





Whistleblowing and management of reports

SGI.ART.IOP.050101

-  **CONFIDENTIAL – CONFIDENZIALE**
-  **SENSITIVE – RISERVATA**
-  **PRIVATE – PRIVATA**
-  **PUBLIC – PUBBLICA**

INDEX OF REVIEWS			
Rev.	Date	Author	Description
0	10/12/2023	M.Brizi	First issue

Editor/Creator	Verification - Approval	Emission
M. Brizi SGSI	M. Lupo – E. Bernardini DPO - CCTO	M. Brizi EMS

COPYRIGHT ART SPA. ALL RIGHTS RESERVED

The information contained in this document, is the confidential, proprietary information of ART SPA, and may not be reproduced, disclosed to any third party or used, for other than the intended purpose for which it was provided to the original recipient, without the prior written approval of ART SPA.

INDEX

1	Purpose and Scope	4
2	References	4
3	Terms and Definitions	5
4	Activity	7
4.1	Macro Work-Flow	7
4.2	What situations can be reported	7
4.3	Exclusions	9
4.4	Who can make a report	10
4.5	When can a report be made?	10
4.6	Anonymous Reporting	10
4.7	Reporting Modes.....	11
4.7.1	Internal channel	11
4.7.2	External channel	12
4.7.3	Public Disclosure	12
5	Management of the Reporting Procedure	13
5.1	Who receives reports.....	13
5.2	Receipt and Acceptance of the Report	14
5.2.1	Preliminary Evaluation of the Report	14
5.2.2	Request for Further Information	15
5.2.3	Investigation of the violation reported.....	15
5.3	Assessment and prevention of the risk of retaliation.....	15
5.4	Outcome of investigations carried out by Manager	16
5.5	Actions which follow the clear finding of a violation or retaliation.....	17
6	Forms of Protection for the Reporting Individual	17
6.1	Measures to Protect the Reporter	17
6.1.1	Prohibition of waivers and settlements.....	17
6.1.2	Duty of Confidentiality to the Reporter.....	17
6.2	Processing of Personal Data.....	18
6.3	Prohibition of Retaliatory Acts against the Reporting Individual.....	19
6.4	Other protected parties	20
6.5	Limits of Criminal, Civil, Administrative Responsibility	20
6.6	Whistleblowing Framework and Organization Model 231	20
6.7	Exclusion of Protection for the Reporting Person.....	21
6.8	Support Measures.....	21

6.9 Training Obligations 21

6.10 Sanctions 22

1 Purpose and Scope

The purpose of this Procedure is to illustrate the methods for making and handling reports of suspected misconduct, suspected wrongdoing or alleged violations (grouped together under the term whistleblowing) and for the protection of persons who report violations of national regulations. The objective is to provide whistleblowers with clear operational indications on the subject, content, recipients and methods of transmitting reports, as well as on the forms of protection offered by our legal system, removing factors that may discourage or hinder the use of reports (such as, for example, doubts and uncertainties as to how to proceed and fears of retaliation or discrimination).

This document is applicable within SGI/EMS ART.

2 References

- ISO 9001 - Quality Management Systems
- IATF 16949 – Automotive Quality Management Systems
- ISO 14001 – Environmental Management System
- ISO 27001 – Information Security Management System
- EMS ART
- ART Code of Ethics
- Organizational Model 231
- SGQ.ART.PRO.050100 - Communication and Information Management.
- Directive (EU) of the European Parliament and of the Council of October 23, 2019, No. 1937 on the protection of persons who report breaches of Union law;
- Legislative Decree No. 24 of March 10, 2023, on “Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws.”
- Regulation (EU) No. 679 of the Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Legislative Decree No. 196 of June 30, 2003, Code on the Protection of Personal Data;
- ANAC Guidelines 311 /2023.
- ISO 37002– Whistleblowing management systems – Guidelines.

3 Terms and Definitions

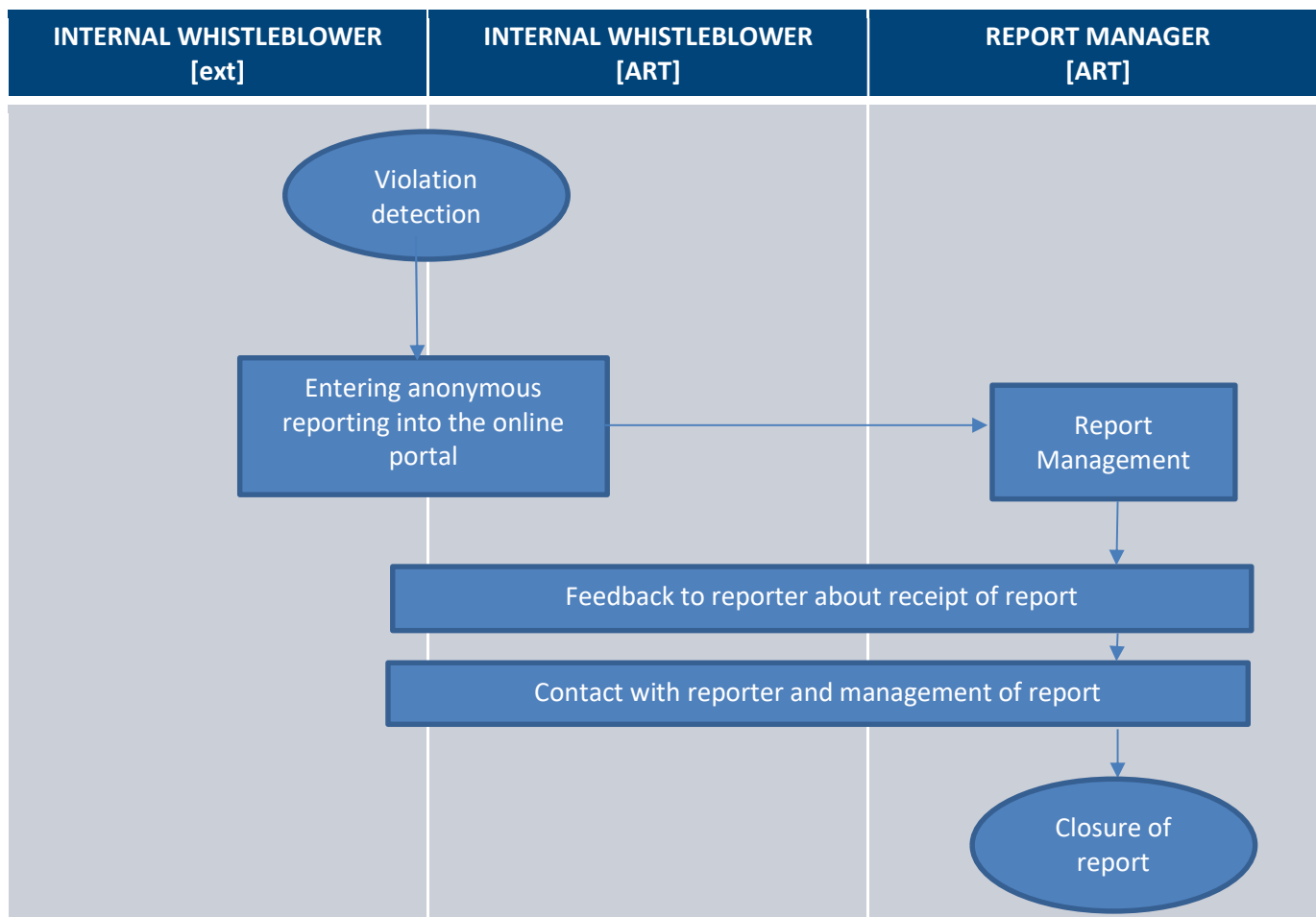
TERM - ACRONYM	DEFINITION
Infringements	behavior, acts or omissions that harm the public interest or the integrity of the Organization
Information on infringements	information, including well-founded suspicions, concerning violations that have been committed or that, on the basis of hard evidence, could be committed within the scope of the Organization as well as elements concerning conduct aimed at concealing such violations.
Reporting	<p>circumstantiated communication based on precise and concordant elements of fact concerning:</p> <ul style="list-style-type: none"> - the commission, attempted commission or reasonable danger of commission of one of the crimes (and/or administrative offenses) relevant under Legislative Decree 231/2001; - violations, even if only suspected, inherent in: Code of Ethics, Model 231, Policy for the Prevention of Corruption, Guidelines of the Management System for the Prevention and Combating of Corruption and/or company procedures; - any irregular conduct or occurrence, which is symptomatic of “maladministration” and/or may entail risks for ART SPA, of which the reporting persons have become aware by reason of duties carried out.
Internal reporting	the written or oral communication of information about violations, submitted through the internal reporting channel specifically set up by the Organization;
Report Manager	person in charge of receiving and handling reports made through the Company's internal reporting channel
SB	Supervisory Body that is that section of the Company, endowed with autonomous powers of initiative and control in accordance with Legislative Decree 231/2001 and established in accordance with the provisions of the Confindustria Guidelines for the preparation of organization, management and control models.
WB MANAGEMENT SOFTWARE	external, independent, anonymity-preserving sw support that ART makes available to the whistleblower to make reports
External notification	the written or oral communication of information about violations submitted through the external reporting channel set up by the Organization.
“Public disclosure” or “publicly disclose”	make information about infringements publicly available through print or electronic media or otherwise through any means of distribution that can reach a large number of people.
Whistleblower	“reporting person” - the individual who makes a report or public disclosure of information on violations acquired in the course of his or her work context.

Reported individual	“person reported” - the individual who is the subject of an alert
Whistleblowing (WB)	is a report made by a person who, in the performance of his or her duties or dealings with the organization, becomes aware of an offence, a risk or a dangerous situation that may cause harm to the organization, as well as to customers, colleagues, citizens, and any other category of subjects
Anonymous reporting	report that does not allow the identity of the reporter to be established
Facilitator	an individual who assists a whistleblower in the reporting process, operating within the same work environment and whose assistance must be kept confidential
Working environment	current or past employment or professional activities through which, regardless of the nature of such activities, a person acquires information about violations and in the context of which he or she could risk retaliation in the event of a public disclosure or report to the Judicial or Accounting authorities
Person reported or person involved	the individual or legal entity mentioned in the internal or external report or in the public disclosure as the person to whom the breach is attributed or as a person otherwise implicated in the reported or publicly disclosed breach
Retaliation	any conduct, act or omission, even if only attempted or threatened, committed on account of the report, the complaint to the judicial or accounting authorities or public disclosure, which causes or is likely to cause the reporting person or the person making the complaint unjust damage, directly or indirectly
Follow-up	the set of actions taken within the management of the reporting channel to assess the existence of the reported facts, the outcome of the analysis and any measures that need to be taken
Feedback	communication to the reporting person of information about the follow up that is being carried out or is intended to be carried out with respect to the report.
Organization	ART Spa
EMS	Enterprise Management System

For other terminology, please refer to the standard: “ISO 9000 - Quality Management Systems - fundamentals and vocabulary”.

4 Activity

4.1 Macro Work-Flow



4.2 What situations can be reported

The following are eligible for reporting - suspected misconduct or suspected wrongdoing or alleged violations, consisting of:

- actions or omissions implemented in violation of the Code of Ethics (the updated version is always available on the employee portal);
- administrative, accounting, civil or criminal offenses;
- offenses related to the following areas: public procurement, services, financial products and markets, and prevention of money laundering and financing of terrorism;
- product safety and compliance;
- environmental protection;
- public health;
- consumer protection;
- privacy and data protection as well as network and information system security;

- acts or omissions that harm the financial interests of the European Union. Examples include fraud, corruption, and any other illegal activities related to EU spending;
- acts or omissions concerning the internal market. This includes violations of EU competition and state aid rules, corporate tax, and mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
- acts or conduct that thwart the object or purpose of the provisions set forth in the acts of the Union.

By way of further example and not limitation, misconduct concerning any of the following falls within the scope of this procedure:

- hypotheses of the specific crime of bribery;
- additional hypotheses of crimes against public administration;
- situations in which, in the course of administrative activity, there is evidence of abuse by a person of the power entrusted to him/her in order to obtain private advantages;
- criminally relevant actions or omissions;
- actions or omissions implemented in violation of the Code of Ethics;
- actions or omissions likely to cause damage to the Company's assets or image;
- actions or omissions likely to cause damage to the health or safety of employees, or damage to the environment;
- actions or omissions to the detriment of employees or others who perform their activities at the Organization.

The report may also be concerned with any of the following:

- information regarding conduct aimed at concealing the above mentioned violations;
- unlawful activities that have not yet been carried out, but which the whistleblower reasonably believes may occur in the presence of definite and concise factual elements.

In order to ensure that the subsequent investigative phase is effective and in view of the Organization's objectives, the report should be as detailed and contextualized as possible through the identification of specific and objective factual elements such as:

- ✓ the time period in which the misconduct occurred;
- ✓ possible other persons with knowledge of the facts;
- ✓ the actual manner in which the unlawful conduct was carried out;
- ✓ the special interests in the pursuit of which the conduct was unlawfully aimed.

It should consequently concern facts and circumstances that can be ascertained and are known directly by the whistleblower (and not reported or referred to by others).

The violations reported must be those that are typified and affect the public interest or the interest in the integrity of the Organization, and may not concern disputes, claims or requests related to an interest of a personal nature of the reporting person that pertain exclusively to his or her individual work relationships or are inherent to his or her work relationships with hierarchically superior figures.

Moreover, reports may not relate to violations where they are already mandatorily regulated by European Union or national acts (Annex to the Whistleblowing Decree, Part II; Annex to the EU Directive, Part II - Financial Services, Products and Markets; Prevention of Money Laundering and Financing of Terrorism;

Transportation Safety; Environmental Protection) or violations relating to national security, as well as procurement relating to defense or national security aspects, unless such aspects are covered by relevant secondary legislation of the European Union.

Reports based on mere suppositions and/or suspicions and/or personal opinions of the Whistleblower and/or any third parties indicated by the Whistleblower are not worthy of protection and, consequently, are not subject to examination by the Company.

Therefore, reports should meet the following requirements:

- be made in good faith;
- be substantiated and based on precise and concordant facts;
- relate to facts ascertainable and known directly to the reporting party;
- contain all the information necessary to identify the authors of the facts or conduct reported and any useful information to describe the subject of the report. In any case, the reporting party must provide, in a clear and complete manner, all the elements useful to carry out the checks and verifications necessary to assess its validity and objectivity, indicating:
 - references to the course of events (e.g., date, place);
 - any information and/or evidence that may provide valid corroboration regarding the substance of what has been reported;
 - the generalities or other elements that would make it possible to identify the person who committed what has been reported;
 - the particulars of any other individuals who may be able to provide information about the facts being reported;

4.3 Exclusions

The report must be made in good faith and must not take an insulting tone or contain personal insults or moral judgments designed to offend or harm the honor and/or personal and/or professional decorum of the person or persons to whom the reported facts are allegedly ascribed. It is especially prohibited to make reports in “bad faith” and more specifically:

- the submission of reports with purely defamatory or slanderous purposes;
- the forwarding of reports that relate exclusively to aspects of private life, without any direct or indirect connection with the reported person's business activities;
- the forwarding of reports of a discriminatory nature, insofar as they refer to sexual, religious and political orientations or to the racial or ethnic origin of the reported person;
- the submission of reports in violation of the law.

“Bad faith”, insulting, offensive, defamatory, libelous and discriminatory reports may give rise to civil and/or criminal liability against the reporter and the application of sanctions in accordance with the last paragraph of this procedure.

The protections under this procedure are not applicable to reports of information that is already totally in the public domain, unsubstantiated news and so-called “rumors.”

4.4 Who can make a report

Reports may be made by:

- ✓ organization staff, including probationary workers, former employees and Candidates in personnel selections;
- ✓ self-employed workers, collaborators, who perform their work for the Organization;
- ✓ suppliers;
- ✓ customers
- ✓ collaborators, freelancers and consultants who perform their activities on behalf of the Company;
- ✓ interns and trainees;
- ✓ individuals with administrative, management, control, supervisory or representative functions at the Company.

The provisions contained in this procedure do not exempt - in any way - those persons who, holding the title of public official or public service appointee, are under obligation to report in accordance with the provisions of Article 331 of the Code of Criminal Procedure and Articles 361 and 362 of the Criminal Code.

4.5 When can a report be made?

The reporting party can file the report:

- 1) when the legal relationship is ongoing;
- 2) during the probationary period;
- 3) when the legal relationship has not yet begun, if the information on violations was acquired during the selection process or other pre-contractual stages;
- 4) after the dissolution of the legal relationship if the information on violations was acquired before the dissolution of the legal relationship.

4.6 Anonymous Reporting

Anonymous reports, where substantiated, according to ART are treated as equal to ordinary reports, considered in their own "ordinary" supervisory proceedings. Ordinary reporting means reporting exempt from the forms of protection provided by whistleblowing under Decree 24/2023.

The Organization has determined to give the possibility, through the chosen channel, to process all reports, including anonymous ones, under the whistleblowing protection regime.

Therefore, without prejudice to the registration of any form of whistleblowing, even anonymous reports will be taken into consideration, when they are adequately substantiated and made with an abundance of details and, in any case, such as to bring out facts and situations by relating them to specific contexts (e.g. indication of particular names or qualifications, mention of specific offices, proceedings or particular events, etc.).

Once a report is received through the established internal channel or by hard copy, a record will be made of the anonymous reports received and documentation will be retained no longer than five years, starting from the date of receipt of said reports, thus making it possible to trace them, in case the reporter, or whistleblower, informs ART that he or she has suffered retaliatory measures because of that anonymous report or complaint.

4.7 Reporting Modes

Reports should be submitted through the channels specifically provided for this purpose:

- internal channel;
- external channel (managed by ART);
- Public Disclosure;
- reporting to the judicial or accounting authority.

As a priority, the use of the internal channel should be encouraged, and only when one of the conditions set forth in Article 6 of Legislative Decree 24/2023 is met, can an external report be made to ART.

4.7.1 Internal channel

The Company provides reporters with various channels through which they can report violations, following this procedure, in particular, it is possible to make reports in oral (non-anonymous) and written (anonymous) form.

As far as reports in written form are concerned, the encrypted computer platform “SIGNALETHIC” provided by SANMARCO INFORMATICA SPA is available to every individual who wishes to file a report.

The SIGNALETHIC platform is a web service that enables the user to fill out a form to report one or more acts of misconduct.

This tool guarantees, from a technological point of view, the confidentiality of the reporting person, the subjects mentioned in the report and the content of the report.

A questionnaire is uploaded on the platform that guides the individual who wishes to file a report through open and closed questions, some of which are mandatory. It is also possible to attach documents to the report. Upon completion, a unique code and password are given to the individual, with which he/she can access the report and communicate bidirectionally with the receiving party, exchange messages and send new information. All information contained on the platform is encrypted and can be read only by individuals who are authorized to receive the report (i.e., visible within the system only by the Report Manager or assigned persons in the support team).

The access link is the following → <https://artspa.signalethic.it/signalethic/>

The main features of the platform are:

- the reporter can make the report either as “internal” to the company or as “external.”
- the report is made by filling out a form made available on the platform which is also free-fill;
- documents can be uploaded to support the report;
- The person making the report can also proceed to enter an anonymous report. The system automatically issues a code that can be used to follow the reporting process, that is, to access the platform's message area;
- with the submission of the report, he/she will be given credentials - report number and password - which must be retained in order to: access the report again, check the response of the reporting agency, and to dialogue with the agency by responding to requests for clarification or further investigation;
- an oral report can also be made by recording and uploading to the voice message platform;
- the report is received and handled while maintaining the reporter's right to confidentiality;
- the report can be made from any digital device (pc, tablet, smartphone) and from any location.

An “acknowledgement of receipt” of the report will be provided to the reporting person within seven days of receipt, and feedback on the report should be given within a time period of no more than three months.

4.7.2 External channel

The competent authority for external reporting is ART, which makes the above-mentioned platform available to any potential whistleblowers. However, it is important to bear in mind that it is possible to report to the Authority only if one of the following conditions is met:

- if there is no provision within the work context for mandatory activation of the internal reporting channel or this channel, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4 of Legislative Decree 24/2023;
- the reporting person has already made an internal report and it has not been followed up. Reference is made to cases in which the internal channel was used but did not function properly, in the sense that the report was not dealt with within a reasonable time, or no action was taken to address the violation;
- the reporting person has reasonable grounds to believe that, if he or she made an internal report, it would not be effectively followed up or that the report itself may result in the risk of retaliation. This is the case when, for example, there is a risk that the violation or related evidence could be concealed or destroyed, the effectiveness of investigations carried out by the relevant authorities could otherwise be compromised, or even because it is believed that ART would be better suited to deal with the specific violations, especially in matters that lie within its field of competence;
- the reporting person has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest. These are cases where the violation requires urgent action, to safeguard the health and safety of people or to protect the environment.
- the reporting person has well-founded reason to believe that evidence may be concealed or destroyed, or where there is well-founded fear that the person receiving the report may be colluding with the perpetrator or involved in the violation itself.

4.7.3 Public Disclosure

In accordance with the regulations, there also exists the possibility for the reporter to make a public disclosure, benefiting from the protection provided under the law.

At least one of the following conditions must be met in order to use this procedure:

- that the internal and/or external channel has been used beforehand, but there has been no response or no follow-up within the timeframe stipulated in the decree;
- that the whistleblower believes there are reasonable grounds to believe that there is an “imminent and obvious danger to the public interest,” considered to be a situation of emergency or risk of irreversible damage, including to the physical safety of one or more persons, which requires that the violation be promptly disclosed with extensive exposure in order to prevent its effects;
- that the whistleblower feels that there are reasonable grounds to believe that the external report may pose a risk of retaliation or may not be effectively followed up because, for example, there may be a danger of destruction of evidence or collusion between the reporting authority and the violator.

It should in other words be in particularly serious situations of negligence or malicious behavior within the company.

5 Management of the Reporting Procedure

5.1 Who receives reports

The person appointed by the Organization to receive and review reports (manager in charge of reports) is an experienced professional in the field, with autonomy and independence from the Company's internal roles who reports directly with the SB (appointed by the board) and with Management.

This person must possess the following characteristics:

- independence and impartiality;
- specific and adequate theoretical and regulatory training,
- specific training inherent to the handling of reports.

This necessary third party status should be framed as “impartiality and independence” of the person in charge. Confindustria guidelines have defined what is to be understood by:

- impartiality: i.e., lack of conditioning and bias against the parties involved in the reports, in order to ensure fair management free from internal and/or external influences that could compromise objectivity;
- independence: i.e., autonomy and freedom from management influence or interference, so as to ensure objective and impartial analysis of the report.

Specialized expertise in crime and investigative acquisition with respect to the case being reported is also essential. The appointed manager must follow the procedure issued by the company for the handling of reports.

In accordance with Article 5 of Legislative Decree 24/2023, the person entrusted with the management of the internal reporting channel (IT platform) performs the following activities:

- issues the reporting person with an acknowledgement of receipt of the report within seven days from the date of receipt;
- maintains contact with the reporting person and has the ability to request additional information from the reporting person, if necessary;
- gives diligent follow-up to any reports received;
- provides a response to the report within three months from the date of the acknowledgement of receipt or, if this is lacking, within three months from the end of the period of seven days following the submission of the report;;
- makes available clear information on the channel covering procedures and prerequisites for making internal reports, as well as providing procedures and prerequisites for making external reports on the same channel. The aforementioned information shall be displayed and made easily visible in the workplaces, as well as being accessible to persons who, while not attending workplaces, have a legal relationship in one of the forms referred to in Article 3, paragraphs 3 or 4 of Legislative Decree 24/2023.

The Organization publishes the information and procedures related to reporting in a dedicated section of its aforementioned website www.artgroup-spa.com .

If the report is made through an in-person meeting, the report may be recorded or minuted with the consent of the Reporter. Any minutes may be verified, corrected and confirmed by the reporter by signature.

An internal report submitted to a person other than the Manager shall be forwarded within seven days of its receipt to the appropriate person, giving simultaneous notice of the transmission to the reporting individual.

The Company would like to point out that the figure of the so-called Facilitator is also envisaged, who is an individual who assists the reporter in the reporting process, operating within the same work context, whose assistance is kept confidential and enjoys the safeguards envisaged by the decree.

5.2 Receipt and Acceptance of the Report

In the case of a report made through the application which is made available by the Organization, the system logs the report and notifies the Manager, who issues the reporter with an acknowledgement of receipt within 7 days from the date of receipt. The acknowledgment of receipt may include, among other things:

- (a) reassurance and request as to the preferred method for continuing the interaction (e.g., the report was made online, but the whistleblower would prefer to continue in person);
- (b) information on the next steps in the process of handling the report, related timelines and possible outcomes (e.g., what further feedback to expect and when);
- (c) information, including through reference to this procedure, on the measures taken to protect the whistleblower, including measures to protect the whistleblower's identity, as well as the whistleblower's responsibilities for loyal cooperation as well as for effective consideration and protection by the institution.

5.2.1 Preliminary Evaluation of the Report

The Manager shall conduct a preliminary examination of the report in order to verify whether it concerns possible violations or retaliations that are within the objective and subjective scope of this procedure. Verification as to whether the circumstances represented in the report are well-founded, are entrusted to the Manager, who carries it out in accordance with the principles of impartiality and confidentiality and any other persons who may report on the facts reported.

In the event that the Manager considers that the report does not fall within the scope of application of this procedure, he/she shall notify the reporter, specifying the reasons and indicating the internal office that may be responsible for handling the issue reported.

If, upon verification, the report is found to be well-founded, the Manager may take action:

- a) taking appropriate measures within his/her competence;
- b) by filing a complaint with the competent judicial authority;
- c) by communicating the outcome of the investigation to the parties responsible for taking management measures, including, if the conditions exist, the exercise of disciplinary action;
- d) through the relevant structures, taking any further measures and/or actions that may be necessary in the specific case to protect the Company.

When there are multiple reports that need to be handled simultaneously, the Manager will assess the urgency of action based on the likelihood of the violation and its potential impact on the Organization, taking into account the following factors:

- Can the violation take on criminal relevance?
- Has the violation already occurred, is it in progress, or is it about to occur?
- Is there an immediate need to stop or suspend business activities?
- Is there an immediate risk to health and safety?
- Is there an immediate risk to human rights or the environment?
- Does the need to secure and protect evidence before it is deleted or destroyed exist?
- Is there a risk to the Organization's Business Management Processes, functions, services, and/or reputation?
- Can the report impact business continuity?
- What media impact might the report have?
- Is additional information available to support the report?
- What is the nature of the wrongdoing (type and frequency of the violation, role and seniority of those involved in the report)?

- What is the likelihood that the violation will also be reported outside the organization?
- Has the violation been reported before?
- How did the reporter obtain the information: is the information “first-hand” or “hearsay”?

5.2.2 Request for Further Information

Where not already in the report, the manager may ask the reporter for, among other things, the following additional information:

- Where did the violation take place?
- When did the violation occur (past, current, future, ongoing)?
- Who is involved in the violation?
- Have you reported it previously? If yes, what, when, and to whom? What action was taken?
- What is the impact to the organization from your perspective?
- Is management involved or aware of the violation?
- Do you perceive risks to yourself or others?
- Do you have documents or other evidence to support your report?
- Is there anyone else who has direct knowledge of the violation that we can contact?
- Has anyone tried to hide the violation or discourage you from sharing your concern? If so, who and how?

5.2.3 Investigation of the violation reported

The Manager shall investigate the reported violation by performing one or more of the following activities:

- (a) involvement of relevant business functions to support the investigation (e.g., IT, HR, internal audit, EMS manager, health and safety, and finance), unless this would compromise the reporter's confidence, the Manager's impartiality, or the successful outcome of the investigation;
- (b) collection of documentary evidence to corroborate the report;
- (c) conduct interviews of any persons in a position to supply information that may be useful in investigating the violation;
- (d) interview of the reported individual, informing him or her in advance of the subject of the meeting, which the Manager must necessarily provide in the event of a request by the latter, including by obtaining written comments and documents.

It is everyone's duty to cooperate with the Manager in the investigation of the reported violation.

The Manager shall document in writing the interviews conducted by means of a special report, the contents of which must be submitted to the interviewee for his or her amendment and signature, if necessary.

During the course of the investigation, the Manager shall maintain contact with the reporter and, if necessary, may request additional information from the reporter.

In any case, the Manager shall protect the identity of the persons involved and mentioned in the report until the final conclusion of the fact-finding process.

5.3 Assessment and prevention of the risk of retaliation

The Manager is to evaluate the risk of retaliation for the reporter based on the following risk factors:

- likelihood of breach of confidentiality. For example: is anyone else aware of the breach? Has the breach been reported to anyone else? Could the nature of the information reveal their identity? Are they the only ones who have access to the information? Does the violation constitute a crime whose proof requires that the identity of the reporter be revealed?

- Danger of retaliation. e.g., has retaliatory conduct already occurred or do you perceive an imminent risk of retaliation?
- Involvement of the reporter in the violation.
- Reporting involves various types of violations.
- Manner of acquisition by the reporter of the violation.
- Interpersonal relationship between the reporter and the reported.
- Relationship between the reporter and the company?

The level of protection and related actions taken are dependent on the type and timing of the report and the potential consequences of the violation.

If the Manager does not have the power to devise and implement strategies to prevent possible harm to the reporter (e.g., internal reorganization of personnel), he or she shall notify the reporter in order to allow the reporter to consent to the disclosure of his or her identity to whomever within the company has such power, subject, however, to the other protections provided in this procedure in the event that any retaliation is then in fact carried out.

5.4 Outcome of investigations carried out by Manager

The Manager shall complete the process of handling the report within 3 months from the date of acknowledgement of receipt and in any case within 3 months and 7 days from the date of receipt of the report by notifying the reporter of the outcome of the investigations.

In the event that the investigations cannot be completed in a timely manner, for example because they are particularly complex, within the same period of time the Manager shall update the reporter on the status of the report and inform the reporter of the additional period of time needed to complete investigations.

Among the possible outcomes that can be communicated to the reporting individual are:

- correction of internal processes;
- initiation of disciplinary proceedings;
- transfer of the results of fact-finding activities to the Public Prosecutor's Office (and/or the Court of Auditors in the event of fiscal harm);
- archiving due to lack of evidence.

At the close of each process of investigation, the Manager should draw up a special report intended for the Management and the SB, in which he/she gives an account of the handling process of the report received and the outcome of the investigations carried out with particular reference to:

- a) the non-existence of the reported violation or retaliation, specifying whether the report is believed to have been made in bad faith for the purpose of determining the possible application of disciplinary sanction against the reporter;
- b) the existence or risk of occurrence of the reported violation or retaliation, specifying the person held responsible and the elements collected.

The report does **not** mention the identity of the reporter and any other information likely to identify him or her, except in those cases where the report was made in bad faith or where the reporter is believed to be responsible for the violation that has been ascertained.

5.5 Actions which follow the clear finding of a violation or retaliation

Management and SB evaluate the contents of the report and take appropriate actions upon the outcome of the findings made by the Manager. In particular:

- (a) in the event of incompleteness of the investigations carried out by the Manager, they can carry out further investigations, including through the relevant corporate functions, a trusted advocate or an external consultant;
- b) in the event of an ascertained violation or the risk of violation, they take appropriate measures to prevent, interrupt or remedy the violation, as well as appropriate disciplinary measures against any person deemed responsible for the violation;
- (c) if there is determined to be a definite risk of retaliation, they should take appropriate measures to protect the reporter (e.g., internal reorganization of personnel);
- d) in cases of established retaliation, implemented or even only threatened, against the whistleblower, they should take appropriate measures to remedy the retaliation suffered (e.g., reinstatement of the whistleblower to his or her previous job position), as well as appropriate disciplinary measures against any person deemed responsible for the retaliation;
- (e) in the event that the reporter is found to have acted in bad faith in making the report, they should take appropriate disciplinary measures against the reporter.

The Management and SB communicate any actions undertaken to the Manager, for timely feedback to the reporter, as well as regularly monitoring the effectiveness of the measures taken.

The report management process concludes with the reporting party being notified of the outcome of the investigations conducted and any actions taken as a result by Management.

6 Forms of Protection for the Reporting Individual

6.1 Measures to Protect the Reporter

The Whistleblower and related persons shall be accorded the protections provided herein, provided that their report was made in good faith and, in the case of an external report or public disclosure, provided the relevant prerequisites are met.

The person's motives for reporting are irrelevant to his or her protection.

Valuing the reporting person's good faith, it is foreseen that he or she will benefit from the protections only if, at the time of reporting, he or she had reasonable grounds to believe that the information about the reported, publicly disclosed, or reported violations was true.

The protections also apply in cases of anonymous reporting if the reporter was later identified and retaliated against.

6.1.1 Prohibition of waivers and settlements

Waivers and settlements - not signed in a protected venue - of the rights and remedies foreseen by Legislative Decree 24/2023 are prohibited. This provision responds to the need to implement and make effective the protection of the whistleblower, as a vulnerable subject, as well as other protected subjects, who, as a result of reporting, disclosure or whistleblowing, could suffer detrimental effects.

6.1.2 Duty of Confidentiality to the Reporter

The Manager is required to deal with reports while preserving their confidentiality. Information regarding the identity of the Reporting Person, the person reported, and any other individuals mentioned in the

report shall be treated in accordance with the principles of confidentiality. Likewise, all information contained in the report is also to be treated confidentially.

The identity of the reporting person may not be disclosed without his or her consent.

The only reason for possible disclosure of the identity of the reporting person may occur in the event that the investigative documents are forwarded to an ordinary public prosecutor's office or accountant's office and knowledge of the same is necessary for the purposes of the right of defense during an ordinary judicial or accounting proceeding at the Court of Auditors.

In the context of disciplinary proceedings, the identity of the Whistleblower may not be disclosed, where the allegation of the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to it.

If the charge of the disciplinary offense is based, in whole or in part, on the report and the knowledge of the identity of the Whistleblower it is therefore essential for the defense of the accused, the report will be usable for the purposes of disciplinary proceedings only in the presence of written consent of the Whistleblower to the disclosure of his or her identity.

The Manager shall assess at the request of the accused, whether the prerequisites are met with regard to the need to know the identity of the Whistleblower for the purposes of the right of defense, giving adequate reasons for his decision both if the request is granted and if it is denied.

The Head of Disciplinary Proceedings shall rule on the accused's petition, communicating the outcome to the latter.

In criminal proceedings, the identity of the Whistleblower is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.

The identity of the Whistleblower may not be disclosed to any external consultants called in to support the handling of the report.

This is notwithstanding the provisions of special laws that require that the identity of the Whistleblower is to be disclosed exclusively to the proceeding Authorities (e.g., criminal, tax or administrative investigations, inspections, etc.).

The reporting by name and the documentation attached to it are, in any case, subtracted from access to administrative acts as per Articles 22 et seq. of Law No. 241/1990, generalized civic access as per Article 5, paragraph 2, of Legislative Decree 33/2013 as well as access as per Article 15 of Reg. Eu. 679/16.

In the information regarding the processing of personal data provided to the Reporting Party at the time of reporting, also via online platform, the Reporting Party is informed of the possibility for which the report could be forwarded to the competent subjects according to the provisions of the law.

6.2 Processing of Personal Data

Personal data of whistleblowers, any persons reported and any individuals involved in the event concerned are processed in accordance with the current legislation regarding the protection of personal data. In particular, the Company ensures that the processing of personal data is carried out with respect for the fundamental rights and freedoms, as well as the dignity of those concerned with particular reference to confidentiality and data security. In particular, it is highlighted in this context that:

- the privacy policy is made available on the Segnaletic portal, which constitutes an integral and substantive part of this procedure, in which are indicated, the purposes and methods of the processing of personal data, the Owner of the processing of personal data, the categories and offices to which the reported data may be transmitted as part of the management of the report, the data retention periods, as well as the rights that can be exercised by the reporter with reference to their personal data;
- the reporting system foresees the processing only of personal data that are strictly necessary and relevant to the purposes for which they are collected. Reports that have been assessed as not relevant under this procedure are archived and not further processed;

- appropriate technical and organizational measures are put in place in order to ensure the security of personal data, in accordance with current regulations, and in particular, encryption of transmissions and encryption of data residing on the information systems pertaining to the reports is guaranteed;
- the Company has carried out an Impact Assessment (DPIA) on data processing for whistleblowing in view of the fact that data processing “may present a high risk to the rights and freedoms of physical persons” ex art. 35 of EU Reg. 679/16.

The outcome of this assessment has defined as acceptable the risk of such processing and the organizational and technical security measures put in place for its adequate protection and the protection of the rights of those concerned.

Reports received, assessment activities, and communications between the reporting individual and the Manager are documented and maintained in accordance with confidentiality and data protection requirements.

Reports contain personal data and may be handled and maintained only for as long as necessary for their processing: this time includes analysis, assessment activities, and communication of outcomes, as well as any additional timeframe for possible additional comments.

In no case will reports be retained beyond 5 years after the outcome of the assessment activities is communicated to the reporting person.

Regarding access to personal data, these are known only to the Manager and, if indicated in a specific organizational act, to members of staff supporting the management of the report.

In the course of the assessment activities, the Manager may share with other functions of the company information that has been previously anonymized and minimized in relation to the specific activities for which they are responsible.

6.3 Prohibition of Retaliatory Acts against the Reporting Individual

A whistleblower who makes a report whether through the internal channel or in accordance with the other modalities provided for, relating to unlawful conduct of which he or she has become aware by reason of his or her employment relationship, may not be sanctioned, demoted, dismissed, transferred, or subjected to any other organizational measure having direct or indirect negative effects on working conditions determined by the report.

The following are some examples of cases that may be considered retaliation, even if attempted or threatened, following reports of wrongdoing:

- Dismissal, suspension (including from training) or equivalent measures
- Demotion (downgrading) or non-promotion
- Job change, transfer, salary reduction, changes in working hours
- Negative merit notes (for variable disbursement)
- Negative references
- Disciplinary measures
- Coercion, intimidation, harassment or ostracism
- Discrimination or any unfavorable treatment
- Failure to convert or renew a fixed-term employment contract into an employment contract of indefinite duration (in the case of legitimate expectation of conversion)
- Failure to renew or early termination of a fixed-term employment contract
- Damage, including to the person's reputation, particularly on social media, or economic or financial injury, including loss of economic opportunities and loss of income

- Blacklisting
- Early termination or cancellation of a contract for the provision of goods or services
- Cancellation of a license or permit
- Request for submission to psychiatric or medical examinations

It is the Company's responsibility to prove that any discriminatory or retaliatory measures - if and insofar as established as such - taken against the Whistleblower are motivated by reasons unrelated to the report itself.

Established discriminatory or retaliatory acts taken are null and void.

6.4 Other protected parties

The same protection provided for the Reporting Party also applies to:

- to the facilitator (an individual who assists the whistleblower in the reporting process, operating within the same work context and whose assistance must remain confidential);
- to persons in the same work context as the reporting person, or the person who made a complaint or public disclosure and who are related to them by a stable emotional or kinship relationship up to the fourth degree;
- to co-workers of the reporting person or the person who has made a complaint or made a public disclosure, who work in the same work environment as the reporting person and who have a regular and current relationship with said person;
- to entities owned by the reporting person, the person who made a complaint or made a public disclosure or for which the same persons work as well as entities that work in the same work environment as the said persons;
- Anonymous whistleblowers, if subsequently identified and subject to retaliation.

6.5 Limits of Criminal, Civil, Administrative Responsibility

In the event that it is necessary to reveal confidential information or information offensive to the reputation of the company in order to make the report, any criminal, civil and administrative liability of the reporter and related persons is waived, provided that the information is related to the report and strictly necessary to reveal the violation.

In any case, reports must relate to lawfully acquired information.

Making a report does not, however, relieve the reporter of his or her possible responsibilities in relation to the reported violation.

6.6 Whistleblowing Framework and Organization Model 231

Whistleblowing regulations are closely linked to the 231 Organizational Model adopted by ART. Therefore, the Model indicates the internal reporting channels adopted by ART in accordance with the whistleblowing regulations, taking care to make explicit: the reference to the prohibition of the perpetration of any act of retaliation as cited in the regulation and the observance of the duties of confidentiality in the processing of information regarding the handling of reports. The Company has taken steps to supplement the Disciplinary System of the 231 Organizational Model itself, considering that the whistleblowing regulations require that it be adjusted by providing for sanctions against those responsible for violations for which the ART applies administrative fines. Specifically, these are the following cases:

COPYRIGHT ART SPA. ALL RIGHTS RESERVED

The information contained in this document, is the confidential, proprietary information of ART SPA, and may not be reproduced, disclosed to any third party or used, for other than the intended purpose for which it was provided to the original recipient, without the prior written approval of ART SPA.

- the committing of any act of retaliation - to be understood as conduct, act or omission, even if only attempted or threatened, carried out by reason of the whistleblowing (of the report to the judicial or accounting authority or public disclosure) - that causes or may cause, directly or indirectly, unfair harm to the person making the report (or the person who made the report or made a public disclosure) and/or the other persons specifically identified by the norm
- the non-establishment of whistleblowing channels, the failure to adopt whistleblowing procedures in accordance with the regulations or even the failure to carry out verification and analysis activities regarding the reports received;
- the implementation of actions or conduct by which whistleblowing was obstructed or attempted to be obstructed;
- the violation of the obligation of confidentiality.

In addition, disciplinary sanctions have been foreseen in the event that the whistleblower has been found to be responsible, even by a judgment of first instance, for the crimes of defamation or slander (or in any case for the same crimes committed in connection with whistleblowing) or his or her civil liability in cases of willful misconduct or gross negligence.

6.7 Exclusion of Protection for the Reporting Person

Without prejudicing the specific assumptions of limitation of liability, the protection provided in case of retaliation is not guaranteed when the reporting person's criminal liability for the offenses of defamation or slander or otherwise for the same offenses committed with the report to the judicial or accounting authority or his or her civil liability, for the same offense, in cases of malice or gross negligence, is established, even by a judgment of first instance. If liability is established, a disciplinary sanction shall also be imposed on the reporting or whistleblowing person.

Any forms of abuse of this Policy, such as reports that are manifestly opportunistic and/or made for the sole purpose of harming the reported person or other persons, as well as any other hypothesis of improper use of the institution of whistleblowing, are also a source of liability, in disciplinary and other competent venues.

6.8 Support Measures

A list of Third Sector entities that provide reporting persons with support services has been established at ART.

The list, published by the ART on its website, contains Third Sector entities that carry out, according to the provisions of their respective statutes, the activities referred to in Article 5, paragraph 1 (v) and (w) of Legislative Decree No. 117 of July 3, 2017, and have entered into agreements with ART.

Support measures consist of information, assistance and advice free of charge on how to report and the protection from retaliation offered by national and European Union regulatory provisions, the rights of the person involved, and the terms and conditions of access to legal aid.

6.9 Training Obligations

Training of support staff to the Manager is of paramount importance to ensure that reports received are handled appropriately and in accordance with applicable regulations. To this end, the Manager and support staff receive appropriate training in relation to certain key topics.

By way of example though not exhaustive, some topics with respect to which staff must be adequately trained are outlined below:

- ✓ regulatory aspects, covering the principles and provisions contained in the Decree, with specific focus on the requirements that must be carried out by the personnel entrusted with the management of the reporting channel (e.g., the activities foreseen by art. 5 of the Decree), as well as with respect to the requirements in the area of Data Protection;
- ✓ procedures and prerequisites: in-depth overview of policies, procedures and operating methods adopted, including in practice, by the company for the management of the reporting channel (e.g., the phases of management of reports from the moment of receipt, to the subsequent activity of investigation and feedback to the reporter);
- ✓ general principles of behavior: in order to foster adequate understanding and awareness of certain general principles such as:
 - confidentiality and discretion: the need for appropriate technical and organizational measures to be applied by personnel entrusted with the handling of reports in order to safeguard the confidentiality of information throughout the reporting process;
 - ethics and integrity: promotion of an ethical and integral environment within the company, as well as regarding the importance of acting with honesty, transparency and responsibility in the handling of whistleblowing;
 - active listening, communication skills and collaboration: raising awareness among personnel entrusted with the management of reports about active listening, empathic communication and understanding of the psychological aspects inherent in the management of reports, with particular regard to interacting with the reporting person, as well as about appropriate and adequate team collaboration practices with other business functions involved in the management of the report (e.g., legal functions, SB).

This training will be provided on a periodic basis, in order to ensure its effectiveness, supplementing and rescheduling the training planning in the event of regulatory updates regarding relevant and applicable provisions regarding the management of reporting channels.

In addition, the Company will make sure to provide adequate training on the issues set forth to all internal personnel (including the regulations on the processing of personal data), so as to create an appropriate awareness of the purposes and protections recognized by the Decree, as well as a culture of integrity and responsibility within the company.

6.10 Sanctions

Violations of this procedure shall assume disciplinary significance and shall be punished in accordance with the provisions of the internal disciplinary system or the applicable collective bargaining agreement. By way of example, the following constitute punishable violations:

- (a) making the report in bad faith;
- (b) making a report whose defamatory or libelous nature has been established by the judicial authority;
- (c) disclosure of the identity of the reporter, related persons and any other information from which their identity may be inferred;
- (d) any conduct aimed at obstructing the reporting;
- (e) any attempt to identify the reporter;
- (f) the failure to handle the report due to malicious intent or gross negligence, including the failure of those empowered to do so to remedy the reported violations or retaliatory actions;
- (g) engaging in retaliatory conduct.

Violations of this procedure by third parties, who are not employees of the entity, may be sanctioned under a specific contractual clause