

WHISTLEBLOWING

2024

English Version

TABLE OF CONTENTS

1. AIM
2. APPLICATION FIELD
3. REFERENCES
4. DEFINITIONS
5. RESPONSIBILITY
6. PEOPLE WHO MAY MAKE A REPORT (SO-CALLED REPORTERS)
7. INTERNAL REPORT CHANNEL
8. EXTERNAL REPORT
9. PUBLIC DISCLOSURE
10. OBLIGATION OF CONFIDENTIALITY
11. PROTECTION OF PERSONAL DATA
12. PROTECTION AND SUPPORT MEASURES
13. PENALTY REGIME
14. ATTACHMENTS

1. AIM

This procedure is adopted by the company in compliance with the provisions of Legislative Decree No. 24 of 10 March 2023, in force as of 30 March 2023, which transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 concerning the protection of persons who report breaches of national or European Union regulatory provisions (so-called whistleblowing directive) of which they become aware in the context of their work, which are detrimental to the public interest or the integrity of the public administration or private entity.

2. APPLICATION FIELD

This procedure applies to any report of information on violations (as better specified in Section 4) acquired within the work context, if detrimental to the public interest or to the integrity of the public administration or of the private entity, made through the appropriate reporting channels made available by the Company.

The following are excluded from the application of this procedure

- disputes, claims or requests linked to an interest of a personal nature that relate exclusively to individual labour relations, or to labour relations with hierarchically superior figures
- breaches relating to national security, as well as to contracts relating to defence or national security aspects;
- violations mandatorily regulated by European Union or national acts[1] that already ensure appropriate reporting procedures.

[1] Please refer to the Annexes to Directive 2019/1937 and Legislative Decree 24/23.

3. RIFERIMENTI

- Legislative Decree No. 24 of 10 March 2023;
- Directive (EU) 2019/1937;
- Organisation, management and control model ex Legislative Decree 231/01;
- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree 196/2003 as amended);
- ANAC Guidelines on the protection of persons who report violations of Union law and the protection of persons who report violations of national laws - procedures for the submission and management of external reports.

4. DEFINITIONS

"alerts": any in written, oral or in an interview communication, including in an anonymous form, containing information about breaches;

"breaches": offences falling within the scope of relevant EU or national acts relating to public procurement, services, products and financial markets, prevention of money laundering, product safety and compliance, transport safety, protection of the environment, food and animal feed safety, animal health and welfare, public health, consumer protection, protection of life and protection of personal data, security of networks and information systems [2]; breaches (acts or omissions) affecting the financial interests of the EU (ref. Article 325

of the Treaty on the Functioning of the European Union); violations (acts or omissions) of competition and state aid rules (ref. Article 26(2) of the Treaty on the Functioning of the European Union); violations (acts or omissions) of corporate tax rules;

[2] Please refer to the annexes of Directive 2019/1937 and Legislative Decree 24/2023.

"information on breaches": all information, including well-founded suspicions, concerning breaches committed or which, on the basis of concrete elements, could be committed in the organisation with which the reporting person or the person making the report to the judicial/accounting authority has a legal relationship, and also information concerning conduct aimed at concealing such breaches;

"internal reporting": communication of "whistleblowing" through the designated internal reporting channel;

"external reporting": written or oral communication of information on violations, submitted through the external reporting channel^[3];

"public disclosure": disclosure of information on breaches in the public domain through the press or electronic media or in any case through means of dissemination capable of reaching a large number of people;

"whistleblower": an individual who reports or publicly discloses information on breaches acquired in the context of his/her work;

[3] cfr. art. 7 del D.Lgs. 24/2023.

'Facilitator': an individual who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;

"work context": present or past work or professional activities through which, irrespective of the nature of such activities, a person acquires information about violations and in the context of which he/she could risk retaliation in the event of a report or public disclosure or a report to the judicial or accounting authorities

"person involved": a physical or legal person mentioned in the report as a person to whom the violation is attributed or as a person otherwise implicated in the reported violation;

"person in charge of managing the channel": a person identified by the Company responsible for managing the channel and the report and endowed with organisational and functional autonomy;

"Retaliation": any conduct, act or omission, even if only attempted or threatened, occurring as a result of the report and closely related to it, to the denunciation to the judicial or accounting authorities or to public disclosure, and which causes or may cause to the person making the report, directly or indirectly, unjust damage;

"follow-up": the action(s) taken by the person entrusted with the management of the reporting channel;

"acknowledgement": communication to the reporting person of information concerning the action taken or intended to be taken on the report, including the measures planned or taken or to be taken and the reasons for the choice made;

"platform": an internal reporting channel adopted by the Company (as further specified in paragraph 7) to transmit information on breaches;

5. RESPONSIBILITY

The person in charge of managing the reporting channel, also by using the platform

- makes available, including by means of this procedure and the information published on the platform, clear information on the channel, procedures and prerequisites for making internal reports
- issues the reporting person with an acknowledgement of receiving the report within the specified deadlines;
- assesses the criteria for processability of the report;
- diligently follows up the reports received;
- provides the reporting person with feedback on the closure of the processing of the report;
- maintains contact with the reporting person and may request additional information from the latter, if necessary;
- files and stores the documentation on the report within the timeframe required by law;
- ensures respect for the principle of confidentiality.

The whistleblower:

- transmits reports in accordance with this procedure;
- is required to provide detailed information on the matter reported.

The legal representative:

- Talks with ANAC in the event of any external reporting or activation of inspection activities by ANAC.

The Administrative Body:

- ensures that any measures are taken in compliance with the provisions of the CCNL or the internal rules;
- approves this procedure together with the related organisational role structure;
- ensures compliance with the measures for the protection of the reporting person.

6. PEOPLE WHO MAY MAKE A REPORT (SO-CALLED "REPORTER")

The following are allowed to make a report

- employees (public and private);
- self-employed workers and collaborators working for public and private entities;
- self-employed professionals;
- volunteers;
- consultants;
- shareholders;
- directors;
- providers of services for third parties in any capacity whatsoever (regardless of the nature of such activities) even in the absence of remuneration;
- trainees, including unpaid ones;
- persons exercising functions of administration, management, control, supervision or representation, even if the relevant activities are performed de facto and not de jure.

This category also includes all those persons who, for any reason, become aware of unlawful acts within the Company's working context, i.e:

- when the employment relationship has not yet started
- during the probationary period
- upon termination of the relationship.

7. INTERNAL REPORT CHANNEL

The Company has provided for an internal reporting channel to be used by whistleblowers for the transmission of information on violations. The use of this channel allows for more effective prevention and detection of violations. This choice responds to the principle of fostering a culture of good communication and corporate social responsibility, as well as improving the organisation.

The internal reporting channel provides for written or oral reports through the Whistleblowing platform accessible through the link <https://whistleblowersoftware.com/secure/Besenzoni> or the related qr code made available by the company to all interested parties.

Internal whistleblowing reports in oral form are made, at the request of the reporting person through the platform itself, by means of a face-to-face meeting set within a reasonable period of time.

The internal whistleblowing channel guarantees the confidentiality of the identity of the whistleblower, the facilitator (if any), the persons involved and in any case mentioned in the whistleblowing, as well as the content of the whistleblowing and of the relevant documentation submitted or that can be supplemented.

As a residual option, a report may also be made in writing, by ordinary or express mail or registered letter, to the attention of the Channel Management Managers at the address Via Molere n. 2, 24067 Sarnico (BG), with the wording "confidential and personal" without indication of the sender. The report in written form, in view of the confidential registration of the report by the Channel Management Manager, shall be placed in two closed envelopes, including in the first one the identification data of the reporter together with an identity document; in the second one the subject of the report; both envelopes to be placed in a third one bearing on the outside the wording "confidential to the Channel Management Manager";

7.1 Person in charge of channel management (so-called “channel manager”)

The management of the internal channel is entrusted to a person in possession of the requirements of autonomy, independence and specifically trained. The assumption of this position is formalised through a specific appointment (form Letter of Appointment for Channel Management Manager or other formal appointment established by the company's administrative body).

The person in charge of channel management and reporting acts exclusively with regard to the acquisition of the report and access to the platform.

7.2 Characteristics of the internal reporting channel

The Company's internal reporting channel is supported by an external IT platform that can be reached through the link indicated above; it is web-based and accessible from all devices (PC, Tablet, Smartphone). Data entered into the platform are segregated in the logical partition dedicated to the company and subjected to a scripting algorithm before being archived. Security in transmission is guaranteed by secure communication protocols.

At the end of the entry of the report (regardless of whether it is anonymous or not), the platform provides an **alphanumeric code** (report identification code), randomly and automatically generated by the platform,

which cannot be reproduced and with which the reporter can at any time view the processing status of his report and interact with the person responsible through a messaging tool.

The report can only be viewed and handled by authorised persons. The person responsible has unique credentials for access. The password policy adheres to international best practices. The platform sends reminders about unread or out-of-date reports to the channel manager.

Data relating to reports will be kept for no more than three years from the date of communication of the final outcome of the reporting procedure; on expiry, the platform will automatically delete the data. This is without prejudice to the possibility of defending the data controller's rights in all venues, in particular in the event of any legal proceedings.

The processing of personal data must always take into account and comply with the obligations provided for by the GDPR and Legislative Decree 196/2003 as amended. The Company, as data controller through the internal reporting channel is required to carry out a prior analysis of the organisational design including the fundamental assessment of the possible impact on data protection (Art. 35 of the GDPR).

7.3 Characteristics of the report and anonymous reports

The report must be as detailed as possible in order to allow the competent subjects responsible for receiving and handling reports to analyse the facts. In particular, the following must be clear

- the circumstances of time and place in which the fact which is the subject of the report occurred
- the description of the fact
- the personal details or other elements enabling identification of the person to whom the reported facts are to be attributed.

The information on the breaches reported must be truthful. Mere suppositions, unreliable indiscretions (so-called "rumours"), as well as news in the public domain, incorrect information (with the exception of genuine error), manifestly unfounded or misleading, or if merely damaging or offensive, shall not be considered such. On the other hand, it is not necessary for the reporter to be certain of the actual occurrence of the reported facts and the identity of the author thereof.

It is also useful for the whistleblower to provide documents providing evidence of the facts reported, as well as the names of other persons potentially aware of the facts. Anonymous reports, if circumstantiated, are equated with ordinary reports and in this case considered within the scope of this procedure, also with regard to the protection of the reporter, if subsequently identified, and to retention obligations.

7.4 Operational procedure for handling the report

1) The reporting party submits the report via the dedicated internal channel accessible through the web-based IT platform.

2) The reporting person activates the report in written mode, by filling in a guided form through the above-mentioned link, or in oral mode by using the voice recording tool on the IT platform or by requesting a meeting with the person in charge of managing the channel, through the above-mentioned platform.

- a. If the whistleblower makes the report orally by means of a meeting set up with the channel manager, the report, with the whistleblower's consent, is documented by the channel manager, through the

preparation of a report which the whistleblower can verify, rectify and/or confirm by signing it (Form Verbale segnalazione orale or other formalization method adopted by the channel manager).

b. Oral reports may also be made through the use of the voice recording tool on the IT platform used as a written reporting channel.

3) The reporting party may choose the recipients of the report by selecting one or more Channel Management Officers.

4) Receipt of the report by the Channel Manager initiates the report handling process. The Channel Manager proceeds to process it according to the predefined process flow chart described below.

5) Upon reception of the report, the platform automatically notifies the reporting party of its reception of the report by assigning a unique report code. The person in charge of managing the channel receives from the platform an automatic notification of the presence of a new report and can then access the dedicated area of the platform to take charge of it by changing the status of the report from "New" to "Open - Received", thus fulfilling the obligation to send an acknowledgement to the reporting party within 7 days of receipt of the report as required by Legislative Decree 24/2023.

6) The Channel Manager shall proceed with an initial check on the correctness of the procedure followed by the reporting person and that

a. the content of the report relates to the scope defined by this procedure (so-called inherent nature of the report content);

b. is verifiable on the basis of the information provided;

c. The channel manager verifies the inherent nature of the report and acquires all the elements.

If the report is not inherent, the Channel Manager formalises the outcome of the check, changing the status of the report on the IT platform from "Open" to "Closed" and specifying the outcome ("Resolved", "Rejected", "Cancelled", "Spam" or "Other") within a reasonable timeframe (no more than 3 months) and archives the report. The reporter can view the progress or closure status of the report by accessing, also at a later stage, the IT platform (<https://whistleblowersoftware.com/secure/Besenzoni>) through the personal credentials associated with the individual report given by the alphanumeric code generated by the system.

The person in charge, guaranteeing respect for the principle of confidentiality, shares the information with the company.

If it is necessary to obtain additional information, the Channel Manager will contact the reporter via the platform or the personal contacts provided. If the whistleblower does not provide additional information within three months of the request for supplementation, the Channel Manager will proceed with the filing of the report and notify the whistleblower accordingly. If it is necessary to transfer data outside the platform, in particular personal data of the whistleblower, the Channel Manager requests the whistleblower's explicit consent via the platform.

7) Acknowledgement to the reporting person must be given within three months of the date of receipt of the report. Only in exceptional cases, should the complexity of the report require it, or in view of the reporting party's response time, the Channel Manager, having promptly informed the reporting party before the deadline, with appropriate justification, may continue the investigation phase for as long as necessary and give the reporting party periodic updates, keeping the report in "Open" status.

The Channel Manager will assess, on a case-by-case basis, with the Company whether and which corporate function should be appropriately involved for the relevant analysis and for any consequent measures, always in compliance with the principle of confidentiality.

8) In the event of defamation or slander, ascertained with a sentence, even at first degree, the company shall proceed with disciplinary proceedings against the whistleblower.

It is specified that, from receipt of the report until its closure, any person in a situation of conflict of interest must refrain from taking decisions in order to ensure compliance with the principle of impartiality.

7.5 Transmissions of reports with wrong addressee

If the report is transmitted to a person other than the one appointed to receive it, the person receiving it is obliged to transmit it within seven days to the competent person, giving notice of the transmission to the reporting person and guaranteeing a chain of custody of the information that complies with confidentiality obligations and with those set out in paragraph 7.2. The Company adopts disciplinary sanctions in case of non-compliance with the transmission obligation.

In the case of unintentional transmission of the report to a person other than the person authorised to receive it, the person making the report must prove mere negligence and the absence of a personal interest in the erroneous transmission.

7.6 Retention of internal reporting documentation

Internal reports and all related attached or supplemented documentation shall be kept, by means of an appropriate digital chain of custody, for the time necessary for the processing of the report itself.

In any case, the documentation is only retained for a time period of a maximum of three years from the date of communication of the final outcome of the reporting procedure.

In all the above cases, the procedure for retaining internal reports and related documentation must comply with EU and national guarantees on the processing of personal data as well as with the measures on confidentiality.

7.7 Information obligations

Information on the channel, procedures and prerequisites for making reports shall be made available to the company's personnel through the company's normal information channels and made known to persons who,

although not frequenting the workplace, have a legal relationship with the company through publication on the company's website.

7.8 Special cases

If the internal report containing serious, precise and concordant elements concerns one of the Channel Management Managers, the reporter in the guided form of the reporting platform may exclude from the recipients the Channel Management Manager indicated as the subject of the offence, sending the report to the other Channel Management Manager in charge and not involved in the report itself.

If the internal report containing serious, precise and concordant elements concerns all the Channel Management Managers, or if the latter are in any case subjects involved or affected by the report or are themselves the reporting subject, the report must be forwarded to the administrative body by hand delivery to the Legal Representative of any supporting documentation or by registered letter with return receipt or express courier addressed to the Company's registered office in Via Molere no. 2, 24067 Sarnico (BG), with the following wording: "Confidential Personnel for the attention of the Legal Representative".

The administrative body, after assessing whether the internal report is accompanied by the necessary information to preliminarily verify its grounds and to be able to start the subsequent in-depth investigations, follows up the report by carrying out the preliminary investigation also by availing itself of the company's expertise and, where appropriate, of specialised consultants, always in compliance with the confidentiality of the relevant legislation and with the provisions contained in this document.

The preliminary investigation follows the procedure described in this procedure.

The decision of the administrative body is formalised by means of a written resolution.

8. EXTERNAL REPORT

If the following conditions are met, the whistleblower may proceed with a report to ANAC through an external channel

- where, in the reference work context, activation of the internal reporting channel is not mandatory or the channel itself has not been activated or does not comply with the regulatory requirements
- where the whistleblower has already submitted an internal report even though it has not been followed up;
- if the whistleblower has justified reasons to believe that by filing an internal report, the report will not be effectively followed up or that the report, in itself, will lead to retaliation against the whistleblower;
- if the report is addressed to the entire administrative body of the company;

- if the whistleblower has a well-founded reason to believe that the reported breach may constitute an imminent or obvious danger for the public interest.

The external body authorised to receive external reports is ANAC in accordance with the appropriately adopted modalities and procedures (<https://www.anticorruzione.it/-/whistleblowing>).

9. PUBLIC DISCLOSURE

On a residual and subordinate basis, the whistleblower may proceed with a public disclosure in the following cases

- when he has already previously made an internal or external report, or has directly made an external report without having received a reply within the prescribed time limit;
- where he has justified reason to believe that the breach constitutes an imminent or obvious danger to the public interest;
- where it has well-founded reasons to believe that the external report carries the risk of retaliation or may not be effectively followed up because of the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient may be colluding with the perpetrator or may be involved in the violation.

10. OBLIGATION OF CONFIDENTIALITY

All reports and their attachments shall not be used beyond the time necessary to follow up on them. It is envisaged that the identity of the reporter together with any other information from which such identity may be inferred, directly or indirectly, shall not be disclosed without the express consent of the reporter to persons other than those competent to receive or follow up on the reports, who are expressly authorized to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2-quaterdecies of the Code on the Protection of Personal Data referred to in Legislative Decree No. 196 of June 30, 2003. The Company shall protect the identity of the persons involved, the facilitators and the persons mentioned in the report until the conclusion of the proceedings initiated due to the report itself, in compliance with the same guarantees provided in favor of the reporting person.

Mitigating circumstances for the protection of the right to confidentiality include:

- within the framework of criminal proceedings, the identity of the reporter is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure: the obligation of secrecy of the acts of the preliminary investigation is required until the suspect has the right to have knowledge of them and, in any case, no later than the closure of that stage
- within the framework of the proceedings established at the Court of Accounts, the identity of the reporter may not be revealed until the closure of the investigative stage;
- within the framework of the disciplinary procedure, the identity of the reporter cannot be revealed where the accusation of the disciplinary charge is based on investigations separate and additional to the report, even if consequent to it;

- where the charge is based, in whole or in part, on the report and the knowledge of the identity of the reporting person is indispensable for the defense of the accused, the report will be usable for the purposes of disciplinary proceedings only if there is the express consent of the reporting person to reveal his or her identity;
- in cases of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, written notice will be given to the reporter of the reasons for the disclosure of confidential data when the disclosure will also be indispensable for the defense of the person involved.

Given the force of the mitigations just listed, the affected person, upon his or her request, is also heard through a cartular procedure by obtaining written observations and documents.

Confidentiality obligations include:

- the subtraction of the report and the documentation attached to it from the right of access to administrative acts provided for in Articles 22 et seq. of Law No. 241/1990 and from the generalized civic access provided for in Articles 5 et seq. of Legislative Decree No. 33/2013;
- the administrations and entities involved in the management of reports guarantee confidentiality during all stages of the reporting process, including the possible transfer of reports to other competent authorities.

11. PROTECTION OF PERSONAL DATA

All processing of personal data, including communication between competent authorities, is carried out in accordance with:

- the Regulation (EU) 2016/679;
- the D. Lgs. 30 June 2003, no. 196, as amended.

The communication of personal data by institutions, bodies or organs of the European Union is carried out in accordance with Regulation (EU) 2018/1725.

The processing of personal data relating to the receipt and management of reports is carried out by the owner, in accordance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, by first providing the appropriate information to the reporting subjects and the persons involved as well as taking appropriate measures to protect the rights and freedoms of the data subjects.

The informative notice to the data subjects, also summarizing their rights and the ways to exercise them, is made available, with the obligation of acknowledgement, within the reporting channel and possibly supplemented through specific documents prepared by the company.

In the event of the need to disclose the identity of the reporting party to parties other than those responsible for receiving and handling the report, in compliance with the provisions of Legislative Decree 24/2023, the reporting party will be asked for express and specific consent.

12. PROTECTION AND SUPPORT MEASURES

Appropriate measures are prescribed to protect whistleblowers from direct retaliation and indirect retaliation. Protective measures apply if, at the time of reporting, the reporting person had reasonable grounds to believe that the information about the reported violations was true (see Section 7.3), fell within the objective scope, and the reporting procedure was followed.

In the case of defamation or slander, established by conviction even in the first instance, protections are not guaranteed.

The protective measures also apply:

- (a) to facilitators;
- (b) to persons in the same work environment as the reporting/whistleblowing person who are related to them by a stable emotional or kinship relationship within the fourth degree;
- (c) to co-workers of the reporting/denouncing person who work in the same work environment as the reporting/denouncing person and who have a regular and current relationship with that person;
- (d) to organizations owned by the reporting/whistleblower person or for which the same persons work, as well as to organizations operating in the same work environment as the aforementioned persons.

12.1 Prohibition of retaliation

Those enumerated in Paragraph 5 cannot be subjected to any retaliation. For informational and non-exhaustive purposes, "retaliation" is considered to be:

- firing, suspension or equivalent measures;
- demotion in rank or non-promotion;
- the change of duties;
- change of place of work;
- the reduction of salary;
- the modification of working hours;
- suspension of training or any restriction of access to training;
- negative merit notes or negative references that are not adequately substantiated;
- the adoption of disciplinary measures or other sanctions (including fines);
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination or otherwise unjustified unfavorable treatment;
- failure to convert a fixed-term employment contract to a permanent employment contract where the employee had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damages, including to a person's reputation, particularly on social media,
- economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion on improper lists on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the cancellation of a license or permit;
- the request for submission to psychiatric or medical examinations.

Acts taken in violation of the prohibition against retaliation are null and void.

In the context of judicial or administrative proceedings or in the case of extrajudicial disputes concerning the ascertainment of the prohibited conduct, acts or omissions with respect to the reporting persons only, it is presumed that the same have been put in place because of the reporting. The burden of proving that such conduct or acts are motivated by reasons unrelated to the reporting is on the person who carried out the retaliatory acts.

Whistleblowers may inform ANAC of the retaliation they believe they have experienced, whether attempted or contemplated.

The ANAC shall inform the National Labor Inspectorate for measures within its jurisdiction.

12.2 Support measures

The reporter may turn to Third Sector organizations on the list published on the ANAC website. These are entities that carry out activities in the general interest for the non-profit pursuit of civic, solidarity and socially useful purposes ("promotion of the culture of legality, peace among peoples, nonviolence and unarmed defense; promotion and protection of human, civil, social and political rights, as well as the rights of consumers and users of general interest activities, promotion of equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing groups") and that have entered into agreements with ANAC. The support measures provided 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.

12.3 Limitation of the whistleblower's responsibility

No liability (including civil or administrative liability) is provided for those who disclose or disseminate information about violations

- covered by the obligation of secrecy,
- relating to the protection of copyright,
- of provisions relating to the protection of personal data,
- offending the reputation of the person involved or reported,

whether, at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the violation and the reporting was made consistent with the conditions for protection.

In addition, among the protection measures:

- the rights to make a report and the related protections cannot be restricted in a contractual manner;
- all other liability is excluded, including civil and administrative liability, for acquiring or accessing information on violations, except where the conduct constitutes a crime;
- any other liability is excluded, with regard to conduct, acts, omissions made if related to the report and strictly necessary to reveal the violation or, in any case, not related to the report.

13. PENALTY REGIME

The system of sanctions adopted by the Company against those whom the organization ascertains to be responsible for the offenses referred to:

- commission of retaliation or proposed adoption, obstruction of reporting (including attempted) or violation of confidentiality obligations,
- failure to establish reporting channels, failure to adopt procedures for handling them, or procedures that do not comply with the requirements of the decree or failure to carry out verification and analysis of reports,
- civil liability of the reporting person for defamation or slander in cases of wilful misconduct or gross negligence, unless the person has already been convicted, also at first degree, for the crimes of defamation or slander,
- violation of this procedure,

shall be applied according to in the mandatory regulations, the provisions of CCNL, and, where present, the internal regulations.

14. ATTACHMENTS

Letter of appointment for channel management manager
Oral report minutes