



COMPANY	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use


# Whistleblowing

-

## Process for the management of internal procedures


DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	<p style="text-align: center;">WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS</p>	<p style="text-align: center;">DATE: 14 Dec 2023 Type: Internal use</p>

Document manager	Whistleblowing team
Editorial board	DataConSec Srl
Approval:	Management

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use


### History of modifications

Version	Date	Changes Description
01	12/14/2023	Emission
		-
		-


DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	<b>WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS</b>	DATE: 14 Dec 2023 Type: Internal use

## SUMMARY

<b>1. SCOPE AND FIELD OF APPLICATION</b>	<b>6</b>
1.1. Recipients and diffusion	6
1.2. CONTACTS	6
1.3. General rules for approval, update, storage, distribution and compliance with the policy	6
<b>2. REFERENCES AND DEFINITIONS</b>	<b>6</b>
2.1. Legislative and regulatory references	7
2.2. Other linked internal normative body documents	7
2.3. Definitions	8
<b>3. GENERAL PRINCIPLES</b>	<b>9</b>
<b>4. REPORTS</b>	<b>9</b>
4.1. Subjects of the reports	10
4.2. Limitations and exclusions	10
4.3. the protected subjects	10
4.3.1 Reporting parties	10
4.3.2 Other protected parties	10
4.4. Reports contents and characteristics	11
4.5. Anonymous reports	11
<b>5. PROCESS FOR THE MANAGEMENT OF INTERNAL REPORTS</b>	<b>13</b>
5.1. Platform for the reports management	13
5.1.1 Insertion of the Reports and any additions	13
5.1.2 Attachment of documentation to support the Report	13
5.2. Oral reporting	14
5.3. Persons responsible for managing reports	14
5.4. internal reports management	14
5.4.1 Preliminary evaluation of the reports	14
5.4.2 Reports analysis	14
5.4.3 Results of the analysis and final report	15
5.5. Measures and decisions	16
5.5.1 Disciplinary measures	16
5.5.2 Consequent and further measures	16
<b>6. OTHER REPORT MODALITIES</b>	<b>16</b>
6.1. external reports	17
6.2. public disclosure	17
6.3. report to the judicial or accounting authority	17

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

<b>7.</b>	<b>PROTECTIONS AND MEASURES IN FAVOR OF THE REPORTER</b>	<b>18</b>
	7.1. protection of confidentiality and personal data	<b>18</b>
	7.2. protection from possible retaliation	<b>18</b>
	7.3. limitation of liability for those who report, complaint or make disclosures	<b>19</b>

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

## 1. SCOPE AND FIELD OF APPLICATION

On 30 March 2023, Legislative Decree no. 24 of 10 March 2023 (hereinafter also referred to as "Decree") on the "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, came into force concerning the protection of persons who report violations of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions" (published in the Official Journal no. 63 of 15 March 2023) which updates, at national level, the discipline regarding "whistleblowing".

By strengthening the protection of reporting subjects, the provision aims to encourage the collaboration of workers in order to encourage communication and the emergence of information (including well-founded suspicions) regarding violations committed or which, on the basis of concrete elements, could be committed in the organization with which the Reporter or the person who files a complaint to the judicial or accounting authority has a legal relationship, as well as the elements regarding conduct aimed at concealing such violations.

In this regard, Gervasoni Spa (hereinafter the "**Company**"), after consulting the trade union representatives, has set up a channel for making reports ("**Platform**"), suitable for guaranteeing, in the reception and management of the same, the confidentiality of the identity of the reporter, of the person involved and/or in any case mentioned in the report, as well as the content of the report and the related documentation.

This document (hereinafter, "**Procedure**") has the purpose of describing and regulating the organizational aspects and operational processes relating to the reporting of offenses and violations of national and/or European regulations, as better described below, as well as behaviors implemented in violation of the Organization, Management and Control Model pursuant to Legislative Decree 231/2001 and/or the Code of Conducts, of which the reporting parties become aware as part of their relationships with the Company.

### 1.1. RECIPIENTS AND DIFFUSION

This document applies to all employees (including future ones), self-employed freelancers, contractors, interns, volunteers and non-executive directors ("Reporter(s)") operating in the Company's work context, as well as to all company functions in various capacities involved in the management of the report and in the subsequent phases. The Procedure is made available through: [www.gervasoni.com/governance](http://www.gervasoni.com/governance)

### 1.2. CONTACTS


If further information is needed regarding the content or application of this document, the recipients referred to in paragraph 1.1 may contact the Whistleblowing Team personally or by email to the following address: [amministrazione@gervasoni.com](mailto:amministrazione@gervasoni.com). The team is made up of the following professional figures:

- HR Manager
- CFO
- IT manager

### 1.3. GENERAL RULES FOR APPROVAL, UPDATE, STORAGE, DISTRIBUTION AND COMPLIANCE WITH THE POLICY

The review of this document is carried out annually or based on significant changes in operations, company organization, regulations, or agreements made with stakeholders.

The adoption of a new version of the document will be made known to the recipients referred to in paragraph 1.1 through specific communications. Responsibility for maintaining, updating and distributing this document is attributed to the Whistleblowing Team.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use


## 2. REFERENCES AND DEFINITIONS

### 2.1. LEGISLATIVE AND REGULATORY REFERENCES

1. Legislative Decree dated 10 March 2023, n. 24 (Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of people reporting breaches of Union law and laying down provisions concerning the protection of persons reporting breaches of national regulatory provisions)
2. Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law;
3. Legislative Decree 8 June 2001, n. 231 (Discipline of the administrative responsibility of legal persons and associations even without legal personality, pursuant to art. 11 of law 29 September 2000, n. 300);
4. Law 30 November 2017, n. 179 (Provisions for the protection of the authors of reports of crimes or irregularities of which they became aware in the context of a public or private employment relationship);
5. National Anti-Corruption Authority - **ANAC**, Guidelines on the protection of people who report violations of Union law and the protection of people who report violations of national regulatory provisions. Procedures for reporting and managing external reports, approved with Resolution no. 311 of 12 July 2023;
6. Confindustria, New “Whistleblowing” regulation – Operational guide for private entities, October 2023
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural people with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/ CE (General Data Protection Regulation – GDPR);
8. Legislative Decree 30 June 2003, n. 196 (Personal data protection code) and subsequent Amendments and Additions;
9. Legislative Decree 10 August 2018, n. 101 (Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, relating to the protection of personal data and the free movement of such data and which repeals Directive 95 /46/EC (General Data Protection Regulation));
10. European Data Protection Supervisor, Guidelines on processing personal information within a whistleblowing procedure.

### 2.2. OTHER LINKED INTERNAL NORMATIVE BODY DOCUMENTS


1. Code of Conduct;
2. Company management;

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

### 2.3. DEFINITIONS

<b>Violations</b>	Behaviors, acts or omissions that harm the public interest or the integrity of the Company, concerning the offenses listed in paragraph 4.1 of the Procedure.
<b>Report(s)</b>	All information, including well-founded suspicions, relating to violations already committed or which, on the basis of concrete elements, could be committed, as well as the elements concerning conduct aimed at concealing such violations (symptomatic indicators such as concealment or destruction of evidence), in the scope of the Company.
<b>Internal Report</b>	The written or oral communication of the information referred to in the Report submitted through the internal reporting channel set up by the Company.
<b>External Report</b>	The written or oral communication of information on violations, presented through the reporting channel set up by ANAC and described in paragraph 6.1 of the Procedure.
<b>Public disclosure</b>	Placing information on violations in the public domain through the press or electronic means, or in any case means of dissemination capable of reaching a large number of people.
<b>Reporter</b>	The natural person who reports (internally or externally) or publicly discloses information about violations acquired within his or her work context.
<b>Working context</b>	The work or professional activities, present or past, carried out by the Reporter in the context of the legal relationships existing with the Company, through which, regardless of the nature of such activities, he acquires information on violations, and in the context of which he could risk suffering retaliation in case of reporting or public disclosure.
<b>People in charge</b>	The subjects, specifically appointed by the Company, and responsible for receiving, examining and evaluating the reports received through the internal violation reporting channels.
<b>Facilitator</b>	The natural person who assists the Reporter in the reporting process, operating within the same working context, and whose assistance must therefore be kept confidential.
<b>Person involved</b>	The person or entity named in the Report (internal or external) or public disclosure as the person to whom the violation is attributed or as the person otherwise implicated in the reported or disclosed violation.
<b>Retaliation</b>	Any behavior, act or omission, even if only attempted or threatened, carried out in the work context as a result of the report, the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause the reporting person or the person who has filed a complaint, directly or indirectly, for unfair damage.
<b>Sequel</b>	The action undertaken by the Persons In Charge of assessing the existence of the facts reported, the outcome of the investigations and any measures adopted.
<b>Feedback</b>	The communication to the Reporter of information relating to the follow-up that is given or intended to be given to the Report.




DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

### 3. GENERAL PRINCIPLES

The recipients of the Procedure (Reporters, Persons in Charge, other subjects involved in the management of reports), within the scope of the respective specific competences attributed by the same, are required to:

- encourage and promote the culture of transparency and legality, in order to avoid the risk of acts or phenomena of corruption within the company and in relations with third parties;
- make detailed reports based on precise factual elements: unfounded reports, based on unconfirmed rumors or hearsay, or in any case not falling within the scope identified in this Procedure will not be taken into consideration (see paragraph 4.1);
- make reports in good faith: the internal reporting system cannot be used for the sole purpose of harming the person involved in the report or for opportunistic reasons;
- guarantee, in carrying out reporting management activities, the confidentiality of the identity and personal data of the reporter and the other subjects involved: the recipients of the Procedure are called upon to encourage and protect the positive behavior, physical and moral integrity of the employees or collaborators who report illicit acts or illegitimate behavior of which they become aware;
- take the reports received seriously into consideration and evaluate them scrupulously;
- even if the report is unfounded, do not carry out acts of retaliation or discrimination, direct or indirect, which have effects on the working conditions of the whistleblower and of the subjects involved in the report;
- guarantee the traceability of the process relating to the evaluation of the report and the adoption of any consequent measures.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

## 4. REPORTS

### 4.1. SUBJECTS OF THE REPORTS

Pursuant to Legislative Decree no. 24/2023 and taking into account the context in which the Company operates and its organizational and structural characteristics, the following may be subject to reporting:

- a) significant illicit conduct pursuant to Legislative Decree no. 8 June 2001, n. 231;
- b) violations of the Organization, Management and Control Model pursuant to Legislative Decree 8 June 2001, n. 231, of the Code of Ethics and/or the procedures of the Company's internal regulatory system;
- c) offenses that fall within the scope of application of European Union or national acts, or national acts that constitute the implementation of European Union acts relating to the following sectors: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental Protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems;
- d) acts or omissions that harm the financial interests of the European Union (e.g. fraud, corruption, other illegal activities related to Union expenditure);
- e) acts or omissions relating to the internal market, including infringements of European Union competition and state aid rules, as well as infringements relating to the internal market linked to acts infringing corporate tax rules or mechanisms the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable corporate tax legislation;
- f) acts or behaviors that frustrate the object or purpose of the provisions of the European Union in the sectors indicated in the previous points (e.g. practices such as abuse of a dominant position);
- g) administrative, accounting and criminal offenses that do not fall under points c) to f).

### 4.2. LIMITATIONS AND EXCLUSIONS

Taking into account the provisions of current legislation, the following cannot be reported:

- a) disputes, claims or requests linked to a personal interest of the Reporting Party, i.e. relating exclusively to the relevant individual employment relationships in general, or to the relationship with hierarchically superior figures (e.g. employment disputes and pre-litigation phases, discrimination between colleagues, interpersonal conflicts between the Reporter and another worker or with hierarchical superiors, in the absence of harm to the public interest or the integrity of the Company);
- b) reports of violations that are already specifically regulated by European or national legislation, and which therefore already provide and regulate specific reporting procedures (e.g. financial services; terrorism; prevention of money laundering; environmental protection);
- c) reports of violations relating to national security, defense procurement or national security, unless such aspects are regulated by secondary law of the European Union;
- d) reports based on information that the Reporter knows to be false: they are not worthy of protection under current legislation;
- e) reports regarding information already in the public domain.


In any case, the application of regulations (national and/or European) regarding: (i) classified information remains unchanged; (ii) medical and forensic secrecy; (iii) secrecy of the deliberations of the judicial bodies; (iv) criminal procedure regarding the secrecy of investigations; (v) autonomy and independence of the judiciary; (vi) national defense and public order and security; (vii) exercise of the right of workers to consult their representatives or trade unions, protection against illicit conduct or acts carried out as a result of such consultations, autonomy of the social partners and their right to stipulate collective agreements, as well as repression of anti-union conduct.

### 4.3. THE PROTECTED SUBJECTS

#### 4.3.1 Reporting parties

Reports of violations can be made by:

- a) workers with subordinate employment contracts, including all types of employment contracts regulated by Legislative Decree 15 June 2015, n. 81 (short-time and flexible work; fixed-term work; job agency);

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

- apprenticeship; accessory work), or by art. 54-bis of the Legislative Decree of 24 April 2017, n. 50, converted with amendments by Law 21 June 2017, n. 96 (occasional performance contract);
- b) self-employed workers, including those indicated in Chapter I of Law 22 May 2017, n. 81 (e.g. professional firms; professionals registered with orders and colleges), and holders of collaborative relationships (relationships of commercial representation agencies and other types of continuous and coordinated collaboration) who carry out their work at the Company;
  - c) suppliers of goods and services or subjects who carry out works in favor of the Company;
  - d) freelancers and consultants who work for the Company;
  - e) volunteers and interns, paid and unpaid, who work for the Company;
  - f) the shareholders and persons with administrative, management, control, supervisory or representation functions (even exercised merely de facto) of the Company.

Such subjects, if they make a Report, benefit from the protections provided by current legislation, as summarized in chapter 7 of this Procedure:

These protections also apply in the following cases:

- a) when the legal relationship with the Company has not yet begun, if the information on the violations was acquired by the Reporter during the selection process or in other pre-contractual phases;
- b) during the probationary period;
- c) after the dissolution of the legal relationship, if the information on the violations was acquired during the relationship itself.

#### **4.3.2 Other protected parties**

Together with the Whistleblowers, the protection measures reported in chapter 7 of this Procedure also apply:

- a) to the Facilitators, as defined in paragraph 2.1 of the Procedure;
- b) to people who work in the same working context as the Reporter and who are linked to the latter by a stable emotional or kinship bond within the fourth degree;
- c) to the Reporter's work colleagues who have a regular and current relationship with the latter;
- d) to entities owned by the Reporter or for which he works, or entities that operate in the same working context as the Reporter.

#### **4.4. REPORTS CONTENTS AND CHARACTERISTICS**

The Report must be made whenever there is a reason to believe that the information relating to the violation is true. It must be carried out with a spirit of responsibility, in the interest of the common good, taking into account the principles identified in chapter 3 of the Procedure.

Therefore, the Report must contain concrete, truthful and useful elements to allow the Persons in Charge to carry out appropriate investigations and checks regarding the validity of the facts and circumstances being reported. It is therefore useful that at least the following elements are clearly reported within it:

- a) the description of the fact;
- b) the circumstances of time and place in which the violation which is the subject of the Report occurred;
- c) the personal details or other elements that allow the identification of the author or, if more than one, the authors of the violation;
- d) any documents useful to prove and give evidence of what has been described (e.g. texts; images; audio; video).


By way of example and not exhaustively, the Reports may relate to:

- a) subjects linked to the Company by an employment or collaboration relationship;
- b) members of the corporate bodies (Board of Directors, Board of Auditors, Auditing Firm);
- c) third parties linked to the Company by a contractual relationship (commercial partners, vendors, agents, customers, suppliers, sub-contractors, etc...).

The reporting party may at any time integrate, rectify or complete the report made or add further evidentiary elements, including documentary evidence, with the same methods in which he made the Report.


#### **4.5. ANONYMOUS REPORTS**

If the Reporter does not identify himself or does not provide sufficient information to be identified, the Report will be considered an anonymous Report.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	<p style="text-align: center;">WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS</p>	<p style="text-align: center;">DATE: 14 Dec 2023 Type: Internal use</p>

However, if it is punctual, detailed and supported by suitable documentation, it can be equated to an ordinary report and, as such, can be treated.

In any case, anonymous reports will be recorded by the people in charge and the documentation received will be kept, also in order to ensure the protections provided for by current legislation if the Reporter is subsequently identified and has suffered retaliation.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

## 5. PROCESS FOR THE MANAGEMENT OF INTERNAL REPORTS

### 5.1. PLATFORM FOR THE REPORTS MANAGEMENT

In accordance with the provisions of the applicable legislation, the Company, having consulted the company trade union representatives, has established specific internal reporting channels which the Reporter can use. More precisely, the Report can be made, anonymously or non-anonymously (see paragraph 4.5 of the Procedure), through the Whistleblowing Platform ("Platform"), which can be reached at the website [ordini.gervasoni.com](http://ordini.gervasoni.com). Together with the Platform, the Company makes clear information available to all potential reporters with references to the Platform itself and the procedures for its use, including the prerequisites for making the Reports. The Platform is equipped with security measures such as to guarantee, where necessary also through encryption tools, the confidentiality of the identity of the Reporter, of the people involved or otherwise mentioned in the Report, as well as of the content of the same and the related documentation.

Access to the Platform is subject to the "no-log" policy, in order to prevent the identification of the Reporter, especially if he intends to remain anonymous. This means that the company IT systems will not be able to identify the access point to the platform (IP address) even if such access is made from a computer connected to the company network.

To further protect the confidentiality of the Reporter, access to the Platform is free: it is therefore not necessary to possess credentials to proceed with the Report.

These settings therefore allow you to send and store the data and documents relating to the Reports in a secure manner, respecting the confidentiality of all the subjects involved in them, and to send them only to pre-determined recipients, duly trained, and formally responsible for managing the Reports. (see paragraph 5.3 of the Procedure). Except for what concerns the Reports subject to archiving (see paragraph 5.4.1 of the Procedure), the data and documentation relating to the Reports are kept for the time necessary to manage them, and in any case no later than five years from the date communication of the final report of the trial (see paragraph 5.4.3 of the Procedure). After this deadline, the Reports and the related documentation are deleted and/or destroyed from all media and archives.


#### 5.1.1 Insertion of the Reports and any additions

The insertion of the Report via the Platform is carried out by completing a questionnaire which requires detailing some elements such as:

- a) the context in which the violation occurred;
- b) the Reporter's relationship with the Company;
- c) whether the latter has already made other reports and with what methods, and whether he has suffered or is afraid of suffering retaliation for the Report;
- d) the identification elements of the Reporter, who can however choose to remain anonymous (see paragraph 4.5);
- e) elements relating to the violation, such as: type of offense committed; description of the facts of which the Reporter has become aware; date on which the violation occurred and whether it is still ongoing; evidence to support the Report (which can also be attached);
- f) indication of any subjects with whom the Reporter has shared the information relating to the violation.

In any case, the information on the processing of personal data pursuant to art. 13 of Regulation (EU) 2016/679 (GDPR) and information relating to the confidentiality of the data contained in the Report and of your identity. At the end of the process, the Platform issues the Report's identification code to the Reporter: this is a unique 16-digit code that the Reporter must keep to subsequently access the Platform, check the status of the Report, receive feedback in this regard or make specific additions. In particular, you will be able to:

- a) if you have opted to make a Report anonymous, enter, at a later time, your identification and contact details;
- b) attach further documentation as evidence of what has been reported;
- c) insert further comments, also in response to requests for further information from the Persons in Charge.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

### 5.1.2 Attachment of documentation to support the Report

As highlighted in the previous paragraph, the Reporter can integrate - even in subsequent phases - the Report with documentation (textual files; images; photographs; videos; etc.) aimed at supporting and proving what has been declared.

The Reporter is obliged to ensure that such attachments are not malicious and/or potentially dangerous or harmful, or such as to compromise the correct functioning and security levels of the Platform.

If the Reporter does not intend to identify himself, he must also ensure that he has correctly deleted the metadata of the files uploaded to the Platform (that is, the data that can be verified by viewing the file properties, such as "Author of the document" and "Last modification").

## 5.2. ORAL REPORTING

If the Reporter requests it, a direct meeting with the Responsible people for managing the Reports may be set up within a reasonable timeframe and in any case not exceeding 3 days from the request itself. In this case, the Report, with the prior consent of the Reporter, will be documented by recording on a device suitable for storage and listening. If the Reporter does not give his consent to this method, a minute of the meeting will be drawn up, which the Reporter will be able to verify, rectify and confirm by signing.

Similarly, to what concerns the Platform, the data and documentation collected during direct meetings are kept for the time necessary to manage the Report, and in any case no later than five years from the date of communication of the final report of the process (see paragraph 5.4.3 of the Procedure). After this deadline, the Reports and the related documentation are deleted and/or destroyed from all media and archives.

## 5.3. PERSONS RESPONSIBLE FOR MANAGING REPORTS

Reports are received by the Whistleblowing Team. This body has been formally responsible for viewing the Reports received and the related management, according to the procedure illustrated below.

If situations of conflict of interest occur (e.g. if the Reporter coincides with the Person in Charge, or with the person reported, or is in any case a person involved or interested in the Report), the Report must be addressed to the supervisory body, so that effective, independent and autonomous management is guaranteed, in compliance with the confidentiality obligation established by current legislation.

Where the Reports have profiles of relevance, depending on the case, the Whistleblowing Team involves without delay, and in any case within one day of receiving the Report, one of the subjects listed below to the extent of their competence:

- a) Supervisory Body, for Reports relating to significant offenses pursuant to Legislative Decree 231/2001, as well as violations of the principles of the Code of Ethics and/or the procedures of the Company's internal regulatory system, as well as for all Reports relating to violations unrelated to what is specified in the following points;
- b) Chief Information Security Officer/Head of IT Security, for reports relating to violations relating to the security of networks and information systems;

Should the existence of situations of conflict of interest occur in the management of the Report by one of the subjects referred to in letter b), this will be replaced by the Supervisory Body.


Where there are situations of conflict of interest in the management of the Report by the Supervisory Body, the auditing firm will be involved.

Should the Report be submitted to a person other than the Whistleblowing Team, it must be transmitted, within 7 (seven days) of its receipt, to the Person in Charge, giving simultaneous notice of said transmission to the Reporter.

## 5.4. INTERNAL REPORTS MANAGEMENT

### 5.4.1 Preliminary evaluation of the reports

Upon receipt, the Person in Charge is required to issue to the Reporter a notice of receipt of the Report, within 7 (seven) days from the date of receipt.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

At the same time, the Person in Charge carries out a preliminary examination of the Report, verifying:

- a) compliance with the criteria and requirements defined by the Procedure, for example in relation to the nature of the reported violation and the legitimacy of the Reporter to proceed with the Report;
- b) the completeness of the Report, and the presence of sufficient elements to evaluate its merit;
- c) the existence of the legal and/or factual conditions for starting the analysis phase of the Report;
- d) the seriousness of the facts reported and the urgency in managing the Report.

If it verifies that the Report is inadmissible because it is unrelated to the object of the Procedure or lacks the requirements indicated therein, the Person in Charge will archive it. The Reporter is notified of the archiving, via the Platform or other defined communication channel. The data and documentation referred to in the archived Report are deleted without delay, and in any case three (three) months from the date of reading of the Report by the Person in Charge.

In the event that, however, the Report is not sufficiently detailed or incomplete, the Person in Charge contacts the Reporter via the Platform, or, especially if the Report is not received anonymously, summons him in person in order to obtain integration of the Report made or the addition of further evidentiary elements, including documentary ones.

Finally, if the Person in Charge detects a possible violation or illicit behavior relevant to the Procedure, he proceeds with the next phase of analysis of the Report. The Reporter is informed, within the deadline indicated above, via the Platform or other defined communication channel.

#### **5.4.2 Reports analysis**


If the Report is relevant, the Person in Charge proceeds to involve the figures indicated in paragraph 5.3 of the Procedure, to the extent of their respective competence, in order to analyze and evaluate the Report.

In this phase, the Person in Charge - taking care not to reveal the identity of the Reporter, that of the subjects involved in the report and the subject of the report - may, by way of example and not exhaustively:

- a) interface with the other functions of the Company to request their collaboration, through the provision of data, documents or information useful for the analysis itself;
- b) agree with the company structure responsible for the function affected by the report, any "action plan" necessary for the removal of the control weaknesses detected;
- c) agree with the Legal Department (and/or with other interested Departments and Functions) on any initiatives to be undertaken to protect the interests of the Company (e.g. legal actions, suspension/cancellation of suppliers from the supplier register; etc.);
- d) interface with subjects external to the Company (e.g. technical support figures, external consultants who are experts in the field, etc.);
- e) request further elements or insights from the Reporter, leaving evidence of the relevant conversation;
- f) carry out any activity deemed useful or necessary to verify the Report, including hearing the Reporter and/or any other parties who may report on the facts reported;
- g) conclude the investigation at any time if, during the course of the investigation, the unfoundedness of the Report is established;
- h) at the conclusion of the analysis activities, submit the results for evaluation by the Management so that the most appropriate measures are taken, involving the competent company structures where necessary (see paragraph 5.3).

In any case, the aforementioned actions will be carried out in compliance with the principles of confidentiality and impartiality of judgment, the legislation on the protection of personal data and the applicable CCNL.

If, as part of the checks on the Report, the bad faith of the Reporter and/or the merely defamatory intent are ascertained (possibly also confirmed by the unfoundedness of the Report itself), the Person in Charge proceeds to report the incident to the HR Department to evaluate the initiation of disciplinary proceedings against the Whistleblower.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

### 5.4.3 Results of the analysis and final report

At the end of the analysis phase, the Person in Charge provides feedback to the Reporter regarding the Report within 3 (three) months from the date of the acknowledgment of receipt or, in the absence of such notice, within three months from the expiry of the seven-day deadline from the submission of the Report. This feedback will be provided via the Platform, which the Reporter can access by entering the identification code of the Report. Furthermore, the Person in Charge prepares a final report on the report ("Report"), which shows:

- a) the data and information contained in the Report (name of the Reporter - where there is consent from the latter - and of the person(s) reported, place and date of occurrence of the facts, evidence or documentary elements);
- b) the checks carried out; the outcomes of the same and subjects within the company or third parties involved in the analysis phase;
- c) a summary evaluation of the analysis process with an indication of the cases ascertained and the related reasons;
- d) the outcome and conclusion of the analysis (archival or validity of the report).

The Report is sent to company management.

## 5.5. MEASURES AND DECISIONS

### 5.5.1 Disciplinary measures

Having received the Report, the Company Management decides whether to initiate any disciplinary proceedings against the person reported against whom, during the analyzes carried out, elements of responsibility in the violation covered by the Report have emerged, and against any other co-responsible persons identified. The company management also evaluates, with the assistance of the HR Department, whether to initiate disciplinary proceedings against:

- a) of the Reporter who has made an unfounded and bad faith Report, when criminal liability for the crimes of defamation or slander or in any case for the same crimes committed with the report to the judicial authority or accountant, or his civil liability, for the same reason, in cases of fraud or gross negligence;
- b) any perpetrators of retaliatory/discriminatory behavior towards the Reporter or those who have a qualified connection with the Reporter (see paragraph 4.3.2 of the Procedure);
- c) of the subjects involved in the process of evaluating and analyzing the report who have violated the confidentiality obligations or have not examined the Report received or, again, have not adopted the procedures for managing the reports in accordance with the provisions of current legislation ;
- d) of anyone who has hindered, or attempted to hinder, the Report;
- e) of those who have not established reporting channels.

Disciplinary measures will be adopted in accordance with the provisions of the CCNL applied by the Company and imposed on the basis of the Workers' Statute and in compliance with the company disciplinary system.


It should be noted that, in case of abuse of the reporting tool, the Company may apply disciplinary sanctions.

### 5.5.2 Consequent and further measures

The Person in Charge may inform the judicial authorities and/or the competent supervisory authorities of the facts covered by the Report.

The Person in Charge may also suggest to the Company Management the implementation, in concert with other competent Company Areas/Functions, of any prevention measures that may be necessary to promote the culture of legality and transparency within the Company, and promote the adoption of any changes and additions to this Procedure and control systems in light of constant monitoring of its application of the results obtained.



DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

## 6. OTHER REPORT MODALITIES

### 6.1. EXTERNAL REPORTS

With the exclusion of violations relating to letters a) and b) of paragraph 4.1 of the Procedure (which can only be reported via internal reporting), the Reporter has the possibility of making the Report also through the external reporting channel activated and managed by the National Anti-Corruption Authority (ANAC ).

The external report can only be made if, at the time of its submission, one of the following conditions exists:

- a) the internal reporting channel is not active, or, even if active, does not comply with the provisions of current legislation;
- b) the Reporter has already made an internal report, but it has not been followed up;
- c) the Whistleblower has reasonable grounds to believe that, if he/she made an internal report, it would not be followed up effectively or that the report could lead to the risk of retaliation;
- d) the Reporter has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

For the operational methods of managing reports through the channel set up by the ANAC, please refer to the procedures issued by this Authority and available on the website: <https://www.anticorruzione.it/-/whistleblowing>. In any case, the protections described in chapter 7 of the Procedure apply to the Reporter.

### 6.2. PUBLIC DISCLOSURE


With the exception of violations relating to letters a) and b) of paragraph 4.1 of the Procedure (which can only be reported via internal reporting), the Reporter has the possibility of making a public disclosure, through the press or electronic means or in any case through means of dissemination, with respect to the information on violations acquired within your work context if one of the following conditions exists:

- a) the Reporter has already made an internal and external Report, or directly an external report, and has not received feedback regarding the measures adopted to follow up on the Report;
- b) the Reporter has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest;
- c) the Reporter has reasonable grounds to believe that the external report may involve the risk of retaliation or may not have an effective follow-up due to the specific circumstances of the specific case, such as those in which evidence may be hidden or destroyed, or in which there is well-founded fear that the person receiving the report may be colluding with the perpetrator of the violation or involved in the violation itself.

In any case, the protections described in chapter 7 of the Procedure apply to the person making the public disclosure.

### 6.3. REPORT TO THE JUDICIAL OR ACCOUNTING AUTHORITY

The protections referred to in Legislative Decree 24/2023 also extend to individuals who report information on violations acquired within their work context through reports to the judicial or accounting authorities.

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

## 7. PROTECTIONS AND MEASURES IN FAVOR OF THE REPORTER

The Company undertakes to ensure the application of the protections provided for by current legislation to the Reporter. As already mentioned, they also extend to subjects other than the Reporter due to the role assumed within the reporting process and/or the particular relationship that binds them to the Reporter himself.

The protection system provides for the protection of the confidentiality and personal data of the Reporter and of the subjects involved in various capacities by the Report, as well as protection from possible retaliation.

### 7.1. PROTECTION OF CONFIDENTIALITY AND PERSONAL DATA

The Company guarantees the confidentiality of the Reported Party, the Facilitator, the person involved and the people mentioned in the report, as well as the content of the report itself and the related documentation. This is also in order to avoid the exposure of such subjects to retaliatory measures that could be adopted following the Report.

The identity of the Reporter and any other information from which the same can be deduced, directly or indirectly, cannot be revealed without the express consent of the latter to persons other than those competent to receive or follow up on the reports, expressly authorized to process such data pursuant to the legislation on the protection of personal data. An exception is made if such information is requested by a judicial or administrative authority.

In the context of any disciplinary proceedings promoted within the Company's organization, the identity of the Reporter cannot be revealed, where the contestation of the disciplinary charge is based on investigations which are distinct and additional to the Report, even if consequent to the itself. If the dispute is based, in whole or in part, on the Report and knowledge of the identity of the Reporter is indispensable for the defense of the accused, the Report will be usable for the purposes of disciplinary proceedings only in the presence of the express consent of the Reporter to the disclosure of their identity.

The processing of personal data collected as part of the reporting process is carried out in accordance with current legislation, and in particular Regulation (EU) 2016/679 (GDPR), and the relevant internal policies and procedures. Therefore, the Company undertakes to use the Reports only within the limits of what is necessary to follow up on them, and to delete without unjustified delay the personal data that are clearly not useful for the management of a specific Report.

The subjects in charge of managing the reports are formally appointed as subjects authorized to process them, pursuant to art. 2-undecies of Legislative Decree 30 June 2003, n. 196, duly trained and instructed, and bound to confidentiality.

The information on the processing of personal data, drawn up pursuant to art. 13 of Regulation (EU) 2016/679 (GDPR) is available on the website [www.gervasoni.com](http://www.gervasoni.com).


Finally, it is specified that the Company proceeds to regulate the relationship with any external suppliers involved in the management of Reports through specific agreements concluded pursuant to art. 28 of Regulation (EU) 2016/679 (GDPR).

### 7.2. PROTECTION FROM POSSIBLE RETALIATION

The Company undertakes to implement all reasonable measures to avoid the risk of retaliation against Whistleblowers and other protected parties (see paragraph 4.3.2 of the Procedure).

Listed below are some cases which may, among others, constitute retaliation:

- a) dismissal, suspension or equivalent measures;
- b) demotion in rank or failure to promote;
- c) change of functions, change of place of work, reduction of salary, modification of working hours;
- d) suspension of training or restrictions on access to it;
- e) notes of merit or negative references;
- f) adoption of disciplinary measures or other sanctions, including pecuniary ones;
- g) coercion, intimidation, harassment, ostracism, or discrimination and other unfavorable treatment;
- h) failure to convert the fixed-term employment contract into a permanent employment contract, where the worker had a legitimate expectation of such conversion;
- i) failure to renew or terminate a fixed-term employment contract, or early termination or cancellation of a contract for the supply of goods or services;
- j) damage, including to the person's reputation, in particular on social media, or measures resulting in economic prejudice, loss of economic opportunities or loss of income;

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS	DATE: 14 Dec 2023 Type: Internal use

- k) inclusion in improper lists, which may make it impossible for the person to find employment in the sector in the future;
- l) cancellation of a license or permit;
- m) request to undergo psychiatric or medical tests.

The Reporter and the protected subjects can communicate the retaliation they believe they have suffered to the ANAC, which will inform the National Labor Inspectorate for the measures within its competence. The communication can also be made, on behalf of the Reporter, by the trade union organization indicated by the latter. Acts undertaken by the organization in violation of the prohibition on retaliation are null and void: for example, individuals who have been fired as a result of the Report have the right to be reinstated in their jobs. Furthermore, waivers and transactions, in whole or in part, which have as their object the rights and protections provided in favor of the Reporter and the protected subjects are not valid, unless they are carried out through a conciliation report drawn up in judicial or extrajudicial proceedings (e.g. : conciliation at the Provincial Labor Directorate; arbitration resolution of the dispute at the Provincial Labor Directorate; other methods of conciliation and arbitration as provided for in art. 412-quater of the civil procedure code).

The application of the protection regime against retaliation provided for by current legislation is in any case subject to the following conditions:

- a) the person must have made the report (or public disclosure, or complaint) based on the reasonable belief that the information on the reported violations was truthful and falling within the objective scope of application of Legislative Decree no. 24/2023. The report cannot therefore be based on mere suspicions or "rumors";
- b) the report (or public disclosure, or complaint) was carried out in compliance with the regulations established by current legislation;
- c) there must necessarily be a consequential relationship between the report (or public disclosure, or complaint) made and the retaliatory measures suffered by the Reporter.

If these conditions do not apply, the Report (or public disclosure, or complaint) will not fall within the scope of the provisions of Legislative Decree no. 24/2023, and the protections described here will therefore not be applicable to the Reporter. Similarly, the protection granted to protected subjects who, due to the role assumed within the reporting/complaint process and/or the particular relationship that binds them to the Whistleblower, indirectly suffer retaliation will be excluded.

Furthermore, the protection provided in the event of retaliation is not guaranteed when the criminal liability of the reporting person for defamation or slander crimes or in any case for the same crimes committed with the complaint to the judicial authority is ascertained, even with a first-degree sentence or accounting or his civil liability, for the same reason, in cases of fraud or gross negligence.


### **7.3. LIMITATION OF LIABILITY FOR THOSE WHO REPORT, COMPLAINT OR MAKE DISCLOSURES**

In addition to the protections illustrated in the previous paragraphs, if certain conditions are met, the Whistleblower is granted limitations of liability with respect to the disclosure and dissemination of categories of information which could otherwise lead to the occurrence of certain types of crime, including.

- a) disclosure and use of official secrecy;
- b) disclosure of professional secrecy;
- c) revelation of scientific and industrial secrets;
- d) violation of the duty of fidelity and loyalty;
- e) violation of the provisions relating to the protection of copyright;
- f) violation of the provisions relating to the protection of personal data;
- g) revelation or dissemination of information on violations that offend the reputation of the person involved.

The aforementioned limitations of liability apply only under the following conditions:

- a) existence, at the time of disclosure or dissemination, of well-founded reasons to believe that the information was necessary to reveal the violation. The Reporter therefore had to reasonably believe, and

DATA CONTROLLER	DOCUMENT	CLASSIFICATION
	<p style="text-align: center;">WHISTLEBLOWING – PROCEDURE FOR THE MANAGEMENT OF INTERNAL REPORTS</p>	<p style="text-align: center;">DATE: 14 Dec 2023 Type: Internal use</p>

not on the basis of simple inferences or for purposes unrelated to the purpose of the legislation (e.g. vengeful, opportunistic, scandalous purposes), that that information should be revealed as strictly necessary to report the violation;

- b) compliance with all the conditions established by current legislation when making the Report, in order to benefit from the protections ensured by Legislative Decree no. 24/2023.

In the absence of these conditions, the liability of the Reporter - from a criminal, civil or administrative point of view - cannot benefit from any limitation.

We also highlight the possibility that the Reporter benefits from an exclusion of liability also in cases of:

- a) “lawful” access to the reported information or documents containing such information;
- b) behaviour, acts or omissions carried out by those who report, report or disclose publicly, provided they are connected to the report, report or public disclosure and necessary to reveal the violation.