Notification on the protection of whistleblowers of violations of national or EU regulatory provisions, as well as violations of the Organizational Model 231 (Legislative Decree No. 24/2023)

≈ When whistleblower protection does not apply ≈

Whistleblower protection is not applicable in the following cases:

a) a) Disputes, claims, or requests related to a personal interest of the whistleblower or the person who has filed a complaint with the judicial or accounting authority that exclusively concern their individual employment relationships, or related to their employment relationships with hierarchically superior figures.
b) For example, reports concerning labor disputes and pre-litigation phases; discrimination among colleagues; interpersonal conflicts between the whistleblower and another worker or with superior managers; reports related to data processing carried out in the context of the individual employment relationship in the absence of injury to the public interest or the integrity of the private entity.
c) b) Reports of violations where already mandatorily governed by European Union or national acts listed in Part II of the annex to the decree (*) or by national acts that constitute the implementation of European Union acts listed in Part II of the annex to Directive (EU) 2019/1937, even if not listed in Part II of the annex to the decree.
d) (*) Specifically, these include: financial services, products and markets, and prevention of money laundering and terrorist financing. Transport safety. Environmental protection.
e) c) Reports of violations concerning national security, as well as procurement related to defense or national security aspects, unless such aspects fall within the relevant derived law of the European Union.

≈ Who is eligible for protection ≈

Protection from possible retaliation following the submission of reports applies to the following individuals:

a) **Employees**, including those with part-time, intermittent, fixed-term, temporary agency, apprenticeship, ancillary work, or those performing occasional tasks.
b) **Self-employed workers,** as defined in Chapter I of Law No. 81/2017 (Protection of self-employment), including workers on project contracts as per Article 2222 of the Civil Code.
Owners of a collaborative relationship as per Article 409 of the Code of Civil Procedure: agency relationships, commercial representation, and other collaborative relationships that result in continuous and coordinated work performance, mainly personal, even if not subordinate; workers who perform their work activity for a private sector entity organizing it autonomously (parasubordinate relationship).
Owners of a collaborative relationship as per Article 2 of Legislative Decree No. 81/2015: collaborations organized by the client that result in exclusively personal and continuous work performances, whose execution methods are organized by the client. Even if the execution methods of the performances are carried out through digital platforms.
c) **Freelancers and consultants,** who carry out their activities at the private entity and who might be in a privileged position to report the violations they witness.
d) **Volunteers and interns,** paid and unpaid, who carry out their activities at the private entity and who risk, nevertheless, facing retaliation for having reported violations. Retaliation against these subjects could materialize, for example, in no longer using their services, in giving them negative work references, in damaging their reputation or career prospects in another way.
e) **Shareholders**, individuals who hold shares in one of the private sector entities, where the latter assume a **corporate form**. This concerns those who have become aware of violations to be reported in the exercise of the rights they hold by virtue of their role as shareholders within the company.
f) **Individuals with functions of administration,** direction, control, supervision, or representation, even if the functions are carried out de facto. Subjects broadly connected to the organization in which the violation occurs and in which they exercise certain functions, even in the absence of a regular assignment (de facto exercise of functions), example: members of the board of directors, even without executive roles.
g) **Facilitators,** individuals who assist the whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential. If it involves a

"union representative" assisting the whistleblower under the union's insignia, they do not act as a facilitator. In such cases, the provisions regarding consultations of union representatives and suppression of anti-union behaviors as per Law No. 300/1970 (Workers' Statute) apply.

h) **Individuals** from the same work environment as the whistleblower, complainant, or those making a public disclosure, linked by a stable emotional or kinship relationship within the fourth degree. This refers to individuals connected by a network of relationships arising because they operate or have operated in the same work environment, even in the past.
   Regarding the interpretation of "stable emotional bond," reference should be made to Article 1, paragraph 36, of Law No. 76/2016 (so-called Cirinnà law), which states that "two adult persons who are stably united by couple's emotional bonds and mutual moral and material assistance, not bound by relations of kinship, affinity or adoption, marriage or a civil union" constitute a "de facto cohabiting" relationship. Civil jurisprudence has also repeatedly addressed this issue, clarifying that cohabitation requires the presence of an interpersonal situation of an emotional nature with a tendency towards stability, a minimum duration, and that is expressed "in a shared life" and interests (e.g., order of the Civil Cassation, section III, April 13, 2018, No. 9178; Cass. judgment 7128, March 21, 2013, Civil Cass. Sec. II, judgment March 21, 2013, No. 7214; Civil Cass. Sec. I, judgment August 8, 2003, No. 11975).
i) **Work colleagues** of the whistleblower, complainant, or public discloser, who work in the same work context and have a regular and ongoing relationship with said individuals. Unlike the previous category, this must be individuals who are currently working with the whistleblower at the time of the report.
j) **Entities** owned by the whistleblower, complainant, or public discloser, or for which the same individuals work, as well as entities that operate in the same work context as the aforementioned individuals. Retaliatory or discriminatory acts could be directed against legal entities of which the whistleblower is: the owner; for which they work; or to which they are otherwise connected within a work context. Examples include: cancellation of the supply of goods and/or services; inclusion of the entity on a blacklist; boycott actions, etc.

≈ Other situations in which whistleblower protection applies ≈

Protection from possible retaliation is also applicable in the following situations:

1) when the legal relationship has not yet started, if the information on the violations was acquired during the selection process or in other pre-contractual phases (e.g., during a job interview);
2) during the probationary period;
3) after the dissolution of the legal relationship if the information on the violations was acquired during the course of the relationship itself.

≈ What can be the subject of reporting, public disclosure, or complaint ≈

Information on **violations, including reasonable suspicions**, of national and EU regulations that harm the public interest or the integrity of the public administration or private entity committed within the framework of the organization with which the whistleblower or complainant has one of the qualified legal relationships considered by the legislature can be the subject of reporting, public disclosure, or complaint.
Information on violations can also concern **violations not yet committed** that the whistleblower, reasonably, believes could be committed based on concrete elements. These elements can also be irregularities and anomalies (symptomatic indices) that the whistleblower believes may lead to one of the violations provided for by the Decree.

≈ What is meant by violations ≈

Behaviors, acts, or omissions that harm the public interest or the integrity of the public administration or the private entity and consist of:

- administrative, accounting, civil, or criminal offenses;
- illicit conduct relevant under Legislative Decree No. 231/2001;
- violations of the organizational, management, and control models provided by Legislative Decree No. 231/2001;
- offenses within the scope of application of European Union or national acts, listed in the annex to Legislative Decree No. 24/2023, or national acts that implement European Union acts

listed in the annex to Directive (EU) 2019/1937, although not mentioned in the annex to the mentioned decree, related to the following sectors:

1) public procurement;
2) services, products, and financial markets, and prevention of money laundering and terrorist financing;
3) product safety and compliance;
4) transport safety;
5) environmental protection;
6) radioprotection and nuclear safety;
7) food and feed safety, and animal health and welfare;
8) public health;
9) consumer protection;
10) privacy and personal data protection;
11) network and information system security.

- acts or omissions that harm the EU's financial interests (Article 325 TFEU) specified in EU regulations, directives, decisions, recommendations, and opinions (Anti-fraud): fraud, corruption, and any illegal activity related to Union expenditure;
- acts or omissions regarding the internal market, undermining the free movement of goods, people, services, and capital (Article 26, paragraph 2, TFEU), including violations of European Union rules on competition and State aid, corporate tax, and mechanisms aimed at obtaining a tax advantage that negates the object or purpose of the applicable corporate tax legislation.

≈ What is meant by retaliation ≈

Any behavior, act, or omission, even if only attempted or threatened, carried out because of the report, complaint to the judicial or accounting authority, or public disclosure, and that causes or may cause direct or indirect unjust damage to the person reporting or to the person who has filed the complaint.

Examples of retaliation, including but not limited to, are:

a) dismissal, suspension, or equivalent measures;
b) demotion or failure to promote;
c) change of duties, change of workplace, salary reduction, change of working hours;
d) suspension of training or any limitation of access to it;
e) demerit notes or negative references;
f) disciplinary measures or other sanctions, including financial penalties;
g) coercion, intimidation, harassment, or ostracism;
h) discrimination or any other unfair treatment;
i) failure to convert a fixed-term employment contract into an indefinite-term contract, where the worker had a legitimate expectation of such conversion;
j) non-renewal or early termination of a fixed-term employment contract;
k) damages, including to the person's reputation, particularly on social media, or economic or financial prejudices, including the loss of economic opportunities and loss of income;
l) improper inclusion on lists based on a formal or informal sectoral or industrial agreement, which may prevent the person from finding employment in the sector or industry in the future;
m) early termination or cancellation of the contract for the supply of goods or services;
n) cancellation of a license or permit;
o) demand for psychiatric or medical examinations.

Furthermore, retaliation could also include, for example:

- the demand for impossible results to be achieved in the ways and times indicated;
- deliberately negative performance evaluation;
- unjustified withdrawal of assignments;
- unjustified failure to assign tasks with simultaneous assignment to another subject;
- repeated rejection of requests (e.g., vacations, leaves);

- unjustified suspension of patents, licenses, etc.

≈ What it means to report ≈

Communicating in written or oral form information about violations that one has become aware of within a work context, in which a qualified relationship must exist between the whistleblower and the Entity.

≈ Internal reporting ≈

Use of the internal channels established by the Entity to report, **in written or oral form**, information on violations that one has become aware of within the work context, in which a qualified relationship must exist between the whistleblower and the entity.

≈ Who is the whistleblower ≈

An individual who reports or publicly discloses information on violations acquired in their work context.

≈ Who is the involved person ≈

A natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as a person otherwise involved in the reported or publicly disclosed violation.

≈ What is meant by work context ≈

Work or professional activities, current or past, conducted within a legal relationship, by virtue of which, regardless of the nature of such activities, a person acquires information on violations and within whose context they might risk retaliation in case of reporting, public disclosure, or complaint to the judicial or accounting authority.
The term “work context” should be given a broad interpretation and considered not only with reference to an employment relationship in the "strict sense" with the organization; that is, those who have established with the private entity other types of legal relationships should also be considered.
In other terms, what matters is the existence of a qualified relationship between the whistleblower and the private entity where they operate, a relationship pertaining to current but also past work or professional activities.

≈ What characteristics the report must have ≈

For its correct management, it is necessary that the report is as detailed as possible. In particular, it is necessary that the following are clear:

- the circumstances of time and place where the reported fact occurred;
- the description of the fact itself;
- the general information or other elements that allow the identification of the subject to whom the reported facts are attributed;
- the intentions to keep one's identity confidential and to benefit from the protections provided in case of retaliations suffered following the report.

It is also useful to attach documents that can provide elements of the foundation of the reported facts, as well as the indication of other subjects potentially aware of the facts.
Where what is reported is not adequately detailed, those managing the reports may ask the whistleblower for additional elements through the dedicated channel or even in person, should the whistleblower have requested a direct meeting.

≈ What happens after submitting an internal report ≈

The manager of the internal reporting channel must:

1) evaluate the admissibility of the report in terms of the existence of its essential requirements;
2) if the report is not adequately detailed, request additional elements from the whistleblower;
3) maintain absolute confidentiality regarding the identity of the whistleblower and the contents of the report;
4) within 7 days from the date of receipt, issue a receipt notice to the whistleblower;
5) maintain communication with the whistleblower;

6) properly follow up on the received report;
7) provide feedback to the whistleblower.

Regarding the **essential requirements of the report**, for the purpose of its admissibility to recognize the protections provided to the whistleblower, in the following exemplary cases, the report might not be considered admissible:

- manifest unfoundedness due to the absence of factual elements suitable to justify investigations;
- verified generic content of the report, such that it does not allow for the understanding of the facts or reporting of wrongdoing accompanied by inappropriate or irrelevant documentation.

Once the admissibility of the report as whistleblowing is assessed, the report manager initiates an internal investigation on the reported facts or conduct to evaluate their actual existence.
For the conduct of the investigation, the report manager can start a dialogue with the whistleblower, asking for clarifications, documents, and additional information, always through the dedicated channel or in person if necessary.
If deemed necessary, the manager can also acquire acts and documents from other offices of the Entity, avail themselves of their support, involve third parties through hearings and other requests, always ensuring that the confidentiality of the whistleblower and the reported individual is not compromised.
Should elements of manifest unfoundedness of the report be identified following the activity carried out, it will be archived with adequate reasoning. Where, on the other hand, the report is found to be substantiated, the manager must immediately turn to the relevant internal bodies, each according to their roles and competencies. It is understood that the relevant internal bodies are also required to maintain absolute confidentiality regarding the identity of the whistleblower, the contents of the report, and the identity of the reported individual as a possible perpetrator of the violation.

It is not the responsibility of the report manager to determine individual responsibilities, of any nature, nor to perform checks on the legality or merit of acts and/or measures adopted by the Entity, under penalty of encroaching on the competencies of other subjects appointed to do so within each entity or of the judiciary, should the report pertain to the possible commission of a crime.

At the conclusion of the **investigative phase**, the report manager provides feedback to the report, informing the whistleblower of the measures envisaged, adopted, or to be adopted to follow up on it, and the reasons for the chosen course of action.

The **response** may consist of:

- notification of the procedure's archiving due to a lack of sufficient evidence or other reasons;
- the initiation of an internal investigation and any related findings, as well as the measures taken to address the issue raised;
- referral to a competent authority for further investigation, to the extent that such information does not prejudice the internal investigation nor infringe on the rights of the involved person.

It's worth noting that the response could also be merely interim, as information about all the above-described activities intended to be undertaken and the progress of the investigation can be communicated. In this last case, upon completion of the investigation, the outcomes must still be communicated to the reporting person.

The *whistleblower*, within 3 months from the date of the receipt notice or, in the absence of such notice, within 3 months from the expiration of the 7-day term from the submission of the report, must be **informed of the outcome** of their report.

≈ Confidentiality protection ≈

Reports cannot be used beyond what is necessary to adequately follow up on them. The identity of the reporting person and any other information from which their identity can be directly or indirectly deduced cannot be disclosed without the **expressed consent** of the reporting person to anyone other than those competent to receive or to follow up on the reports.

In particular:

- in the case of the initiation of **criminal proceedings**, the identity of the whistleblower is protected by secrecy in the ways and limits provided by Article 329 of the Code of Criminal Procedure. This provision mandates secrecy on the actions taken in the preliminary investigations "until the defendant can be aware of them and, in any case, not beyond the closure of the preliminary investigations."
- - in the case of the initiation of **disciplinary proceedings**, the identity of the reporting person cannot be revealed if the charge is based on findings distinct and additional to the report, even if consequent to it. If the charge is based, wholly or in part, on the report and knowing the identity of the reporting person is indispensable for the defense of the accused, the report will only be usable for the purposes of the disciplinary proceedings with the expressed consent of the reporting person to reveal their identity. In this last hypothesis, a written communication of the reasons for such revelation is also required.

The MOG 231 adopted provides disciplinary sanctions against all those found to be responsible for violating the confidentiality obligation in the management of reports.

≈ Violations of personal data protection legislation ≈

Any violations of the personal data protection regulations by authorized persons or data processors entail **liability** on the part of the data controller or the data processor under whose direction said persons have operated.

In such cases, the Data Protection Authority can adopt corrective measures and, in cases provided by law, **apply administrative monetary penalties**. These administrative penalties do not apply to processing carried out in the judicial sphere; the same violations may also be relevant under criminal law and lead to civil liability.

≈ Limitations on the data subject's rights ≈

The involved person or the person mentioned in the report, regarding their personal data processed within the context of the report, cannot **exercise the rights** that the GDPR normally recognizes for data subjects (Articles 15 to 22 of GDPR 679/2016), namely:

- the right of access by the data subject (Art. 15);
- the right to rectification (Art. 16);
- the right to erasure (so-called 'right to be forgotten') (Art. 17);
- the right to restriction of processing (Art. 18);
- the obligation to notify in cases of rectification or erasure of personal data or restriction of processing (Art. 19);
- the right to data portability (Art. 20);
- the right to object to processing (Art. 21);
- automated individual decision-making, including profiling (Art. 22).

Exercising such rights could result in actual and concrete harm to the confidentiality of the whistleblower's identity (Art. 2-undecies, paragraph 1, letter f) Privacy Code - Legislative Decree 196/2003 and subsequent modifications). The reported subject or the person mentioned in the report is also precluded from, should they believe that the processing concerning them violates the aforementioned rights, addressing the data controller and, in the absence of a response from the latter, filing a complaint with the Data Protection Authority.

≈ Limitations to the whistleblower's liability ≈

Among the protections recognized for the whistleblower, there are also certain **limitations of liability** regarding the revelation and dissemination of certain categories of information.

These limitations apply under certain conditions, in the absence of which there could be **consequences in terms of criminal, civil, administrative liability:**

a) the **first condition** requires that at the time of revelation or dissemination, there are reasonable grounds to believe that the information is necessary to disclose the violation. Therefore, the person must reasonably believe, and not on the basis of mere speculation, that this information needs to be disclosed because it is indispensable for bringing the violation to light, excluding superfluous information, and not for further and different reasons (e.g., gossip, vengeful, opportunistic, or scandalous purposes);

b) the **second condition** demands that the reporting has been carried out in compliance with the conditions set by the regulation to benefit from protections against retaliation: 1) reasonable grounds to believe that the information on the violations was true and fell within the reportable violations according to the decree; 2) reports, both internal and external, or public disclosures made in compliance with the methods and conditions of this notice.

Both conditions must exist to exclude liability; if met, persons who report, denounce or make a public disclosure do not incur any type of civil, criminal, administrative, or disciplinary liability.

The limitations of the whistleblower's liability also concern **the "lawful" access to the reported information** or documents containing said information.

Should the acquisition or access to the information or documents have been obtained by **committing a crime** (e.g., unauthorized access or act of cyber piracy), the exclusion of the whistleblower's liability does not apply, but criminal liability remains, along with any other civil, administrative, and disciplinary liability.

≈ Prohibition of waivers and settlements ≈

Acts of waiver and settlements, whether total or partial (e.g., pursuant to agreements or other contractual conditions) concerning the right to make reports, public disclosures, or complaints in accordance with regulatory provisions are not valid.

Similarly, it is not permitted to impose on the whistleblower, as well as other protected subjects, to deprive themselves of the possibility to access means of protection to which they are entitled: confidentiality; any retaliatory measures suffered because of the report, public disclosure, or complaint made; limitations of liability resulting from the report, disclosure, or complaint under the conditions provided. These protections cannot be the subject of **voluntary waiver**.

The above does not apply if waivers and settlements are signed in protected venues (judicial, administrative, union): the whistleblower and other protected subjects can validly waive their rights and means of protection or make them the subject of a settlement, if this occurs in the protected venues indicated in Article 2113

c) The circumstance that such acts are concluded before bodies that, due to their composition, ensure authority and impartiality, allows considering the position of the subject who waives or settles as more protected, also in terms of greater genuineness and spontaneity of consent.

≈ Conditions for enjoying protection from retaliation ≈

In the case of retaliation, the application of the protection regime requires that the reports made by one of the subjects identified by the legislature satisfy certain conditions and requirements:

a) The whistleblower must reasonably believe, also in light of the circumstances of the specific case and the data available at the time of reporting, that the information on the reported violations is true. **Mere assumptions or rumors as well as publicly known news are not sufficient.** What matters is that the whistleblower has acted based on a reasonable belief (e.g., a wrongdoing has occurred or is about to occur). This represents an essential safeguard against harmful or offensive reports and ensures that those who have deliberately and knowingly reported incorrect, blatantly unfounded, or misleading information do not enjoy protection.
b) For protection purposes, it is irrelevant whether the subject reported without being certain of the actual occurrence of the reported facts and/or the identity of their author or also reported inaccurate facts due to a **genuine error**.
c) Similarly, whoever makes a report is entitled to protection if they have acted based on **concrete circumstances alleged** and information actually obtainable such to reasonably believe that the information on the reported violations is relevant as it falls among the offenses considered by the legislature.
d) Furthermore, the report must be made **using the designated channel** and according to the methods provided by the Decree. In the case of reports sent to a subject other than the competent one, the latter must forward them without delay to the subject authorized to receive and manage the reports, simultaneously informing the reporting person of the transmission. To allow this timely transmission, the whistleblower must **clearly indicate** in the subject of the report that it is a whistleblowing report (see also above).

e) There must be a **close connection** between the report and the unfavorable behavior/act/omission suffered, directly or indirectly, by the reporting person, for these to be considered retaliation and, consequently, for the subject to benefit from protection.

For protection purposes, the specific personal reasons that led **individuals to make a report are irrelevant**. Focusing on motivations could be a strategy used to deflect attention from the reported issues and delegitimize the whistleblower at the same time.

In the absence of compliance with these general conditions, protection cannot be guaranteed even to **subjects other than the one who reports** if, due to the role assumed in the reporting process and/or the particular relationship that binds them to the whistleblower, they indirectly suffer retaliation.

Notwithstanding the specific limitations of liability provided by the legislature, the protection foreseen in case of retaliation does **not apply in the case of a sentence**, even if not final of the first degree, against the whistleblower for criminal responsibility for the **crimes of slander or defamation** or anyway for the same crimes connected to the report, or of civil liability, for having reported intentionally false information with **malice or gross negligence**.
In cases of verification of the cited responsibilities, a **disciplinary sanction** must also be applied to the reporting or complaining subject: it is necessary to include this specific punishable case in the codes of conduct or in the MOG 231.

≈ External reporting ≈

Written or oral communication of information on violations or any retaliation suffered following the report made through the internal channel, forwarded via the external reporting channel managed by ANAC (National Anti-Corruption Authority).
For the use of the external reporting channel, at least one of the following conditions must be met:

a) the internal channel, although mandatory, is not active or, even if activated, does not comply with the provisions of the decree with reference to the subjects and the methods of presenting internal reports that must be able to guarantee the confidentiality of the identity of the whistleblower and other protected subjects;
b) the reporting person has already made an internal report and it has not been followed up. This refers to cases where the internal channel was used but the channel manager did not undertake, within the prescribed terms, any activity regarding the admissibility of the report, the verification of the existence of the reported facts, or the communication of the outcome of the investigation carried out. In this regard, it is sufficient that even just one of the indicated activities (admissibility check, investigation, communication of outcomes) was not performed to consider the "lack of follow-up" and, therefore, to be able to legitimately access the external channel;
c) the reporting person has reasonable grounds to believe that, if they made an internal report, it would not be effectively followed up or that such reporting could lead to the risk of retaliation;
d) the reporting person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest.

≈ Public disclosure ≈

Through this method, information about violations is made public via the press, electronic means, or other distribution methods capable of reaching a large number of people (e.g., social networks).
The whistleblower who makes a **public disclosure** benefits from the protection provided by the regulation if, at the time of the public disclosure, one of the following conditions applies:

a) an **internal report** was made, to which the entity did not respond within the prescribed terms (3 months from the date of the receipt notice or, in the absence of such notice, within 3 months from the expiration of the 7-day term from the submission of the report), followed by an **external report to ANAC** which, in turn, did not provide a response to the whistleblower within reasonable terms (3 months or, if justified and motivated reasons exist, 6 months from the date of receipt notice of the external report or, in the absence of said notice, from the expiration of the 7 days from receipt);

b) the person has already directly made an external report to ANAC which, however, did not respond to the whistleblower regarding the measures envisaged or adopted to follow up on the report within reasonable terms (3 months or, if justified and motivated reasons exist, 6 months from the date of receipt notice of the external report or, in the absence of said notice, from the expiration of the 7 days from receipt);
c) the person directly makes a public disclosure because they have a **reasonable basis** to believe, based on concrete circumstances alleged and information actually obtainable, not on mere speculation, that the violation may represent an imminent or manifest danger to the public interest. Consider, for example, an emergency situation or the risk of irreversible harm, including to the physical safety of one or more individuals, that requires the violation to be promptly revealed and widely publicized to prevent its effects;
d) the person directly makes a public disclosure because they have reasonable grounds to believe that the external report may lead to the risk of retaliation or may not be effectively followed up because, for example, they fear that evidence may be hidden or destroyed, or that those who received the report may be colluding with the author of the violation or involved in the violation itself. Consider, as an illustrative case, where the recipient of a violation report, in agreement with the person involved in the violation, proceeds to archive said report in the absence of the prerequisites.

In public disclosure, where the subject **voluntarily** reveals their identity, confidentiality protection is not relevant, all other forms of protection provided by the Decree for the whistleblower remain in place.

≈ Anonymous reports and their treatment ≈

These are reports from which it is not possible to establish the identity of the whistleblower.
If detailed, for ANAC, they are equated to ordinary reports and, therefore, considered by it in its "ordinary" supervisory procedures.
Anonymous reports received through internal channels should be considered the same as ordinary ones and treated according to the criteria set by the organization.
Such reports, if received via an internal channel, must be registered and the related documentation stored for no more than 5 years from the date of receipt, in order to be able to trace them should the whistleblower communicate to ANAC that they have suffered retaliatory acts as a result of the anonymous report.

This information, in addition to being displayed on the company website, is directly forwarded to: Personnel, External Collaborators (including Professionals), and all Suppliers of goods and/or services (including any contractors).