finerge

INTERNAL BREACH REPORTING POLICY

VERSION 1.0 07.06.2023

finerge

1.
LEGAL FRAMEWORK

finerge

Finerge Group is committed to maintaining the highest standards of conduct and ethics and preventing corruption and associated breaches. This commitment involves all employees, directors, department heads, suppliers, and other third parties who interact with Finerge. To prevent corruption and misconduct, Finerge requires that all parties with whom it has a direct labor, commercial, or professional relationship comply with applicable laws and codes of conduct. Collaboration with these parties to detect and prevent illegal or irregular conduct that could damage Finerge's reputation is critical.

To support these efforts, the European Parliament and Council enacted Directive (EU) 2019/1937 on the protection of individuals who report breaches of Union law (EU Whistleblowers Directive). This directive aims to enhance the enforcement of Union law by providing a high level of protection to those who report breaches. The directive also includes provisions for the design of internal reporting channels, allowing reporting individuals to choose the most appropriate channel for their specific circumstances.

Member States are required to ensure that both public and private entities establish channels and procedures for internal reporting of breaches under article 8 of the directive.

Law no. 93/2021, of 20 December, establishes the general rules for protecting persons who report breaches and transposes Directive (EU) 2019/1937 into Portuguese Law. This legislation mandates the establishment of internal reporting channels. Similarly, Decree-Law no. 109-E/2021, of 9 December, outlines general rules for preventing corruption and requires the inclusion of reporting channels as part of compliance programs.

In Spain, Law no. 2/2023, of 20 February, governs the protection of whistleblowers and the prevention of corruption, and transposes Directive (EU) 2019/1937 into Spanish Law.

In compliance with these laws and regulations, Finerge Group has established an Internal Reporting Channel that aligns with applicable legislation. The procedures governing the use of this channel are outlined in the present Policy.

In addition to these measures, Finerge Group is committed to complying with all relevant legislation and regulations in the countries where it operates.

2. INTERNAL REPORTING CHANNEL

2.1

Finerge Group has established an internal reporting channel to facilitate the reporting and follow-up of information related to breaches (hereinafter «Reporting Channel»). This channel ensures compliance with the security, confidentiality, and data protection requirements outlined in the present Policy, as well as applicable legislation.

2.2

The Reporting Channel is accessible via the following link: Reporting Channel. It is designed to maintain the completeness and integrity of the reports, protect the identity of the reporting person and any third persons mentioned in the report, and prevent unauthorized access.

2.3

The Reporting Channel is also designed to ensure that records of the reports are maintained in accordance with applicable regulations.

3. SCOPE

3.1

Reports submitted through the Reporting Channel should only relate to instances of corruption or associated breaches that have the potential to impact the contractual or commercial relationship between Finerge Group and its employees, suppliers, or other parties with whom it has a direct relationship. These include:

a)
Violations to Finerge Group's current Code of Ethics and Conduct;

b)
Violations to Finerge Group's current Suppliers' Code of Conduct;

c)
Any acts or omissions that constitute breaches of European Union Law, national regulations implementing or complying with EU Law, or other related legislation in the following areas:

1. Public procurement;

2. Financial services, products and markets, and prevention of money laundering and terrorist financing;

3. Product safety and compliance;

4. Transport safety;

5. Protection of the environment;

6. Radiation protection and nuclear safety;

7. Food and feed safety, animal health and welfare;

8. Public health;

9. Consumer protection;

10. Protection of privacy and personal data, and security of network and information systems.

D)

All acts or omissions that constitute fraud or other illegal activities that affect the European Union's financial interests, as referred to in article 325 of the Treaty on the Functioning of the European Union ("TFEU").

E)

All acts or omissions in breach of the rules of the European internal market, including breaches of EU competition and State aid rules, as well as corporate tax law.

3.2

All Finerge Group employees, suppliers and third parties with a direct relationship and a legitimate commercial or professional interest (hereinafter "Reporting Persons"), regardless of their rank and geographical or working location, may report via the Reporting Channel any of the breaches listed above of which they have become aware in their work-related context and which affect the Finerge Group,

and which have been committed by other employees, suppliers or third parties with whom the Finerge Group has a direct relationship, by making a report in good faith and with solid grounds to believe the information contained in the report is accurate.

3.3

The internal report may include breaches that have already occurred, are currently occurring, or are foreseeable in the future.

3.4

When submitting a report, Reporting Persons are instructed to provide only specific and objective information to determine whether the subject matter of the claim falls within the defined scope. It's important to note that private or sensitive data, such as a person's sex life, political or religious opinions, health, or trade union affiliation, should not be included in the report, unless it's crucial to understanding the report scope.

3.5

The Reporting Channel complements rather than replaces the Finerge Group's normal communication channels for its employees, suppliers and third parties with whom it has a direct relationship.

4.
REPORTING PERSONS

finerge

4.1

The Reporting Channel is a means for the following categories of individuals to report breaches of conduct or unethical behaviour within the Finerge Group:

a)
Finerge Group employees;

b)
Former Finerge Group employees;

c)
Candidates in recruitment processes and bidders in pre-contract negotiations;

d)
Service providers, contractors, subcontractors and suppliers;

e)
Finerge Group's shareholders and boards of directors' members, as well as audit and supervisory bodies, including non-executive members.

4.2

For the purposes of the provisions of 4.1 (c), candidates in recruitment processes, including those with no professional relationship with Finerge, are deemed Reporting Persons.

4.3

Reporting Persons who use the Reporting Channel to report breaches of conduct or unethical behaviour within the Finerge Group qualify for protection under applicable legislation. This protection includes the prohibition of retaliation against Reporting Persons and other protective measures.

4.4

The above protection measures extend to:

a)
Individuals who support the reporting person in the reporting process;

b)
Third parties who are connected to the Reporting Persons, namely work colleagues and family members, who could suffer retaliation in a work-related context;

c)
Legal entities owned or controlled by the Reporting Person, and legal entities the Reporting Person works for or is connected to in a work-related context.

5. CHANNELS AND CONFIDENTIALITY

5.1

Reporting Persons can submit written claims/reports through the Reporting Channel either anonymously or by providing their name.

5.2

Finerge Group will maintain strict confidentiality of the identity of the Reporting Persons and any other information that could reveal their identity. Only the Audit Committee will have access to the information.

5.3

Any person who receives information about the reports must keep it confidential.

5.4

If required by law or court order, Reporting Person's name may be disclosed, but only after the Reporting Person has been given written notice of the reasons for disclosure and in compliance with applicable legislation.

6. PERSONAL DATA PROTECTION

6.1

The Reporting Channel allows the collection of the following personal data regarding the reported breaches:

a)
Identifying data of both the Reporting Person and the concerned party, including names, contact details, and position/employee number;

b)
The relationship between the Reporting Person and the Finerge Group and/or the concerned Group company;

c)
Alleged breach details;

d)
Documentary proof of the alleged breaches.

6.2

In accordance with applicable regulations on personal data protection, the Reporting Person and the concerned party will be informed about who will handle their personal data during the report process and how to exercise their rights to access, amend, delete, or challenge the recorded personal data.

6.3

In any event, the concerned party has the right to access their personal data only.

6.4

Personal data included in the report, as well as any information collected during the internal investigation, will only be used to lawfully detect, investigate, and assess suspected non-compliance with labour, commercial, or professional duties outlined in the employment contract, including failure to adhere to Finerge policies and internal regulations.

6.5

Under applicable personal data protection legislation, those responsible for handling the data are the following:

a)
the Finerge Group company with a labour, commercial, or professional relationship with the Reporting Person or the concerned party, as well as

b)
Finerge S.A., the holding company. The latter appointed the Audit Committee for receiving and following up on internal reports and ensuring compliance with the Code of Ethics and Conduct, the Suppliers Code of Conduct, and other internal policies and regulations, as described in chapter 8 of this Policy.

7. RECORD KEEPING OF REPORTS

7.1

The Audit Committee shall keep an up-to-date register of all communications received through the Reporting Channel, as well as, where applicable, the internal investigation conducted and the measures taken for a period of at least 5 years, or during the entire course of any legal or administrative proceedings relating to the reports whenever they exceed that period.

7.2

The aforesaid reports register shall adopt the technical and organisational security measures provided for in applicable data protection legislation.

7.3

aTo ensure record keeping is always current, it must contain, at least, the following information:

A)
Date of receiving the report;

B)
Method of receiving the report;

C)
Reporting Person's and the concerned party personal information;

D)
Report Summary as well as alleged facts;

E)
Timings of the information provided by Reporting Persons and concerned parties;

F)
Follow-up, as well as corresponding investigation documentation where applicable;

G)
Follow-up status.

7.4

Any personal data collected during the internal report process, which is no longer necessary or relevant, or after three (3) months of being collected, shall be immediately erased unless an investigation is ongoing.

7.5

Personal data related to internal reports that do not require follow-up will be deleted immediately.

7.6

Data erasing will involve data blocking, which means that it will be held in reserve and made available only to relevant authorities to assess potential liabilities during the legally defined period. Once this period is over, the data will be physically deleted.

8. REPORTING PROCESS

8.1

Reports may be made through the Reporting Channel.

8.2

Upon receiving a claim/internal report, the Audit Committee shall inform the Reporting Person within 7 days and provide them with clear and accessible information on the requirements, relevant authorities, and form and admissibility of external reports, as required by applicable legislation.

8.3

During the report follow-up, the Audit Committee shall first check whether the report falls within the Reporting Channel's scope, as defined in Chapter 3 of this Policy. If so, they will take internal actions to verify the report by contacting relevant departments and divisions, as necessary, and initiate an internal investigation or inform relevant authorities.

8.4

If the report is outside the scope of the Reporting Channel as defined in Chapter 3 of this policy and/or is groundless, it shall be dismissed.

8.5

During the course of an internal investigation, both the Audit Committee and the department or division that is taking part in or cooperating with the investigation, may gather information and documents they deem appropriate from any Finerge Group company or division, always bearing relevance in the nature of the alleged facts.

8.6

The Audit Committee shall inform the Reporting Person of the steps to be taken or already taken to follow up on the report and the respective grounds, within 3 months of receiving the report.

8.7

Based on the conclusions of the internal investigation, the Audit Committee may propose taking the following steps:

a)
Immediate non-conformity correction;

b)
Propose penalties or corrective actions, when non-compliance is verified, which may range from a simple warning to dismissal and the perpetrator having to pay compensation consequentially for non-compliance;

c)
If no non-compliance or groundless/bad faith/falsified claim is confirmed after the investigation concludes, the claim will be dismissed.

8.8

The Reporting Person may request a claim outcome analysis from the Audit Committee within 15 days of its conclusion.

8.9

If a member of the investigation team is the subject of a report, they must excuse themselves immediately due to a conflict of interest and will no longer participate in the investigation.

9. MEMBERS DESIGNATED FOR HANDLING REPORTS

9.1

The Reporting Channel is used for receiving and following up on internal reports by the Audit Committee.

9.2

The Audit Committee must be independent and impartial, ensure confidentiality and data protection, maintain secrecy, and avoid conflicts of interest while performing their duties.

Av. D. Afonso Henriques 1345
4450-017 Matosinhos, Portugal

Av. Eng. Duarte Pacheco, 26-2º
1070-110 Lisboa, Portugal

Calle Quintanavides 13
Edifício 3, Planta 3
28050 Madrid

8-10 Rue Mathias Hardt,
L-1717 Luxemburgo

+351 226 080 180

info.geral@finerge.pt

finerge.pt

finerge