Whistleblowing Procedure

Version	Date of approval
I edition	15 December 2023
II edition	22 December 2023

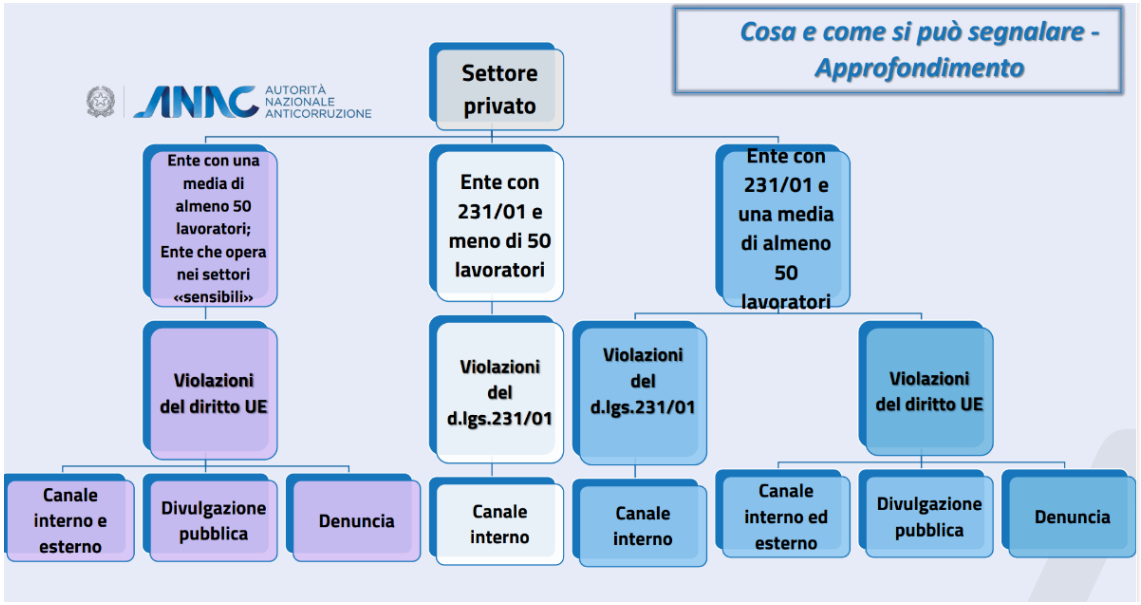
Sommario

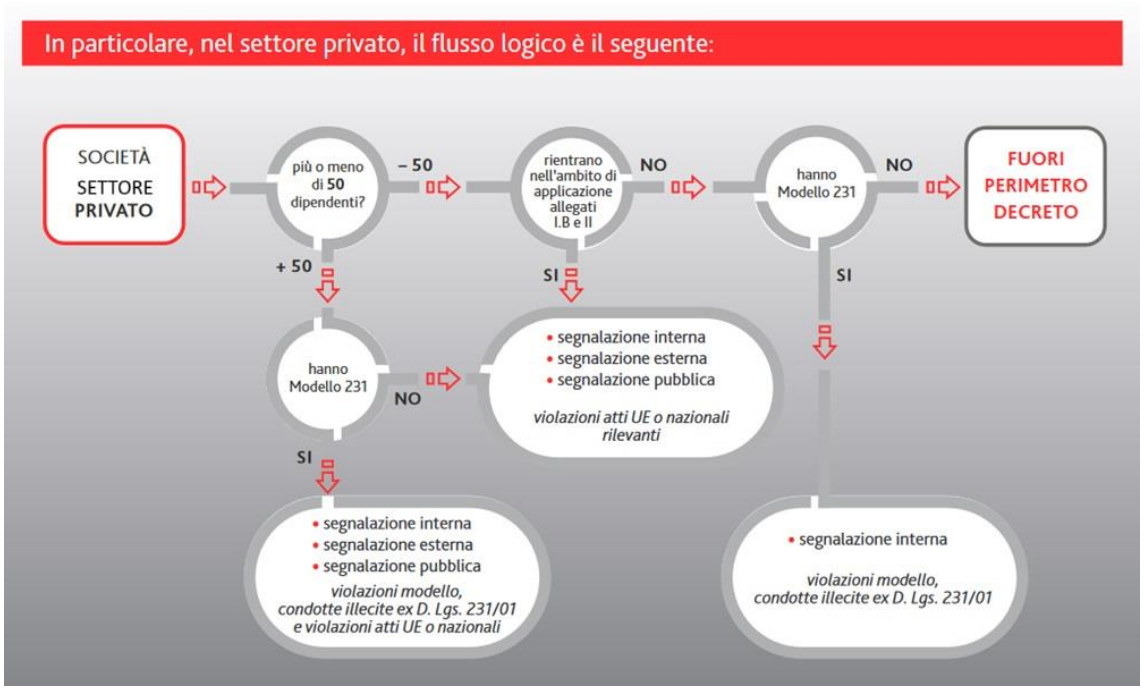
1. INTRODUCTION AND LEGAL BACKGROUND

Legislative Decree No. 24/2023, implementing Directive (EU) 2019/1937, repeals the previous regulations on whistleblowing (Legislative Decree 179/2017) and encloses in a single regulatory text – for the public and private sectors – the protection regime for individuals who report unlawful conduct of which they have become aware in a work context (so-called whistleblower).

More generally, the regulatory framework is as follows:

- Directive (EU) 2019/1937
- Legislative Decree 24/2023
- ANAC Whistleblowing Guidelines of 12/7/2023
- Legislative Decree 196/2003
- Regulation 2016/679 (GDPR)
- Legislative Decree 231/2001
- Code of Ethics of Civitanavi Systems Spa
- Organizational Model 231 of Civitanavi Systems Spa.





2. OBJECT AND PURPOSE

In light of the provisions of Legislative Decree 24/2023 and the regulatory context in force, Civitanavi Systems Spa (hereinafter also referred to as "Civitanavi" or the "Company") has activated its own internal reporting channels. The main objective of this procedure (hereinafter also the "Procedure") is to define:

- the scope of the whistleblowing system;
- the entities that can make reports;
- the scope of the conduct, events or actions that may be reported;
- the channels (written and/or oral) through which reports are made;
- the principles and general rules that govern the reporting process, including the safeguards for the reporting party, the person involved (the so-called reported party) and any subjects mentioned, as well as the consequences of any abuses in the use of the established channels;
- the process of managing Reports in its various phases, with the identification of roles, responsibilities and operating methods.

3. DEFINITIONS

For the purposes of this Procedure, unless expressly and/or otherwise provided, the terminological definitions referred to in art. 2 of Legislative Decree 24/2023, and in particular:

- "***violation***" or "***violations***": conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity, as specified in art. 2, letter a) of Legislative Decree 24/2023[1];
- '***information on violations***' means information, including well-founded suspicions, concerning infringements committed or which, on the basis of concrete evidence, may be committed in the organisation with which the reporting person or the person making a complaint to the judicial or accounting authority has a relevant legal relationship, as well[2] as elements concerning conduct aimed at concealing such violations;
- "***Reporting Person***" or "**Whistleblower"** *means a natural person who reports or publicly discloses information about violations acquired in the context of his or her work*;[3]

---

[1]Art. 2 comma became 1. (a) D.Lgs 24/2023:
"*1. For the purposes of this Decree, the following definitions shall apply:*
(a) 'infringements' means conduct, acts or omissions which are detrimental to the public interest or the integrity of the public administration or private entity and which consist of:

1) *administrative, accounting, civil or criminal offences that do not fall under numbers 3), 4), 5) and 6);*
2) *unlawful conduct pursuant to Legislative Decree no. 231 of 8 June 2001, or violations of the organisational and management models provided for therein, which do not fall under numbers 3), 4), 5) and 6);*
3) *offences falling within the scope of the European Union or national acts referred to in the annex to Decree 24/2023 or the national acts implementing the European Union acts referred to in the annex to Directive (EU) 2019/1937, even if not indicated in the annex to Decree 24/2023, relating to the following areas: public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems;*
4) *acts or omissions affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union as specified in the relevant secondary legislation of the European Union;*
5) *acts or omissions concerning the internal market, as referred to in art. Article 26(2) of the Treaty on the Functioning of the European Union, including infringements of the European Union competition and State aid rules, as well as infringements concerning the internal market linked to acts infringing corporate tax rules or mechanisms the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable corporate tax legislation;*
6) *acts or conduct which frustrate the object or purpose of the provisions laid down in Union acts in the areas referred to in points (3), (4) and (5)*;

[2] Pursuant to art. 3 paragraphs 1-2 of Legislative Decree 24/2023.
[3] In addition to the company's direct full-time employee, the following are also included:

- part-time employee;
- worker with intermittent employment contract, apprenticeship contract, ancillary work, work supply contract,
- provision of occasional work;
- coordinated and continuous collaborators;
- self-employed;
- interns, volunteers, and trainees, paid and unpaid;
- shareholders and persons with administrative, managerial, controlling, supervisory or representative functions;
- Suppliers;

- '***facilitator***' means a natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- "***work context***": the work or professional activities, present or past, carried out in the context of the relationships referred to in art. 3, paragraphs 3 or 4, through which, regardless of the nature of such activities, a person acquires information on violations and in the context of which he or she could risk suffering retaliation in the event of a report or public disclosure or complaint to the judicial or accounting authority;
- "***Reported***" or "Affected Person*" means the natural or legal person named in the internal or external report or public disclosure as the person to whom the violation is attributed or as a person otherwise implicated in the reported or publicly disclosed violation;*
- "***retaliation***(s)" means any conduct, act or omission, even if only attempted or threatened, carried out by reason of the report, the complaint to the judicial or accounting authority or the public disclosure and which causes or may cause unjust damage to the reporting person or to the person who filed the complaint, directly or indirectly;
- "***Whistleblowing manager***" or "Reporting manager": person/office/internal/external body composed of personnel specifically trained for the management of the internal reporting channel in line with the provisions of art. 4 of Legislative Decree 24/2023 and specifically appointed/appointed by the Company;
- "***Recipients***": for the purposes of this Procedure, the following are understood, as better identified below: the Company's employees; all the Company's stakeholders; the reporting person; the person reported; the manager of the report and the company functions that may be involved in the consequent activities;
- "***Employee(***s)": the natural person who works for the Company on the basis of an employment contract or by reason of the role held (including the company's directors);
- "***Stakeholder***" means a person or organization that may influence, be influenced, or perceive itself as being influenced, directly or indirectly, by a decision or activity of the Company. The stakeholder may be internal or external to the Company and include, by way of example, employees (including workers hired for the purpose of leasing) and collaborators, candidates, third parties (customers, suppliers, consultants and professionals), investors, regulators;
- "Model 231***":** *the Organizational Model adopted by the Company pursuant to Legislative Decree 231/2001.*
- "***Supervisory Body"*** (also "***SB***"): pursuant to Article 6, paragraph 1 letter b) of Legislative Decree 231/2001, the body responsible for monitoring and regularly verifying the effectiveness of the Company's Model 231, for reporting any deficiencies and/or need for updating.
- "***Platform***": the software for the creation and management of the Company's internal reporting channel pursuant to Legislative Decree 24/2023.

4. RECIPIENTS

This Procedure applies to all Recipients (as defined above), who intend to report information relating to relevant violations pursuant to Legislative Decree 24/2023 through the Company's internal channels.

5. ACTIVITIES

5.1 REPORTING THE VIOLATION

5.1.1 Who can report misconduct and violations

Anyone in the context of their work who becomes aware of (or has a well-founded suspicion that unlawful conduct and/or a violation has occurred or may occur), may report it in accordance with this Procedure, refraining from taking independent in-depth and/or investigative initiatives. In particular, reports can be made by all the subjects defined above as "*Reporting person*" or "Whistleblower".

- workers or collaborators of suppliers;
- freelancers and consultants;
- third parties;
- probationary workers;
- candidates (if the information about the violation was acquired during the selection process);
- former employees (if the information about the violation was acquired during the employment relationship).

5.1.2 Subject of the reports

The following are reported:

- information on violations of which the Whistleblower has become aware in the context of his/her work context, during the performance of his/her work duties or in any case due to the existing or past relationship with the Company;
- information relating to conduct aimed at concealing the violation[4];
- information on violations that have not yet been committed, but that the Whistleblower believes can be verified in the presence of precise and consistent concrete elements.

Referring to the specific definition of "violation" in the "Definitions" paragraph above, it is specified here that the information on violations that can be reported through the Company's internal channels may concern:

1) relevant unlawful conduct pursuant to Legislative Decree 231/2001 and violations of Model 231 and/or the Company's Code of Ethics;
2) offences that fall within the scope of European or national legislation referred to in the Annex to the Decree or of the national legislation implementing the European Union acts indicated in the Annex to Directive (EU) 2019/1937 (although not present in the Annex to the Decree), relating to the following sectors: public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems;
3) acts or omissions affecting the EU's financial interests[5];
4) acts or omissions relating to the internal market[6];
5) acts or conduct which defeat the object or purpose of the provisions laid down in EU acts.

5.1.3 Reports not protected by whistleblowing regulations

Whistleblowing protections do not apply to:

- anonymous (see below);
- consisting of disputes, claims or requests related to a personal interest of the whistleblower or of the person who has filed a complaint with the judicial authority that relate exclusively to their individual employment relationships or inherent to their employment relationships with hierarchically superior figures or with colleagues[7];
- based on mere suspicions or rumours, unless the Whistleblower, although not certain of the actual occurrence of the facts reported and of the author of the same, considers it highly probable, based on his knowledge, that the reported unlawful act has actually occurred;
- infringements already compulsorily regulated by EU or national acts concerning financial services, products and markets and the prevention of money laundering and terrorist financing, transport security and environmental protection[8];
- violations of national security, as well as procurement relating to defence or national security aspects, unless such aspects fall within the scope of secondary EU law;

[4] For example, concealment or destruction of evidence about the commission of the violation.
[5] By way of example: fraud, corruption and any other illegal activity related to the expenses of the European Union.
[6] Examples include: infringements of competition and state aid.
[7] In such circumstances, you can contact your HR department and/or your reporting manager.
[8] As indicated in art. 1, par. 2, lett. b), of Legislative Decree no. No. 24/2023. By way of example, in the "financial services and prevention of money laundering and terrorist financing" sector, the application of Article 52-ter of the Consolidated Law on Banking and Articles 4-undecies and 4-duodecies of the Consolidated Law on Finance remain unaffected, respectively. In addition to specific internal communication channels, these provisions also include an external channel, addressed to the Bank of Italy or Consob, depending on the supervisory division. In the field of anti-money laundering and terrorist financing, Legislative Decree no. 231/2007 as amended by Legislative Decree no. 90/2017 which introduced art. Amendment No 48 on internal breach reporting systems.
In addition, in the area of transport safety, the application of the rules on the monitoring of occurrences in the field of civil aviation, flag State responsibility for compliance with the Maritime Labour Convention, as well as international standards for ship safety, pollution prevention and living and working conditions on board for ships calling at Community ports and sailing in waters under the jurisdiction of the Member States remains unaffected. Member States; Finally, with reference to the "environmental protection" sector, the special rules on the safety of offshore oil and gas operations will continue to apply.

- facts or circumstances falling within the scope of national or European Union provisions on classified information, legal or medical secrecy and the secrecy of court decisions, or falling within the scope of national provisions on criminal procedure, the autonomy and independence of the judiciary, the provisions on the functions and powers of the Superior Council of the Judiciary, in the field of national defence and public order and security, as well as in the exercise and protection of the right of workers to consult their representatives or trade unions, protection against unlawful conduct or acts carried out as a result of such consultations, the autonomy of management and labour and their right to enter into collective agreements, as well as the repression of anti-union conduct;
- consisting of commercial complaints;
- requests to exercise the rights regarding the protection of personal data against the Company (so-called privacy rights) pursuant to art. 15-22 of EU Regulation 2016/679 (so-called "GDPR") for which please refer to the procedure in use by the Company. If these circumstances are also relevant pursuant to the 231 Organizational Model, they must be reported, as provided for in this Procedure.

Reports falling within the above types, although excluded from whistleblowing protections, will be handled pursuant to paragraph 8.2 below, as inadmissible reports as "not material".

In the case of anonymous reports, also in the light of ANAC's indications, it is specified that the same, if they are punctual, detailed and supported by appropriate documentation, are processed by the competent company department as indicated in the following paragraph 8.

In any case, anonymous reports must be registered by the Reporting Manager and the documentation received must be kept. In fact, where the anonymous whistleblower is subsequently identified and has suffered retaliation, the whistleblower must be guaranteed the protections provided for the whistleblower.

5.1.4 Unfounded reports

Reports that are unfounded as a result of the activities provided for in this Procedure, if made intentionally with intent or gross negligence, may result in the application of disciplinary sanctions, as provided for by this Procedure, Model 231 and the Company's Disciplinary Code (if any).

5.1.5 Form and minimum content of internal reports

For the purposes of the admissibility of the Report and the activation of the protections provided for by Legislative Decree 24/2023, the Whistleblower must indicate his/her personal details.

In order for a report to be acted upon, it must:

1) be carried out in good faith,
2) be substantiated and based on precise and consistent facts,
3) relate to facts that can be ascertained and known directly by the Whistleblower.

To this end, it is necessary[9] that the Whistleblower:

a) provides a detailed description of the (alleged) violation, indicating the circumstances of the time and place in which the facts, conduct and/or omissions described were committed (or could be committed);
b) identifies the perpetrator of the (alleged) unlawful conduct (so-called reported) by specifying any element that allows identification (name/function/company role);
c) indicates any witnesses or persons in any way involved in the circumstance referred to in letter a).

It is the Whistleblower's right, both at the time of sending the report and subsequently, to attach documents and/or circumstances that may further substantiate and/or further substantiate what has been declared.

5.2 SAFEGUARDS

5.2.1 Content of the safeguards and subjective scope of application

The safeguards provided by whistleblowing legislation mainly consist of:

[9] Mandatory elements for the purpose of the correct management of the report or the verification of its admissibility.

- guarantee of confidentiality and confidentiality
- the prohibition of retaliatory acts

These safeguards apply:

a) to the Whistleblower;
b) Facilitators;
c) relatives[10] who work in the same work context;
d) to the work colleagues of the reporting person or of the person who has filed a complaint with the judicial or accounting authority or made a public disclosure, who work in the same working context as the same person and who have a habitual and current relationship with that person;
e) entities owned by the reporting person or the person who has filed a complaint with the judicial or accounting authority or who has made a public disclosure or for which the same persons work, as well as entities operating in the same working environment as the aforementioned persons.

5.2.2 Confidentiality

From the moment the report is sent, the internal reporting channels adopted by the Company guarantee the confidentiality of:

a) Whistleblower;
b) Facilitators;
c) Reported;
d) Persons other than the Reported but mentioned in the report.

Consequently, without the express consent of the Whistleblower, the following may not be revealed:

- identity of the whistleblower,
- identity of the person reported,
- content of the report,
- any documents attached to the report.

The channel manager and any other parties involved (e.g. SB or HR department) are required to maintain the utmost confidentiality and to manage reports in order to guarantee professionalism, objectivity, impartiality and confidentiality of the activities undertaken to follow up on the report.
To this end, the Company's reporting process requires that:

- personal data that are clearly not useful for the management of a specific report are not collected or, if collected accidentally, are processed in compliance with the principle of data minimization;
- the identity of the Whistleblower and any other information from which it may be inferred, directly or indirectly, may not be revealed, without the express consent of the reporting person himself, to persons other than those competent and/or appointed and/or appointed to receive or follow up on the reports, expressly authorised to process such data[11];
- In the context of disciplinary proceedings, the identity of the reporting person cannot be revealed, if the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if they are consequent to the same. If the complaint is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the accused, the report will be used for the purposes of disciplinary proceedings only in the presence of the express consent of the reporting person to the disclosure of his or her identity.

5.2.3 Prohibition of retaliatory or discriminatory acts

Acts of retaliation or discrimination, direct or indirect, against the Whistleblower and other protected persons (as clarified in the previous paragraphs) are prohibited.

Any violation of this prohibition will result in the application of the measures provided for in Model 231.

By way of example and not limited to, the following constitute retaliatory acts:

a) dismissal, suspension or equivalent measures;

[10] Persons linked to the whistleblower by a stable emotional or family bond within the fourth degree.
[11] Pursuant to art. 29 and 32, paragraph 4, of the GDPR and art. 2-quaterdecies of the Code regarding the protection of personal data referred to in Legislative Decree no. 196 of 30 June 2003

b) relegation or non-promotion;
c) change of duties, change of place of work, reduction of salary, modification of working hours;
d) suspension of training or any restriction of access to it;
e) negative merit notes or negative references;
f) the adoption of disciplinary measures or other sanctions, including financial sanctions;
g) coercion, intimidation, harassment or ostracism;
h) discrimination or unfavourable treatment;
i) the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the worker had a legitimate expectation of such conversion;
j) non-renewal or early termination of a fixed-term employment contract;
k) damage, including to the person's reputation, in particular on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
l) improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person not being able to find employment in the sector or industry in the future;
m) the early termination or cancellation of the contract for the supply of goods or services;
n) the cancellation of a licence or permit;
o) the request to undergo psychiatric or medical examinations.

6. INTERNAL REPORTING CHANNELS

6.1 I INTERNAL REPORTING CHANNELS

The Company fosters and promotes a culture of transparency and communication of reports and to this end has established and made available various internal reporting channels:

- reporting **channel to the Supervisory Body 231**;
- internal whistleblowing reporting channel **in written form, through the Platform;**
- internal whistleblowing reporting channel **in oral form, through the Platform**;
- Whistleblowing internal reporting channel **in oral form, through a face-to-face meeting**.

6.2 REPORTS TO SB 231

The report of violations of Model 231, of the Code of Ethics and/or of the commission of predicate offences pursuant to Legislative Decree 231/2001 can be made to the SB through the SB's e-mail address (odv231@civitanavi.com), access to which is reserved only for members of the SB.

6.3 THE PLATFORM FOR INTERNAL WRITTEN REPORTS

6.3.1 The Platform

The Company has adopted an IT platform for whistleblowing reports called "**Integrity Line**" (the "Platform"), provided by the specialized service provider **EQS,** VAT 11630410964, with registered office in Corso Vercelli 40, 20145 Milan (MI).

The provider and the service offered by it guarantee confidentiality, confidentiality and anonymity, as required by Legislative Decree 24/2023. The provider has also been qualified for privacy purposes.

The Platform is structured in such a way as to ensure that:

- During the reporting process, the information acquired complies with the principles of personal data protection and maximum confidentiality. This is done through the adoption of encryption techniques and the implementation of technical and organizational security measures defined, evaluated and implemented also in the light of an impact assessment pursuant to Article 35 of the GDPR;
- the relevant information is accessible exclusively to the Whistleblowing Manager, within which the individual components have been authorised, as well as to any persons who have received specific authorisation;
- it is available continuously 24 hours a day, 7 days a week;
- the segregation of the reporting channel is allowed with reference to the company functions and the subjects who can access it for the collection and management of reports.

Access to the Platform is allowed, in general, to "reporting" parties, through:

- Company Website: https://www.civitanavi.com/it/governance/whistleblowing

- URL: https://civitanavi.integrityline.com.

6.3.2 Reporting in writing via the Platform

When submitting the Report, the Platform provides the Whistleblower with the credentials to allow him/her to subsequently recall the Report submitted, verify its status, obtain information on the follow-up and outcome and communicate with the Reporting Manager.

The Referral Manager accesses the Platform to consult all the Reports received and follow up on them and/or carry out verification activities.

6.3.3 Oral reporting through the Platform

The Platform allows the whistleblower to send the report also in oral form, through a special voice messaging system, integrated into the Platform itself, which allows audio messages to be recorded and sent.

6.4 THE INTERNAL REPORTING CHANNEL MANAGER ("*Whistleblowing manager*")

6.4.1 Appointment of the person or office to handle reports

For the management of internal reporting channels, the Company appoints a person in charge pursuant to Article 4 of Legislative Decree no. 24/2023, who corresponds to the **"Head of the Internal Audit function"** (also "Internal Audit").

Since the Company manages the Internal Audit function in an outsourced manner, the person in charge referred to above is an "external party" pursuant to art. 4, paragraph 2, second part, Legislative Decree 24/2023, equipped with professionalism and specific skills, specially trained in whistleblowing and privacy, as well as equipped with the necessary independence, autonomy and impartiality.

During the reporting phase, the Whistleblower, with express consent, may indicate whether his/her report:

- it can only be visible to the above-mentioned manager;
- or, if the same can also be visible to other parties who may be involved in order to follow up on the report and take the consequent measures.

6.4.2 The activity of the internal reporting channel manager

The internal reporting channel manager, also through the Platform, carries out the following activities[12]:

a) issues the Whistleblower with acknowledgment of receipt of the report within 7 (seven) days from the date of receipt;
b) maintains dialogue with the Whistleblower and may request additions from the latter, if necessary;
c) diligently follows up on reports received;
d) may interface with other company functions and figures to request their collaboration for the purposes of any analysis and consequent investigation regarding the Report, in absolute compliance with the guarantees of confidentiality referred to in Legislative Decree 24/2023, the GDPR and this Procedure;
e) may also carry out investigation activities with the involvement of other corporate functions or figures and/or external consultants, in full compliance with the guarantees of confidentiality referred to in Legislative Decree 24/2023, the GDPR and this Procedure;
f) provides the Whistleblower with respect to[13] the report within 3 (three) months from the date of the acknowledgment of receipt of the report (or, in the absence of such notice, within 3 months from the expiry of the 7-day period from the submission of the report) and, in any case, informs him/her of the closure of the report.

6.4.3 Reports sent to parties other than the appointed reporting manager

If the Report is submitted to a person other than the Whistleblowing Manager, the same report must be sent to the latter by the recipient within 7 (seven) days of receipt, providing written notice to the Whistleblower.

[12] In this regard, see also paragraph 8 below "INTERNAL WHISTLEBLOWING PROCESS".
[13] Please refer to the "Definitions" section above for the definition of "feedback" and "follow-up".

6.4.4 Reports on 231 sent to the internal reporting channel manager

In the event that the Whistleblowing Report relates to Violations attributable to relevant unlawful conduct pursuant to Legislative Decree 231/2001 and/or violations of the 231 Organizational Model and/or the Code of Ethics (and does not concern Violations attributable to the SB itself or to one of its members), the Whistleblowing Manager shall promptly inform the SB, by means of a specific information flow, concerning both the receipt of the report and its content, and the follow-up that is given to it.

In the event of a 231-relevant report sent through the Platform, the Whistleblowing Manager shares the information with the SB for the exclusive and limited purpose of viewing the report, its content and the attached documents in order to be able to carry out any consequent activities provided for by the 231 Model.

6.5 MANAGEMENT OF CONFLICTS OF INTEREST

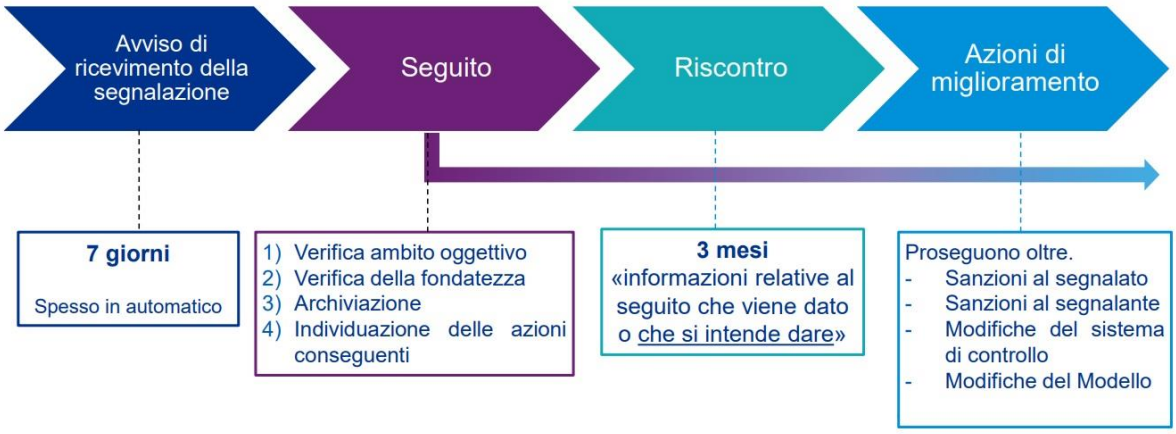
In cases where the Report concerns facts and/or conduct concerning the internal reporting channel manager, or in cases where the Report concerns facts and/or conduct concerning the person or office appointed by the Company to manage the investigations relating to the reports (if different from the entity that manages the mere reporting channel: for example, the internal committee appointed to investigate well-founded reports) and/or any consequent measures (e.g. the sole director, one or more members of the Board of Directors, or other persons with managerial powers and/or appointed to decide on disciplinary measures), the Whistleblower may alternatively:

a) send the report through the reporting channel of the Supervisory Body 231;

b) submit the report through the Platform; in this case, the Internal reporting Channel Manager promptly involves the Chairman of the Board of Statutory Auditors, in order to coordinate and define the follow-up to be given to the report and the methods for its management.

In the aforementioned cases a) and b), the entire process of managing the Report (including the communication of the response, follow-up and final outcome) is not the responsibility of the Manager(s) involved in the Report itself (who must therefore be treated and guaranteed as a "person involved").

WHAT THE COMPANY SHOULD DO AFTER RECEIVING A REPORT



7. PROTECTION OF PERSONAL DATA

7.1 DATA CONTROLLERS AND DATA PROCESSORS

The Company assumes the role of Data Controller in relation to the processing carried out in the context of the reports under its responsibility.

The Company has formally appointed a Data Processor pursuant to art. 28 of Regulation (EU) 2016/679:

- the supplier EQS Group S.r.l. for the supply and maintenance of the "Integrityline" software/platform. It should be noted that the data relating to the Company's reports are stored on data *servers* located in the European Union.

7.2 EVALUATION OF IT TOOLS

The tools adopted by the Company to establish the written and oral internal reporting channels have been the subject of a Data Protection Impact Assessment (DPIA) pursuant to art. 35 of Regulation (EU) 2016/679 necessary to describe the processing of data, assess its necessity, proportionality and related risks, as well as in order to prepare the necessary appropriate measures.

7.3 INFORMATION AND CONSENT

7.3.1 Acknowledgment of the privacy policy

The Whistleblower must read the privacy policy of the Data Controller and declare the acknowledgment as follows:

- in the case of a written or oral report through the Platform, by means of the appropriate flag "*I have read and understood the Privacy Policy and I accept*".

7.3.2 Express Consent to Data Disclosure

At the time of sending the report, the Whistleblower, through the Platform or in person meeting, may give his[14]/her consent that his/her identity and/or any other information from which the same may be inferred, directly or indirectly, may be revealed to parties other than those competent to receive or follow up on the reports, expressly authorized to process such data.

The reporting entity may disclose the identity of the whistleblower (and/or any other information from which the same may be inferred, directly or indirectly) exclusively:

- in cases where the disclosure is strictly necessary and functional to the process of verifying the report; in this case, the receiving subjects or functions are required to observe the utmost confidentiality and confidentiality;
- in the case of disciplinary proceedings, when knowledge of the identity of the whistleblower is essential for the defence of the accused person[15]. In this case, the reporting manager shall notify the whistleblower by written communication of the reasons for the disclosure of the confidential data.

7.4 REGISTER OF TREATMENTS

The processing carried out as part of the whistleblowing activity, as a separate activity, has been included and mapped as specific processing within the register drawn up pursuant to art. 30 Reg. (EU) 2016/679. The Company's Data Register is updated, at least annually, by the Data Controller, with the help of the Company's Privacy Office/Function.

7.5 DATA RETENTION

7.5.1 Traceability and Storage

The Platform guarantees the traceability of each operation.

All information and documentation relating to the submission of the report and its management are strictly confidential and stored in a secure place, accessible only to the personnel in charge, for the period of time allowed by law, defined by the Privacy Policy and in accordance with the Company's policies on data retention.

In particular, internal reports and related documentation are kept for a period not exceeding 5 (five) years from the date of communication of the closure of the reporting procedure, without prejudice to longer retention periods determined by procedural and/or legal requirements.

---

[14] The consent in question is not an obstacle to the submission of the report, but it could have an impact on the process of ascertaining the report.

[15] That is, in the cases provided for by art. 12, paragraph 5 of Legislative Decree 24/2023: "*In the context of disciplinary proceedings, the identity of the reporting person cannot be revealed, where the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if consequent to the same. If the complaint is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the accused, the report will be used for the purposes of disciplinary proceedings only in the presence of the express consent of the reporting person to the disclosure of his or her identity*".

Internal reports and related documentation are stored on servers located in the territory of the European Union[16].

8. INTERNAL WHISTLEBLOWING MANAGEMENT PROCESS

The internal whistleblowing management process includes the following operational steps:

1) receipt of the report;
2) assessment of the admissibility of the report;
3) investigation;
4) closure of the report;
5) reporting;
6) Retention of reports.

8.1 RECEIPT OF THE REPORT

Following receipt of the Report, the Reporting Manager shall send the Whistleblower acknowledgement of receipt within 7 (seven) days from the date of receipt[17].

In the event that the Report is submitted to a person other than the Whistleblowing Manager (e.g., another corporate function) and qualified as a Report covered by this Procedure by the same Reporting Person (e.g., describing it as a "whistleblowing report", "whistleblowing report", etc.), such different person shall promptly transmit it (possibly via the Platform) to the Reporting Manager, within 7 (seven) days of its receipt, giving written notice of the transmission to the Whistleblower.

In cases of conflicts of interest, the provisions of paragraph 6.5 above on conflicts of interest shall apply.

Upon receipt of a Report, regardless of the channel used, the Reporting Manager, including through the Platform:

- assigns a progressive identification number that allows them to be uniquely identified;
- compiles and keeps a Register of Reports (on a confidential IT medium, possibly through the Platform) containing at least the following fields (which must then be updated consistently with the results of the activities referred to in the subsequent phases of the process outlined in this Procedure):
  - Identification number/protocol;
  - Date of receipt;
  - Classification of the Report, according to the results of the preliminary verification phase referred to in paragraph 8.2. "Assessment of the admissibility of the report" means: (a) not relevant; (b) non-negotiable; (c) relevant and negotiable;
  - Management status.

8.2 PRELIMINARY ASSESSMENT OF ADMISSIBILITY OF THE REPORT

The Reporting Manager, after receiving and registering the report, as well as sending the acknowledgment of receipt itself:

- diligently **follows up** on the report, first of all providing a **preliminary analysis,** both to identify the potential regulatory framework of reference (for example: anti-corruption, money laundering, environmental, 231 legislation, etc.), and for the purpose of an initial assessment of its merits;
- maintains **dialogue** with the whistleblower;
- if necessary, and where the reporting procedures allow it, the Reporting Manager may **request additional information or additional documentation** from the Whistleblower, in order to better substantiate the report and allow a more exhaustive and conclusive assessment;

[16] However, the management of reports may involve transfers of personal data outside the European Union, in particular for cases of intra-group transfers to subsidiaries with establishments in non-EU countries or for cases of engagement of suppliers based in non-EU countries. In both cases, the transfer will be carried out in compliance with the rules for the protection of personal data, to which reference is made.

[17] Such acknowledgment of receipt does not constitute express confirmation or tacit admission of the admissibility and/or validity of the Report.

- in cases where the Report relates to Violations attributable to relevant unlawful conduct pursuant to Legislative Decree 231/2001 and/or violations of Model 231, the Reporting Manager promptly informs the 231 Supervisory Body, subsequently ensuring adequate information flows regarding the follow-up that is given (or intended to be given) to the Report;

Following these preliminary in-depth analyses and assessments, the Whistleblowing Manager will **classify the Report** into one of the following categories, which imply a different and specific management flow of the Report itself:

a) Non-relevant report: the Report that is not attributable to *admissible "violations*" referred to in this Procedure or made by persons who do not fall within the definition of "*reporting person*" and in general all those referred to in paragraph 5.1.3 above, including anonymous ones. In this case, if the report is sufficiently detailed but falls outside the scope of this procedure, the Reporting Manager shall submit it to the attention of the Head of the Human Resources Function (also "HR Manager") and the Head of the Administration-Finance Function (also "CFO"), so that they can forward it to the company functions deemed competent, which will process it according to the applicable procedures and rules, also in order to detect any weaknesses in the internal control and risk management system or impacts on sensitive processes for the purposes of Legislative Decree 231/2001.

b) Non-negotiable **report**: the Report that, at the end of the in-depth and preliminary assessment phase (possibly following discussion with the whistleblower), is manifestly unfounded, or is not sufficiently detailed and therefore does not allow further investigations to be carried out. In this case, the Reporting Manager archives the Report with adequate reasons, and notifies the whistleblower through the platform;

c) Relevant **and negotiable** report: the Report that – possibly following in-depth analysis and preliminary assessments by the manager, and/or dialogue with the whistleblower – is deemed not manifestly unfounded, sufficiently detailed and falling within the scope of application of this Procedure. In this case, the Reporting Manager initiates the investigation phase, described in the following paragraph.

For the purposes of assessing admissibility and the consequent classification of the report (not material; not negotiable; material and treatable), the report received must also be examined taking into account the likelihood of occurrence of the reported offence and its potential impact[18].

In cases of conflicts of interest, the Reporting Manager takes action in accordance with the provisions of paragraph 6.5 "Management of conflicts of interest".

8.3 INVESTIGATION

At the end of the preliminary assessment phase, where the Report received has been classified as "material and negotiable", the Reporting Manager:

a) initiates the internal analyses and investigations deemed necessary for the purpose of ascertaining the reported facts, involving, where necessary, the corporate functions involved in the Report and/or the SB;
b) may request further information and/or documentation from the Whistleblower, as well as involve him/her in the investigation phase and provide him/her with any information about the start and progress of the investigation;
c) can hear the Reported (or must hear him, at his request), also through the acquisition of written observations and documents;

[18] For example, useful indications can be drawn from the following parameters:

- If the report does not fall within the scope of whistleblowing, should it be handled in accordance with another procedure?
- Does the wrongdoing need to be reported to law enforcement or regulators?
- Is there an immediate need to stop or suspend business operations?
- Is there an immediate health and safety risk?
- Is there an immediate risk to human rights or the environment?
- Is there an immediate need to protect evidence before it is deleted or destroyed?
- Is there a risk to the organization's functions, services, and/or reputation?
- Will business continuity be impacted by the report being investigated?
- Could the report of wrongdoing arouse media interest?
- Is there any additional confirmation information available?
- Have wrongdoings been reported before?
- How did the whistleblower get the information?

d) where necessary for the purposes of the investigation, it may avail itself of the support of experts or consultants or specialized companies external to the Company, providing the necessary guarantees of confidentiality and protection referred to in this procedure. These subjects, if involved, draw up a report relating to the activities carried out, which is sent to the Reporting Manager;
e) may conclude the investigation at any time, if in the course of the investigation it is ascertained that the Report is unfounded.

8.4 CLOSURE OF THE REPORT

Within 3 (three) months from the date of the acknowledgment of receipt or, in the absence of such acknowledgement, within 3 (three) months from the expiry of the term of 7 (seven) days from the submission of the report, the Whistleblowing Manager shall provide *feedback*[19] to the Whistleblower through the platform, regarding *the follow-up* that has been given (or is intended to be given) to the Report.

At the end of the investigation phase, the Whistleblowing Manager draws up a written report, which must show:

a) the descriptive elements of the Violation (e.g.: place and date of the facts, facts and/or conduct ascertained, supporting evidence and documents);
b) the analyses and verifications carried out, the results of the same and the company subjects or third parties involved in the preliminary assessment and/or investigation phase;
c) a summary evaluation of the analysis process with an indication of the cases ascertained and the related reasons;
d) the outcome of the investigations, any violations found and the reasons for them.

In cases where the Report relates to Violations attributable to relevant unlawful conduct pursuant to Legislative Decree 231/2001 and/or violations of Model 231, the Reporting Manager shall make the aforementioned final report available on the Platform to the SB, for any assessment and/or determination.

In cases where, as a result of the investigation, it appears that the Report is well-founded (i.e. unfounded, but has been carried out with wilful misconduct or gross negligence on the part of the Whistleblower), the Whistleblowing Manager makes the relevant final report available on the Platform to the competent company department for the evaluation of appropriate initiatives, possibly also of a disciplinary nature (if the violation is committed by an employee) or commercial/contractual (if the violation is not committed by an employee).

8.5 REPORTING

The Whistleblowing Manager informs the following subjects in writing about the activities carried out and their outcome, by sending a summary report containing statistical and quantitative information (e.g. number of reports received, categorization of the same pursuant to paragraph 8.2, etc.), and with anonymization of any data from which the identity of the whistleblower and/or the reported and/or the other subjects involved in the report and its reporting process can be deduced dispatch.

On a quarterly basis:

- Audit Committee, Risks, Related Parties and Sustainability.

On an annual basis:

- Board of Directors;
- Board of Statutory Auditors;
- Control, Risks, Related Parties and Sustainability Committee;
- 231 Supervisory Body, as part of the information flows provided for by Model 231.

Reference should be made to Model 231 and its annexes for the regulation of any event-based information flows to the SB.

[19] For the purposes of this procedure, *"feedback*" means: the communication to the reporting person of information relating to the follow-up that is given or intended to be given to the report; "*Follow-up*" means the action taken by the person entrusted with the management of the reporting channel to assess the existence of the reported facts, the outcome of the investigations and any measures taken.

The adoption of any measures following the ascertainment of violations reported or, in any case, following reports received through internal whistleblowing reporting channels is the responsibility and competence of the Board of Directors and/or the company departments concerned.

The Board of Directors and/or the corporate functions involved must promptly inform and keep the Manager updated of the report about the measures taken (and/or intended to be taken) as a result of the evaluation of the written report referred to in paragraph 8.4, also in order to allow the Manager to respond to the whistleblower.

9. PENALTIES

9.1 DISCIPLINARY SYSTEM

Violation and/or failure to comply with the contents and provisions of this procedure, as well as the commission of conduct for which Legislative Decree 24/2023 provides for the application of administrative pecuniary[20] sanctions by the ANAC, may result in the imposition of disciplinary sanctions by the Company, as provided for by the Company's Disciplinary Code (if any), the applicable National Collective Labour Agreement and/or Model 231, in respect of:

a) of those who, having an obligation pursuant to current legislation and/or this procedure: i) have not established the internal reporting channels provided for by Legislative Decree 24/2023, and/or ii) have not adopted whistleblowing procedures that comply with the regulations, and/or iii) have omitted one or more of the activities referred to in the previous paragraphs;
b) those who commit retaliation (as defined in this procedure) against the Whistleblower;
c) those who obstruct or attempt to obstruct the Reports;
d) of those who have not followed up on the Reports received;
e) of those who violate the confidentiality obligations referred to in art. 12 of Legislative Decree 24/2023 as described above[21];
f) of the Reported, if the Reports, as a result of the management process, are found to be well-founded;
g) of the Whistleblower, if he/she has made a Report in bad faith and/or with intent or gross negligence and/or in abuse or exploitation of this procedure, when his/her criminal liability (including with a first instance judgment) for the crimes of defamation or slander or in any case for the same crimes committed with the complaint to the judicial or accounting authority or his/her civil liability is ascertained, for the same reason, in cases of wilful misconduct or gross negligence.

As for the responsible parties, it is specified that:

- in the cases under a), the person responsible for the sanctioned conduct is identified in the steering body;
- in cases under b), the person responsible for the sanctioned conduct is the natural person identified as responsible for the retaliation;

[20] In detail, the administrative fines imposed by ANAC are as follows:
a) from €10,000 to €50,000 when it ascertains that the natural person identified as responsible has committed retaliation;
b) from €10,000 to €50,000 when it ascertains that the natural person identified as responsible has obstructed the report or attempted to obstruct it;
c) from €10,000 to €50,000 when it ascertains that the natural person identified as responsible has violated the obligation of confidentiality pursuant to art. 12 of Legislative Decree no. No. 24/2023. This is without prejudice to the sanctions applicable by the Guarantor for the protection of personal data for profiles of competence based on the regulations on personal data;
d) €10,000 to €50,000 when it ascertains that no reporting channels have been established; In this case, the steering body in both public and private sector entities is considered to be responsible;
e) from €10,000 to €50,000 when it ascertains that no procedures have been adopted for the making and management of reports or that the adoption of such procedures does not comply with the provisions of the decree; In this case, the steering body in both public and private sector entities is considered to be responsible;
f) from €10,000 to €50,000 when it ascertains that the verification and analysis of the reports received has not been carried out; In this case, the manager of the reports is considered to be responsible;
g) from €500 to €2,500, when the civil liability of the reporting person for defamation or slander in cases of wilful misconduct or gross negligence is ascertained, even by a first instance judgment, unless the same has already been convicted, even in the first instance, for the crimes of defamation or slander or in any case for the same crimes committed with the complaint to the judicial authority.

[21] This is without prejudice to the sanctions applicable by the Privacy Guarantor for the protection of personal data for profiles of competence based on the regulations on personal data.

- In cases under d) and e), the person responsible for the sanctioned conduct is the person managing the reports[22].

The disciplinary proceedings are initiated and managed in accordance with the principle of proportionality, as well as the criterion of correlation between violation and sanction and, in any case, in compliance with the procedures provided for by the applicable legislation and the CCNL in force.

In order to ensure impartiality and avoid conflicts of interest, decisions regarding any disciplinary measures, complaints or other actions to be taken in relation to reports or non-compliance with this procedure are taken by the company organizational functions in charge and, in any case, by parties other than those who conducted the activities of receipt and/or verification of the Report.

For any other provisions regarding the disciplinary and sanctioning system, reference is made to the Company's Model 231.

9.2 LIMITATION OF LIABILITY OF THE REPORTING PERSON

A Whistleblower shall not be punishable if he or she reveals or disseminates information on violations covered by the duty of secrecy (other than that on classified information, medical and forensic secrecy and court decisions), or relating to the protection of copyright or the protection of personal data, or that offends the reputation of the person involved or reported, when, at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or disclosure of the same information was necessary to uncover the infringement. In such cases, any further liability, including civil or administrative liability, is excluded.

In any case, criminal, civil or administrative liability is not excluded for conduct, acts or omissions not related to the Report, the complaint to the judicial or accounting authority or the public disclosure, or that are not strictly necessary to disclose the violation.

10. STORAGE AND UPDATING OF THE PROCEDURE

The Company's HR Department is responsible for the maintenance and practical and formal updating of this procedure.

11. INFORMATION AND TRAINING

11.1 INFORMATION

Before its formal adoption and on the occasion of any subsequent amendments, prior notice of this procedure must be given to the trade union representatives, if any.

This Procedure must be carried out by the HR Department:

- displayed and made easily visible and knowable at all company offices;
- published on the Company's website, on a page or section specifically and exclusively dedicated to whistleblowing and the internal reporting channel;
- made available on the company intranet;
- communicated to Recipients and Stakeholders by e-mail and/or by other means deemed appropriate, at the time of its adoption and on the occasion of any modification, revision or update thereof.

11.2 TRAINING

The person appointed by the Company for the management of the internal reporting channel pursuant to art. 4 Legislative Decree 24/2023 must receive adequate training:

- general, in terms of corporate compliance;
- on whistleblowing and privacy.

[22] In this regard, it should be noted that the management of reports falls within the prerogatives attributable to the performance of the work activity of the person in charge of managing reports; therefore, any non-compliance provides for the application of the sanctions sanctioned by the applicable CCNL.

The Company periodically carries out training activities for all staff regarding corporate compliance, and in particular on whistleblowing. This activity must be documented and archived, ensuring traceability.

12. EXTERNAL REPORTING CHANNEL AND PUBLIC DISCLOSURE

12.1 REPORTING TO ANAC

The Whistleblower may submit an "external report" [23]through the channels made available by the National Anti-Corruption Authority (ANAC) if, at the time of submission, at least one of the following conditions is met:

- within the context of one's work context, there is no mandatory activation of the internal reporting channel or this channel, even if mandatory, has not been established or the same, even if provided, has not been activated;
- The internal channel adopted does not comply with the provisions of art. 4 of the Decree;
- the Report made through an internal channel was not followed up;
- the Whistleblower has reasonable grounds – on the basis of the particular circumstances of the case, which are precise and consistent – to believe that, if he/she were to make a Report through internal channels, it would not be effectively followed up or that the same Report could lead to the risk of retaliation;
- the Whistleblower has reasonable grounds – on the basis of the particular circumstances of the case, which are precise and consistent – to believe that the Breach may constitute an imminent or obvious danger to the public interest.

The methods of access to these external channels and, in general, the regulations on External Reporting are indicated by Legislative Decree no. 24/2023, to which reference is made, and are detailed by ANAC on its website (https://www.anticorruzione.it/), as well as through specific Guidelines that the Authority issues.

12.2 PUBLIC DISCLOSURE

The Whistleblower who makes a "public disclosure[24]" enjoys the protections provided for by Legislative Decree 24/2023 on whistleblowing if, at the time of disclosure, at least one of the following conditions is met:

- the whistleblower has previously made an internal and external report or has made an external report directly, under the conditions and in the manner provided for by Legislative Decree 24/2023 and has not been responded to within the prescribed terms;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- The whistleblower has reasonable grounds to believe that the external report may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances of the specific case, such as those in which evidence may be concealed or destroyed or where there is a well-founded fear that the person receiving the report may be colluding with the infringer or involved in the breach itself.

[23] Pursuant to Article 2 of Legislative Decree 24/2023, "external reporting" means "*the communication, written or oral, of information on violations, submitted through the external reporting channel referred to in Art. 7 Legislative Decree 24/2023 established by the ANAC*".

[24] Pursuant to Article 2 of Legislative Decree 24/2023, "public disclosure" means "*making information on violations public through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people*".