# WHISTLEBLOWING PROCEDURE



TITLE: WHISTLEBLOWING PROCEDURE

SCOPE OF APPLICATION: all reports of unlawful conduct relevant pursuant to Legislative Decree 231/2001, breaches of the Organization, Management and Control Model, the Code of Ethics, or national and European Union legislation pursuant to Legislative Decree 24/2023 (the so-called "Whistleblowing Law"), made by employees, collaborators and recipients of the 231 Model who become aware of such matters in the context of their relationship with KAARAL.

PURPOSE: to define the methods for receiving, handling and closing whistleblowing reports, ensuring the confidentiality of the reporting person and compliance with Legislative Decree 24/2023.

## DESCRIPTION AND APPROVAL OF REVISIONS

| Rev. | Date | Description of change |
|---|---|---|
| 0 | 11/24 | First issue |
| 1 | 08/26 | Reformatted in accordance with the document layout used for KAARAL management system procedures; a maximum period of 60 days from receipt of the report to its closure/filing has been introduced for handling the report (section 4.5). |

**WHISTLEBLOWING PROCEDURE**

## 1. REFERENCES

Legislative Decree no. 24 of 10 March 2023 (the so-called "Whistleblowing Law")
Organization, Management and Control Model pursuant to Legislative Decree no. 231 of 8 June 2001
Company Code of Ethics
Procedures and operating instructions relating to corporate management systems

## 2. RESPONSIBILITIES AND COMPETENCIES

The offices and functions involved in the activities covered by this procedure are:

• Management;

• the Supervisory Body (hereinafter "OdV") established pursuant to Legislative Decree 231/01: receives, registers, examines and files reports, ensuring the confidentiality of the reporting person and traceability of the process;

• all recipients of the Organization, Management and Control Model pursuant to Legislative Decree 231/01, who may report unlawful conduct relevant under Legislative Decree 231/2001 and based on precise and consistent factual elements, or breaches of the Company's organization and management model, of which they have become aware by reason of the duties performed;

• the HR function: receives the outcome of the investigation for the possible initiation of disciplinary proceedings.

## 3. DEFINITIONS AND ABBREVIATIONS

The following apply:

• the terms and definitions set out in the latest edition of the KAARAL Quality Management Manual;

• the acronyms and abbreviations listed in the relevant list.

Whistleblowing: a report made by a person who, in the course of carrying out their duties, becomes aware of an offence, a risk or a hazardous situation that may cause harm to the company/entity for which they work, as well as to customers, colleagues, citizens or any other category of person.

OdV: Supervisory Body established pursuant to Legislative Decree 231/01.

Software: the "My Whistleblowing" add-on to the "My Governance" software, a reporting channel designed to ensure, by electronic means, the confidentiality of the reporting person's identity.

Reporting Person: the person who makes a report pursuant to this procedure.

The Company, which is attentive to ethical issues and proper business conduct, has implemented internal reporting systems to enable the persons identified by law to report breaches of national or European Union provisions that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private work-related context, including breaches of the Code of Ethics or of the Organization, Management and Control Model pursuant to Legislative Decree 231/01.

The Whistleblowing Law identifies:

• the persons who may make a report;

• the acts or facts that may be reported, as well as the requirements that reports must meet in order to be taken into consideration;

• the methods through which suspected breaches may be reported and the persons responsible for receiving reports;

• the preliminary assessment and, where appropriate, investigation process once a report is made;

• the guarantee of confidentiality and protection of the personal data of the reporting person, any person concerned and the data contained in the report;

• the prohibition of retaliation and discrimination against the reporting person.

# 4. PROCEDURE DESCRIPTION

## 4.1 Reference framework

The legislator approved Legislative Decree 24/2023 (the so-called "Whistleblowing Law"), which defined, inter alia:

• the protection measures for the person, as identified in Article 3 of the Whistleblowing Law, who makes a report;

• the obligations of entities and companies with regard to the prohibition of retaliatory acts and non-discrimination against reporting persons, and protection of their confidentiality;

• the need for one or more reporting channels (including electronic channels) enabling reporting persons to submit reports while ensuring the confidentiality of the identity of the reporting person, the person concerned and any person mentioned in the report, as well as the content of the report and the related documentation;

• the need to consult the workers' representatives or trade union organizations referred to in Article 51 of Legislative Decree no. 81 of 2015 before activating the aforementioned reporting channels;

• the conditions for making an external report;

• the prohibition of retaliatory or discriminatory acts against the reporting person for reasons connected with the report;

• the need to provide, within the disciplinary system adopted pursuant to Article 6, paragraph 2, letter e), of Legislative Decree 231/2001, for sanctions against persons found responsible for the offences referred to in paragraph 1 of Article 21 of the Whistleblowing Law.

## 4.2 Subject matter

The purpose of this procedure is to define the operating methods for handling reports and any consequent investigations concerning matters of which authorized persons have become aware by reason of the duties performed.

The cases excluded by the Whistleblowing Law do not fall within the scope of this procedure, including:

a. complaints, claims or requests linked to a personal interest of the reporting person or of the person who has filed a complaint with the judicial or accounting authority, which relate exclusively to their individual employment or public employment relationships, or to their employment or public employment relationships with hierarchically superior persons;

b. reports of breaches where such matters are already mandatorily regulated by European Union or national acts, or by national acts implementing European Union acts;

c. reports of breaches concerning national security, as well as contracts relating to defence or national security aspects, unless such aspects fall within the relevant secondary law of the European Union.

## 4.3 Objectives

The objective of this procedure is to bring to light unlawful acts or irregularities within the Company, clarifying and facilitating the use of the reporting mechanism by the reporting person and removing any factors that may hinder or discourage its use.

The procedure therefore aims, on the one hand, to provide the reporting person with clear operational guidance concerning the subject matter, contents, recipients and methods of transmitting reports and, on the other hand, to inform them of the forms of protection and confidentiality granted and guaranteed to them.

To ensure that the Company's values are shared, respected and put into practice in the working life of its stakeholders.

## 4.4 Subject matter and requirements of the report

The Company's Organization, Management and Control Model pursuant to Legislative Decree 231/01 identifies the methods for submitting to the Supervisory Body reports concerning conduct that may amount to the possible commission of offences relevant under Legislative Decree 231/2001 or, in any event, breaches of the Model.

To facilitate reporting, the following channel has been established:

## WHISTLEBLOWING PROCEDURE

• through the My Whistleblowing add-on to the My Governance software, as a reporting channel designed to ensure, by electronic means, the confidentiality of the reporting person's identity, in compliance with applicable legislation (hereinafter, the "Software").

The Company may also take anonymous reports into consideration, provided that they are sufficiently detailed[1] and include enough particulars to bring facts and situations to light and relate them to specific contexts (e.g. documentary evidence, names or specific job titles, references to specific offices, proceedings or events, etc.).

A report, including a non-anonymous report, must be detailed and as complete and exhaustive as possible.

The reporting person is required to provide all available and useful elements enabling the competent persons to carry out the necessary and appropriate checks and verification of the validity of the reported facts, including:

i. a clear and complete description of the facts being reported;

ii. the time and place in which the reported facts occurred;

iii. the personal details or other information enabling identification of the person(s) who carried out the reported acts (e.g. job title, work location where the activity is performed);

iv. any documents supporting the report;

v. the identification of any other persons who may provide information on the facts being reported;

vi. any other information that may provide useful confirmation of the existence of the reported facts.

For a report to be considered sufficiently detailed, these requirements do not necessarily have to be met simultaneously, taking into account that the reporting person may not have all the information requested.

Through the electronic channel, and therefore via the Software, the reporting person will be guided through each stage of the report and will be required, in order to provide the fullest possible details, to complete a series of mandatory fields in accordance with the required criteria.

It is essential that the information provided be directly known to the reporting person and not merely reported or relayed by other persons.

### 4.5 Handling of reports

Once a report has been received through the channels provided for in this procedure, it is handled in four stages:

a. registration and safekeeping;

b. preliminary assessment;

c. investigation and communication of the outcome;

d. filing.

Maximum closure period: the entire report-handling process, from the date of receipt (registration) to the date of closure/filing, must be completed within a maximum period of 60 (sixty) days. Progress status and the relevant dates are recorded in the reports register referred to under letter a) below. If the complexity of the case does not allow this deadline to be met, the OdV shall document the reasons for the delay and record them in the same register, notifying the reporting person where possible.

a. Registration and safekeeping

Where the report is submitted through the Software, the Software itself will provide for complete and confidential registration in accordance with the applicable legislation.

Where the report is received in paper form or through other means, upon receipt the Supervisory Body, through its secretariat, assigns the reporting person a specific alphanumeric ID and records the details of the report in an electronic and/or paper register, in particular:

• date and time;

• reporting person;

[1] A report may be considered sufficiently detailed if it makes it possible to identify factual elements reasonably sufficient to initiate an investigation (e.g. the offence committed, the relevant period and, where applicable, the value, causes and purpose of the offence, the company/division concerned, the persons/units involved, and the anomaly in the control system).

• subject matter of the report;

• notes;

• status of the report, to be completed at each stage of the process (e.g. preliminary assessment, investigation and communication of the evidence identified, filing), with the relevant date, for the purpose of verifying compliance with the maximum 60-day period referred to above.

Instructions and organizational measures are adopted to protect the confidentiality of the reports register: its location, the persons authorized to access it, instructions to such persons regarding the obligation of absolute confidentiality, and measures ensuring that the documentation is inaccessible to unauthorized persons (e.g. locked cabinet).

b. Preliminary assessment

The preliminary assessment is intended to verify the merits of the report received. For this purpose, the OdV meets to assess the contents by carrying out an initial screening and:

• where it immediately finds that the report is manifestly unfounded, it proceeds with immediate filing;

• where the report is not sufficiently detailed, it requests further information from the reporting person where possible; where it is not possible to collect sufficient information to substantiate the report and commence the investigation, the report is filed;

• where the report appears sufficiently detailed and supported by precise and consistent factual elements, it proceeds with the investigation stages.

c. Investigation and communication of the outcome

The investigation consists of all activities aimed at verifying the content of reports received and gathering useful elements for the subsequent assessment stage, while ensuring the utmost confidentiality regarding the identity of the reporting person and the subject matter of the report.

The main purpose of the investigation is to verify the truthfulness of the information under review, providing an accurate description of the facts established through objective audit procedures and investigative techniques.

The person responsible for the investigation is Internal Control/Audit and/or external consultants appointed ad hoc and/or the committee of shareholders of the company holding more than 20% (twenty per cent) of the share capital.

Everyone is required to cooperate with the person responsible for the investigation in carrying it out.

For each investigation, the person responsible for the investigation prepares a final report containing at least:

• the facts established;

• the evidence collected;

• the causes and deficiencies that allowed the reported situation to occur.

At the conclusion of the investigations, where the report received is found to be unfounded, the OdV files the report and, where possible, informs the reporting person.

Where the report is found to be substantiated, the OdV involves the relevant company managers so that the necessary and most appropriate mitigation and/or corrective actions may be undertaken.

It forwards the outcome of the investigation to the HR function for the possible initiation of disciplinary proceedings aimed, where appropriate, at imposing disciplinary sanctions in accordance with applicable legislation and the relevant collective bargaining agreements.

d. Filing

In order to ensure traceability, confidentiality, retention and retrievability of data throughout the entire process, documents are stored and filed both digitally, through the Software and password-protected network folders, and in paper form in a specially secured cabinet located at the Company's premises, accessible only to specifically authorized and appropriately instructed persons.

All documentation will be retained for 10 years from the date on which the activities are closed, without prejudice to any longer statutory retention periods expressly provided for by law.

In accordance with applicable law and the Company's privacy procedures, the personal data of persons involved in and/or mentioned in reports are protected.

### 4.6 Protection of the reporting person

The entire process must in all cases guarantee the confidentiality of the reporting person's identity from the moment the report is received and throughout every subsequent stage.

For this purpose, in accordance with applicable legislation, the Company has established a series of mechanisms to protect non-anonymous reporting persons, providing for:

a. protection of the confidentiality of the reporting person;

b. prohibition of discrimination against the reporting person.

a. Protection of the confidentiality of the reporting person

Use of the Software guarantees complete confidentiality of the reporting person, as only the OdV may access the report.

In the event of reports made through any other methods, once the report has been received and registered, the recipients assign the reporting person a specific anonymous ID. To protect the confidentiality of the reporting person, the ID will be used in all official documents and communications during the investigation.

Within any disciplinary proceedings initiated against the person concerned:

• if the allegations are based on findings that are separate and additional to the report, even if resulting from it, the identity of the reporting person may not be disclosed;

• if the allegations are based wholly or partly on the report, the identity of the reporting person may be disclosed to the person(s) concerned by the report where both of the following requirements are met: the consent of the reporting person and the proven need of the person concerned to know the reporting person's identity in order to fully exercise the right of defence.

b. Prohibition of discrimination against the reporting person

The reporting person may not be sanctioned, dismissed or subjected to any discriminatory measure, whether direct or indirect, affecting working conditions for reasons directly or indirectly connected with the report.

Discriminatory measures include unjustified disciplinary actions, workplace harassment, any changes to duties or workplace location, and any other detrimental change to working conditions that constitutes retaliation for the report. A reporting person who believes they have suffered discrimination as a result of making a report must provide the Company's OdV with a detailed notification thereof.

A reporting person who believes they have suffered discrimination may bring legal proceedings against the person responsible for the discrimination and also against the Company if the Company actively participated in the discrimination. In such a case, the law provides for a reversal of the burden of proof: the Company will therefore be required to demonstrate that the change in the reporting person's working conditions did not arise from the report.

## 4.7 Breach of the procedure

Failure to comply with this procedure may result, for Company employees, in the application of the Company's Disciplinary System, in accordance with applicable legislation and the relevant collective bargaining agreements.