Whistleblowing Procedure

CONTENTS

1. Objective

This procedure has been adopted by the company in compliance with that established by Italian Legislative Decree no. 24 of 10 March 2023 (referred to in the text as: The Decree or Italian Legislative Decree no. 24/2023) in force since 30 March 2023, which implements Directive (EU) 2019/1937 of the European Parliament and of the Council dated 23 October 2019 concerning the protection of persons who report breaches of national or European Union law (known as the Whistleblowing directive) of which they have become aware within their work-related context, that are detrimental to public interest, or to the integrity of public administration or private enterprises.
This procedure was approved by the Board of Directors on 18/12/2023, together with the identification of the organisational roles involved in the management of whistleblowing reports and the related responsibility.

The document in question is applicable to all of the companies within the Euricom Group: Euricom S.p.A., Curti S.r.l., Molini Certosa S.r.l., Coriso S.r.l. and Pigino S.r.l. (hereinafter also referred to as the "Company").

For the purposes of application, it is hereby stressed that for companies implementing models pursuant to Italian Legislative Decree 231/01 and with fewer than 50 employees, the internal reporting channel (paragraph 8), can only be used to report breaches pursuant to Italian Legislative Decree no. 231/2001 or breaches of the Organisation and management model adopted by the Company.

2. Field of application

This procedure is applicable to any report providing information on behaviour, actions or omissions (i.e., breaches) detrimental to public interest or to the integrity of public administration or private entities, and that consists or consist in:

- offences pursuant to Italian Legislative Decree no. 231/2001 or breaches of the Organisation and management model adopted by the Company.
- offences that fall under the scope of application of relevant national or UE laws related to[1]:
    A. public procurement (award and appeal procedures).
    B. financial services, products and markets, and prevention of money laundering (regulations regarding governance and oversight regulations, as well as consumer and investor protection).
    C. product safety and compliance (regulations on safety and compliance requirements, on the commercialisation and use of delicate and hazardous products, so-called military goods).
    D. transport safety (railway, civil aviation, road and maritime sectors, the internal transportation of hazardous goods by road/rail/internal waterways, both within the nation state and between states within the European Community).
    E. protection of the environment and the climate (marine, atmospheric and acoustic pollution, waste management, soil water, biodiversity, chemical substances, biological products).
    F. nuclear safety (systems, radiation exposure, management of nuclear fuel and radioactive waste, shipping of radioactive substances).
    G. food and feed safety, animal health and welfare.
    H. public health (quality and safety regulations regarding human tissues and cells, human blood and its components, organs for transplantation, medicinal products and medical devices, patient rights regarding cross-border healthcare, the processing and sale of tobacco products).

[1] Reference is made to the annexes of Directive (EU) 2019/1937 and Italian Legislative Decree 24/23.

I. consumer protection (product quality and safety, information and advertising, contractual relations, commercial practices).
J. protection of privacy and personal data, and security of network and information systems.

- breaches (acts or omissions) affecting the financial interests of the EU (ref. art. 325 of the Treaty on the functioning of the European Union).
- breaches (acts or omissions) of regulations regarding competition and State aid (ref. art. 26, paragraph 2 of the Treaty on the functioning of the European Union).
- breaches (acts or omissions) of regulations regarding corporate tax.

The area of application of this procedure does not cover:

- disputes, claims or requests regarding matters of a personal character that refer exclusively to individual working relationships or to working relationships with one's superiors.
- breaches regarding national security, as well as contracting relating to national defence or security.
- breaches that are obligatorily governed by European Union laws or by national laws[2] that already provide for specific reporting procedures.

Information regarding breaches is acquired from within the work-related context and must be communicated via the dedicated reporting channels provided by the Company.

3. References

- Italian Legislative Decree no. 24 of 10 March 2023.
- Directive (EU) 2019/1937.
- Organisation, management and monitoring model pursuant to Italian Legislative Decree 231/01.
- Regulation (EU) 2016/679 (GDPR).
- Privacy Code (Italian Legislative Decree no. 196/2003 as amended).
- ANAC Guidelines regarding the protection of persons who report breaches of Union law and the protection of persons who report breaches of national laws - procedures for the submission and handling of external reports.

4. Definitions

- "**Reports**": any communication written, oral or made in conversation, also in anonymous form, containing information on breaches.
- "**Information on breaches**": all the information, including well-founded suspicions, regarding breaches committed or that, on the basis of tangible elements, may be committed within the organisation with which the reporting party or person making a report to judicial/administrative authorities has a legal relationship. as well as informative elements regarding conduct aimed at obscuring said breaches.
- "**Internal report**": communication of the "reports" via the dedicated internal report channel.
- "**External report**": written or oral communication of information regarding breaches, presented via the external reporting channel.
- "**Public disclosure**": the publicising of information regarding breaches, via the press or electronic media or in any case via publication methods that can reach a large number of people.
- "**Reporting party**": a natural person who reports or publicly discloses information regarding the breaches acquired within the context of their work-related context.

[2] Reference is made to the annexes of Directive (EU) 2019/1937 and Italian Legislative Decree 24/23.

- "**Facilitator**": a natural person who assists the reporting party during the reporting process, who operates within the same work-related context and whose assistance must be kept confidential.
- "**Work-related context**": past or present working or professional activities through which, irrespective of the nature of said activities, a person acquires information on the breaches, and within which said person may risk retaliation in the event of public reporting or disclosure or reporting to judicial or accounting authorities.
- "**Person involved**": a natural person or legal entity named in the report as being suspected of committing the breach or as a person in any way implicated in the breach reported.
- "**Channel manager**": an external subject identified by the Company as responsible for the management of the channel and the report, vested with organisational and functional autonomy.
- "**Internal contact**": a subject within the Company identified by the executive body. In the event that the Internal contact is the person involved in the report, the role of Internal contact will be covered by the Chairperson of the Board of Statutory Auditors or the Sole auditor of the relative Company, in the person of:
  - Mr. **Marco Taglioretti**, Chairman of the Board of Statutory Auditors for Euricom S.p.A.
  - Mr. **Daniele Fossati**, Sole auditor of Curti S.r.l.
  - Mr. **Marco Trotter**, Chairman of the Board of Statutory Auditors of Molini Certosa S.p.A.

  For reports regarding Coriso S.r.l. and Pigino S.r.l., the role of Internal contact will be covered by the Chairperson of the Board of Statutory Auditors of Euricom S.p.A.
- "**Retaliation**": any conduct, act or failure to act, even if only attempted or threatened, carried out as a result of an internal report and strictly related to the same, of a report to law enforcement or accounting authorities or public disclosure and which causes or may cause unjust damage, directly or indirectly, to the Reporting party or person making the report.
- "**Follow up**": the action or actions carried out by the subject appointed with the management of the reporting channel.
- "**Feedback**": communication to the Reporting party of information regarding the follow up or intended follow up to the report, including the measures provided for or adopted or to be adopted, and the reasons for the choice made.
- "**Platform**": the internal reporting channel adopted by the Company (as described in further detain in paragraph 8) to send information on breaches.
- **"Supervisory Board" ("SB"):** Supervisory board pursuant to Italian Legislative Decree no. 231/2001 appointed by the Company.
- **"Model 231":** Organisation, management and monitoring model pursuant to Italian Legislative Decree no. 231/2001 appointed by the Company.

5. Responsibility

The channel manager, also through the use of the platform:

- provides clear information regarding the channel, procedures and conditions for making internal reports, also through this procedure and the information published on the platform.
- provides the reporting party with feedback regarding the receipt of the report within the established terms.
- assesses the criteria for the suitability for processing of the report.
- communicates the report to the internal contact, defined as part of this procedure, and informs the SB (in the relative cases), of any enquiries, their outcome and the feedback to provide to the reporting party.

- provides the reporting party with feedback regarding the conclusion of the process of report management.
- maintains communications with the reporting party and, if necessary, manages requests for integration and the carrying out of any interviews for further information with the reporting party, if required.
- archives and conserves documentation regarding the report for the periods of time normally provided for.
- guarantees respect for the principles of confidentiality.

The internal contact:

- identifies, within the context of the Company, the subjects to involve, and communicates to said subjects the results of the analysis carried out by the channel manager.
- is appointed with the task of providing the channel manager feedback regarding the decisions taken by the Company in terms of the content of the report.
- implements the recommendations made by the channel manager to further examine the content of the report.
- coordinates and monitors the stages of any enquiries with the internal functions/external teams appointed.
- informs the channel manager of the commencement of any enquiries, their outcome and the feedback to provide to the reporting party.
- identifies programmes for improvement aimed at avoiding the recurrence of the events contained in the report.
- ensures that all the information required regarding the channel, the procedures and the conditions for making internal reports is available via company channels.
- manages the activities resulting from public disclosure in relative cases with the support of the responsible company functions.
- guarantees respect for the principles of confidentiality.

The reporting party:

- sends the report in compliance with this procedure.
- is required to provide substantiated information regarding the contents of the report.

The SB:

- in the event of reports pursuant to Italian Legislative Decree 231/01, coordinates and monitors the various stages of the enquiry with the appointed internal functions/external teams, assessing the outcome of the enquiry and any resulting measures.
- guarantees respect for the principles of confidentiality.

The legal representative:

- communicates with the National Anti-Corruption Authority in the event of external reports or the carrying out of inspections by the National Anti-Corruption Authority.

The Board of directors:

- ensures that any measures are implemented in compliance with the system of sanctions provided for by the 231 Organisational model.
- approves this procedure together with the structure of the relative organisational roles.
- guarantees respect for measures aimed at protecting the reporting party.

6. Subjects authorised to make a report (known as the "reporting party")

Reports can be made by:

- employees.
- autonomous workers and collaborators who carry out their professional activities for public and private subjects.
- self-employed professionals.
- volunteers.
- consultants.
- shareholders.
- directors.
- suppliers of services to third parties in any form (regardless of the nature of said activities), also in absence of consideration.
- apprentices whether paid or unpaid.
- subjects carrying out administrative, executive, supervisory, monitoring or representative functions, even if the relative activities are carried on the grounds of fact and not of law.

This category also includes all those subjects who, for whatever reason, become aware of breaches within the company's work-related context, i.e.:

- when an employment relationship has not yet begun.
- during a trial period.
- upon termination of the relationship.

7. Internal contact:

The Company has appointed Mr. Mario Francese as the internal contact pursuant to this procedure.

8. Internal reporting channel

The Company has set up an internal reporting channel which reporting parties must use to send reports related to breaches. The setting up of said channel allows for more efficient prevention and identification of violations. This measure is in line with the principle of favouring a culture of good communication and corporate social responsibility, as well as improvement of the company organisation.

The internal reporting channel allows for written or oral reporting via the "@Whistleblowing" channel accessible respectively via the following links:

- **https://digitalroom.bdo.it/euricom** for Euricom S.p.A.
- **https://digitalroom.bdo.it/coriso** for Coriso S.r.l.
- **https://digitalroom.bdo.it/pigino** for Pigino S.r.l.
- **https://digitalroom.bdo.it/curti** for Curti S.r.l.
- **https://digitalroom.bdo.it/molinicertosa** for Molini Certosa S.r.l.

On accessing the platform, a voice-message recording system also allows the reporting party to request an in-person meeting with the report manager.

The internal reporting channel guarantees the confidentiality of the identity of the reporting party, the facilitator (where present), the persons involved and, in any case, mentioned in the report, as well as the content of the same and the relative documentation provided or suitable for integration.

8.1 Subject responsible for the management of the channel (the so-called "channel manager")

The management of the internal channel has been assigned to:

- **BDO Advisory Services S.r.l., represented by Renato Marro,** an external subject having the requirements of impartiality, independence and specific training.

The channel and report manager acts independently with regards to the acquisition of the report and access to the platform, except for cases in which the report contains information relative to the activities carried out by the auditing company "BDO Italia S.p.A." or relative to matters of an accounting nature. In these circumstances, the management of the internal channel will be entrusted to the "Chairperson of the Board of Statutory Auditors or the Sole Auditor" of the relative Company, in the person of:

- Mr. **Marco Taglioretti**, Chairman of the Board of Statutory Auditors for Euricom S.p.A.
- Mr. **Daniele Fossati**, Sole auditor of Curti S.r.l.
- Mr. **Marco Trotter**, Chairman of the Board of Statutory Auditors of Molini Certosa S.p.A.

For reports regarding of an accounting nature related to Pigino S.r.l., the role of Internal contact will be covered by the Chairperson of the Board of Statutory Auditors of Euricom S.p.A.

8.2 Characteristics of the internal reporting channel

The Company's internal reporting channel is managed by the web-based "Whistleblowing" platform, which can be accessed from all devices (PC, tablet, smartphone).
The data entered on the platform are held in the logic partition dedicated to the Company and subject to a scripting algorithm before storage. Security during transportation is guaranteed by secure communication protocols.
Once the report has been entered, the digital platform issues a randomly and automatically generated 12-character alphanumeric code (for both anonymous and non-anonymous reports) that cannot be reproduced, that the reporting party can use at any time to see the status of their report and interact with the manager via a messaging application.
In the event of non-anonymous reports, the data of the reporting party ("user data") cannot be accessed by the channel manager. At their discretion, the channel manager may view the relative fields (the so-called "non-encrypted fields") only after providing justification, which is appropriately traceable, within the platform.
The report can be viewed and managed exclusively by the channel manager. The manager has unique access credentials that expire every 3 months. The password policy is in line with international best practices.
Data retention is governed by pre-defined expiry dates with automatic reminders sent to the channel manager, who will, on expiry, proceed with erasure of the data.
The company BDO, which provides the platform access services, has ISO 27001 certification.
The processing of personal data must always take into account and comply with the obligations set out by the GDPR and by Italian Legislative Decree no. 196/2003 as amended. The company, in its role as data controller for the internal reporting channel, is required to carry out prior analysis of the relative organisational plan, including a fundamental assessment of any possible impact on the protection of data (art. 35 of the GDPR).

8.3 Characteristics of reports and anonymous reports

It is necessary for reports to be as substantiated as possible in order to allow an analysis of the events by the subjects responsible for receiving and managing said reports. In particular, it is necessary that clear information is provided regarding:

- the time and the place in which the reported events took place.
- the description of the events.

- general information or other elements that allow the identification of the subjects to which the events reported are to be attributed.

Information on reported breaches must be truthful. Simple supposition, unreliable rumours, news in the public domain, incorrect information (with the exception of honest errors), information that is clearly unfounded or misleading, or simply harmful or offensive, will not be taken into consideration. It is not, however, necessary for the reporting party to be certain of the effective occurrence of the events reported or of the identity of the person responsible for the same.

It is also opportune for the reporting party to provide documentation that may service as evidence to support the subjects reported, as well as the indication of any other subject who are aware of the events.

Anonymous reports, where substantiated, are treated in the same manner as standard reports and as so are considered in line with this procedure, also with regards to protection for the reporting party, in the event of their subsequent identification, and to requirements concerning conservation.

8.4 Whistleblowing management procedure

The whistleblower transmits their report via the dedicated internal channel.

The whistleblower activates the report via the link indicated above in writing, by filling in a special written or oral form. Using the platform, the whistleblower can make a request to have a meeting with the channel manager.

If the whistleblower makes the report orally in a meeting with the channel manager, with the consent of the whistleblower, the same is documented by the channel manager by recording on a suitable storage device that is capable of vocal reproduction or by drafting a report. In the latter case, the whistleblower can verify, rectify and/or confirm the report of the meeting by signing the same.

Receipt of the report by the channel manager starts the whistleblower management process. The channel manager starts to "process" it using a predefined process flow chart.

Once the report has been received, the manager will provide the whistleblower with an acknowledgment receipt within 7 days of receiving and taking charge of the report.

The manager in charge of managing the report proceeds with an initial verification of the correctness of the procedure followed by the whistleblower and the contents of the report both in terms of the scope of application defined by this procedure (so-called relevance of the contents of the report) and its verifiability based on the information provided. In this phase, if the channel manager deems it necessary (e.g., in the event of any doubts), they can involve the Supervisory Body to evaluate the relevance of the report pursuant to Italian Legislative Decree no. 231/01. If the report is not relevant, the channel manager formalises the outcome of the check and communicates it to the whistleblower within a reasonable time (no longer than 3 months) and archives the report. The manager will promptly inform the internal contact, guaranteeing compliance with the principle of confidentiality, who will share the report with the company.

If it is necessary to acquire additional elements, the channel manager will contact the whistleblower using the platform. If the whistleblower does not provide additional information within 3 months from the request for integration, the channel manager will proceed with archiving the report, communicating this to the whistleblower and informing the internal contact.

Having checked the relevance of the report and acquired all the elements the channel manager, in compliance with the principle of confidentiality, will inform the internal contact, and if it involves information on significant violations pursuant to Italian Legislative Decree no. 231/01, the Supervisory Body, to evaluate how to start the investigation phase, without prejudice to compliance with the principle of autonomy and independence of the S.B. in terms of the way in which the report is managed pursuant to Italian Legislative Decree no. 231/01.

At the end of the investigation the internal contact will prepare a final report and will share the findings with the channel manager to provide feedback to the whistleblower. Feedback must be sent to the whistleblower within three months from the date of acknowledgment of receipt that is before the expiry of the deadline of seven days from submitting the report. Only in exceptional circumstances, if the complexity of the report requires it, or taking into account response times of the whistleblower, after having informed the whistleblower the channel manager will be able to continue the investigation phase for the necessary time and give the whistleblower periodic updates.

In the event of significant violations pursuant to Italian Legislative Decree no. 231/01, the internal contact will inform the Supervisory Body about the results of the investigation. The S.B., within its operational autonomy, will evaluate the results received and if the report is credible, any consequent measures and evaluate the possibility to adopt any measures deemed necessary for the purposes of adapting the Model providing the necessary communications to apply any penalties. Any consequent measures are applied in compliance with the provisions of the sanction regime provided for in the Organisation, Management and Control Model 231.

For reports that are not included in the scope of the violations pursuant to Italian Legislative Decree no. 231/01, the internal contact, will evaluate case by case with the company whether and which corporate function should be appropriately involved in the relative analysis and any consequent measures in compliance with the principle of confidentiality.

In the event of defamation or slander, confirmed with a first instance judgement, the company will proceed with sanctioning proceedings against the whistleblower.

It is specified that, from receipt of the report until its closure, any subject that finds themselves in a conflict of interest must refrain from making decisions in order to guarantee compliance with the principle of impartiality.

8.5 Transmission of reports to the wrong recipient

If the report is sent to a person other than the one responsible for receiving it, the person who receives it is obliged to send it to the competent person within seven days informing the whistleblower and ensuring a chain of custody of information that complies with confidentiality obligations and those outlined in paragraph 8.2. The company will adopt disciplinary sanctions in case of failure to comply with the transmission obligation.

In the event of involuntary transmission of the report to a person other than the one authorised to receive it the whistleblower must demonstrate mere negligence and the absence of a personal interest in the erroneous transmission.

8.6 Keeping internal report documentation

Internal reports and all related attached documentation must be stored with an appropriate digital chain of custody for the time necessary to process the report.

In any case the documentation is kept for a time period identified as a maximum of five years starting from the date of communication of the final outcome of the reporting procedure.

In all cases mentioned, it is necessary that the procedure for storing internal reports and the relative documentation complies with European community and national regulations on processing personal data as well as existing measures on the right to confidentiality.

8.7 Information obligations

Information on channels, procedures and conditions for reporting are displayed in paper form in the workplace in the reception and in electronic form in the appropriate company intranet section and communicated to people who despite not being present on company premises, have a legal relationship with the company.

Furthermore, this information is published on the company website:

- **https://www.euricom.it in the area "ABOUT US"** for Euricom S.p.A.
- **https://www.euricom.it in the area "GROUP ORGANIZATION/Companies"** for Coriso S.r.l. and Pigino S.r.l.
- **https://www.curtiriso.it/azienda/** for Curti S.r.l.
- **https://www.molinicertosa.it/** for Molini Certosa

The company has implemented their own internal reporting channel after consulting trade union representatives.

9. External reports

If the following conditions are met the whistleblower can send a report to ANAC via external channels:

- in the event it is not mandatory to use the internal reporting channel for the working environment in question, i.e., the channel has not been implemented or does not comply with regulatory requirements;
- when the whistleblower has already sent an internal report even though it was not followed up;
- if the whistleblower has a credible reason to believe that by sending an internal report the same will not be given an effective follow-up or will lead to retaliation against them;
- in the event the whistleblower has a credible reason to believe that the violation reported could constitute an imminent or obvious danger to the public interest.
- The external body authorised to receive external reports is ANAC according to the methods and procedures appropriately adopted (www.anticorruzione.it).

10. Public disclosure

As a residual and less favoured alternative the whistleblower can proceed with a public disclosure in the following cases:

- when an internal or external report has been sent, or an external report has been sent directly without having received feedback by the expected deadlines;
- in the event they have a credible reason to believe that the violation reported could constitute an imminent or obvious danger to the public interest;

- when they have a credible reason to believe that the external report could involve a risk of retaliation or it may not be effectively followed up due to the specific circumstances of the case, such as those in which evidence may be hidden or destroyed or where there is a well-founded fear that the person receiving the report may have colluded with the perpetrator of the violation or been involved in the violation itself.

11. Confidentiality obligations

All reports and relative attachments are not used beyond the time necessary to follow them up.

It is expected that the identity of the whistleblower together with any information from which the same can be deduced, directly or indirectly is not to be revealed without the express consent of the whistleblower to persons other than those competent to receive or follow up on reports, expressly authorised to process such data pursuant to articles 29 and 32, paragraph 4 of Regulation (EU) 2016/679 and article 2-quaterdecies of the Italian Personal Data Protection Code, Italian Legislative Decree no. 196 of 30 June 2003.

The company will protect the identity of the people involved, the facilitators and the people mentioned in the report until the conclusion of the proceedings initiated due to the report, in compliance with the same guarantees provided in favour of the whistleblower.

The circumstances mitigating the protection of the right to privacy include:

- in the context of criminal proceedings, the identity of the whistleblower is covered by secrecy in the ways and within the limits established by article 329 of the Italian Code of Criminal Procedure: the obligation of secrecy of the preliminary investigation documents is imposed until the suspect has the right to know about it and, in any case, no later than the closure of this phase;
- in proceedings before the Court of Auditors the identity of the whistleblower cannot be revealed until the conclusion of the preliminary investigation phase;
- in disciplinary proceedings, the identity of the whistleblower cannot be revealed where the disciplinary charge is based on investigations that are distinct and additional to the report, even if consequent thereto;
- if the dispute is based, in whole or in part, on the report and knowledge of the identity of the whistleblower is indispensable for the defence of the accused, the report can be used for the purposes of disciplinary proceedings only with the express consent of the whistleblower to reveal their identity;
- in the event of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, the whistleblower will be informed in writing of the reasons for disclosing confidential information when disclosure is indispensable to defend the person involved.

Given the validity of the mitigations listed above, the person involved, at their request will also be heard through a paperwork procedure with written observations and documents.

Confidentiality obligations include:

- removing the report and the documentation attached to from the right of access to administrative documents provided for in articles 22 et. seq. of Law no. 241/1990 and generalised civic access referred to article 5 et. seq. of Italian Legislative Decree no. 33/2013;

- administrations and entities involved in managing reports will guarantee confidentiality during all phases of the report procedure, including the possible transfer of reports to other competent authorities.

12. Protection of personal data

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

- Regulation (EU) 2016/679;
- Italian Legislative Decree no. 196 of 30 June 2003, et. seq.

Disclosure of personal data by institutions, bodies or entities of the European Union is carried out in compliance with Regulation (EU) 2018/1725.

Processing of personal data relating to receiving and managing reports is carried out by the data controller, in compliance with the principles provided for in articles 5 and 25 of the Regulation (EU) 2016/679, by providing the appropriate information to the reporting parties and other people involved in advance, as well as by adopting appropriate measures to protect the freedom and rights of the interested parties.

The data controller is the company the report applies to. Each company has appointed BDO Advisory Services S.r.l. as their data processor, pursuant to article 28 of Regulation (EU) 2016/679. Any other subjects involved in receiving and managing reports will be duly authorised for processing.

To protect personal data a DPIA has been created pursuant to article 13, paragraph 6 of Italian Legislative Decree no. 24 of 2023 which states: "The subjects referred to in article 4 define their own model for receiving and managing internal reports, by identifying technical and organisational measures suitable to guarantee a level of safety appropriate to the specific risks deriving from the processing carried out, based on a data protection impact assessment, and by regulating the relationship with any external suppliers who process personal data on their behalf pursuant to article 28 of Regulation (EU) 2016/679 or article 18 of Italian Legislative Decree no. 51 of 2018".

Personal data relating to the reports is kept and stored for the period of time strictly necessary to manage the reports in all their phases (submission and managing the reports), the adoption of consequent measures and the fulfilment of related legal obligations, and in any case no longer than five years starting from the date of communication of the outcome of the report management process.

Processing in the field of whistleblowing was implemented in the register of processing activities.

The privacy policy, also summarising rights and how to exercise them can be found directly on the platform.

13. Protection and support measures

Appropriate measures are in place to protect whistleblowers from direct or indirect retaliation.

Protection measures will apply if at the time of the report the whistleblower has reasonable grounds to believe that the information about the reported violations is true (see. paragraph 8.3), falls within the objective scope and the reporting procedure was complied with.

In the event of defamation or slander, confirmed with a first instance judgement, protection measures are guaranteed.

Protection measures will also apply:

a) to facilitators;

b) to people in the same working environment as the whistleblower/complainant who are linked to them by a stable emotional bond or a degree of kinship up to the fourth degree;

c) to work colleagues of the whistleblower/complainant who work in the same working environment and who have a habitual and current relationship with that person;

d) to entities owned by the whistleblower/complainant or which the same people work for, as well as to entities that operate in the same working environment as the aforementioned people.

13.1 Prohibition of retaliation

People listed in 5 cannot suffer any retaliation. For example, but not limited to, "retaliation" is considered as:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties;
- change of location of place of work;
- reduction in wages;
- change in working hours;
- withholding of training or any form of restricted access to the same;
- an unjustified negative performance assessment or employment reference;
- the adoption of any disciplinary measures, or other penalties (including financial penalties);
- coercion;
- intimidation;
- harassment;
- ostracism;
- discrimination, or unjustified disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that they would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly on social media,
- financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

Actions taken in violation of the prohibition on retaliation are void.

In the context of judicial or administrative proceedings or in the event of out-of-court disputes concerning the verification of conduct, prohibited acts or omissions towards whistleblowers, it is assumed that the same were instigated due to the report. The burden of proving that such conduct or acts are motivated by reasons unrelated to the report is the responsibility of the person who carried out the retaliatory acts.

Whistleblowers can communicate any attempted or threatened retaliation they believe they have suffered to ANAC.

ANAC will inform the National Labor Inspectorate, for the measures within its jurisdiction.

13.2 Measures of support

Whistleblowers can contact third sector entities listed on the ANAC website. These are non-profit entities that carry out activities of general interest for the pursuit of civic, solidarity and social utility purposes ("promoting a culture of legality, peace between peoples, of non-violence and unarmed defence; promoting and protecting human, civil, social and political rights, as well as consumer rights and the rights of users of services of general interest, promoting equal opportunities and mutual aid initiatives, including time banks and solidarity purchasing groups") that have drawn up agreements with ANAC.

Measures of support provided consist of information, assistance and consultancy provided free of charge on reporting methods and on protection from retaliation provided by national regulatory provisions and those of the European Union, on the rights of those involved, as well as on the methods and conditions of access to legal aid at the state expense.

13.3 Limitation of liability of whistle-blowers

Absence of liability is expected (also of a civil or administrative nature) for anyone who reveals or disseminates information about violations:

- covered by the obligation of professional secrecy,
- relating to the protection of copyright,
- relating to protecting privacy and data protection regulations,
- that offend the reputation of the person involved or reported,

if at the time of revelation or diffusion, there were reasonable grounds to believe that disclosure or dissemination of the same information was necessary to disclose the violation and the report was submitted in accordance with the protection conditions.

Furthermore, among the protection measures the following is pointed out:

- the right to make a report and the relative protection cannot be contractually limited;
- the exclusion of any other liability, including civil and administrative, for obtaining or accessing information on violations, except in the case in which the conduct constitutes a crime;
- the exclusion of any other responsibility with regard to conduct, actions or omissions carried out if connected to the report and strictly necessary to reveal the violation or, in any case, not connected to the report.

14. Penalty regime

The disciplinary system adopted by the company pursuant to article 6, paragraph 2, letter e), of Italian Legislative Decree no. 231/2001, and referred to in the General Part of the 231 Model, provides for sanctions to be applied to those who the Company ascertains to be responsible for the offenses referred to as:

- retaliation or adopting behaviour to hinder the report (even attempted) or breaching the duty of maintaining confidentiality,
- failure to establish reporting channels, failure to implement procedures to manage the same, or procedures that do not comply with the provisions of the decree or the absence of activities to verify and analyse reports,
- civil liability of the whistleblower, even with a first instance judgement, for defamation or slander in cases of fraud or gross negligence, unless the same has already been convicted in first instance for crimes of defamation or slander;

as well as against anyone who breaches this procedure.

For the same offences, ANAC can intervene by applying financial penalties (from € 500 up to € 50,000) in the event the same offences are confirmed.