against the Reporting Party for the fact of the report, unless the internal investigation determines that the report has been made with knowledge of its truthfulness or that it has been made with reckless disregard for the truth, bad faith or abuse of rights.

## 3. Responsible Committee

In accordance with Article 8 of Law 2/2023, FINSOLUTIA's management body has appointed the Ethics Committee as responsible for Internal Information System, who delegates this function to the Head of the Compliance Department. He is responsible for the implementation of the Internal Reporting System and for ensuring compliance with it. In order to avoid possible conflicts of interest, the management of any

report received will be assigned to a responsible third party, expert in the field and external to FINSOLUTIA.

Reporting Parties may send a report through the form available makes on FINSOLUTIA home page of its corporate website, on the organisation's intranet or directly through the following link:

[Access to the Ethical Channel](#)

In addition, the Reporting Party may address directly with the responsible for the Internal Information System at company's offices, as well as accessing external information channels with the competent authorities and, where appropriate, with the institutions, bodies or agencies of the European Union.

## 4. Reports management and research

FINSOLUTIA has an internal regulation that sets all aspects related to management and investigation of reports received through organisation's ethical channel, ensuring compliance with applicable regulations and more specifically with Law 2/2023, of 20 February (and/or Law 93/2021, of 20 December), regulating the protection of individuals who report regulatory infringements and fight against corruption.

All reports will be managed and approved for processing will be duly investigated. In any case, if deemed necessary, the sanctioning or precautionary measures deemed appropriate will be taken.

FINSOLUTIA's Internal Information System complies with Law 2/2023, Organic Law 3/2018 on Data Protection and Guarantee of Digital Rights and the General Data Protection Regulation (Law 93/2021, of 20 December, Law 58/2019, of 08 August data protection law) having implemented the necessary personal data security measures. Adequate compliance with personal data processing is ensured, and in particular with respect to data subjects rights to be informed about the processing of such data. More specifically, the use of personal data only for the relevant purposes, minimisation of data processed, compliance with personal data retention periods, as well as the exercise of rights by data subjects are duly assured.

## REVISIONS

*This document is a controlled document that supersedes all previous versions. Copies bearing versions earlier than the current version or bearing a date prior to the date of publication will not be considered valid. Any person obtaining a printed version of this document is responsible for ensuring that the version they have is the latest version. The current version of this document is formally published in the Finsolutia Internal Repository in the Integrated Management System.*

*All product names used in this document are for identification purposes only and may be trademarks of their respective organisations.*