WHISTLEBLOWING PROCEDURE

1. PURPOSE

The purpose of this procedure is to define the process for managing whistleblowing.

2. SCOPE OF APPLICATION AND DUTY OF CONFIDENTIALITY

This procedure applies to violations of national or European Union legal provisions that harm the public interest or the integrity of a public administration or private entity, of which the reporting person has become aware in a public or private work-related context.

This procedure applies where unlawful acts are reported by:

- employees of public administrations;
- employees of independent administrative authorities responsible for guarantee, supervisory or regulatory functions;
- employees of publicly owned economic entities;
- employees of private-law entities subject to public control pursuant to Article 2359 of the Italian Civil Code;
- employees of in-house companies;
- bodies governed by public law or concessionaires of public services;
- employees of private-sector entities, including agency workers and apprentices;
- self-employed workers, including those carrying out flexible/remote work or engaged under collaboration arrangements;
- workers or collaborators carrying out their work activity at public-sector or private-sector entities that supply goods or services or carry out works for third parties;
- freelance professionals and consultants;
- volunteers and interns, whether paid or unpaid;
- shareholders and persons holding administrative, management, supervisory or representative functions, including where such functions are exercised on a purely de facto basis.

Confidentiality protection applies to the persons mentioned above even when:

- the legal relationship referred to above has not yet begun, if information on the violations was acquired during the selection process or other pre-contractual stages;
- during the probationary period;
- after termination of the legal relationship, if the information on the violations was acquired during the course of that relationship.

Confidentiality protection is further extended to:

- a) facilitators;
- b) persons from the same work context as the reporting person, the person who has filed a report with the judicial or accounting authority, or the person who has made a public disclosure, and who are linked to them by a stable emotional bond or a family relationship up to the fourth degree;
- c) work colleagues of the reporting person or of the person who has filed a report with the judicial or accounting authority or made a public disclosure, who work in the same work context as that person and who have a habitual and ongoing relationship with them;

- d) entities owned by the reporting person or by the person who has filed a report with the judicial or accounting authority or made a public disclosure, or for which such persons work, as well as entities operating in the same work context as the aforementioned persons.

3. REGULATORY REFERENCES

This procedure complies with Legislative Decree No. 24 of 10 March 2023.

The Data Protection Impact Assessment must be carried out in accordance with Article 35 of EU Regulation 679/2016.

A further reference is Legislative Decree No. 165 of 30/03/2001, Article 54-bis, concerning the protection of public employees who report unlawful conduct, and the ANAC Guidelines of 12 July 2023.

This procedure also incorporates ANAC Resolution No. 479 of 26 November 2025 (which amends and supplements ANAC Resolution No. 311/2023 on external reports) and ANAC Guidelines No. 1/2025 on whistleblowing through internal reporting channels, approved by ANAC Resolution No. 478 of 26 November 2025, which constitute interpretative and operational guidance for the management of the internal channel.

4. RESPONSIBILITIES

4.1 Responsibilities of the Whistleblower or Reporting Person

The whistleblower or reporting person must be protected and safeguarded from any form of retaliation; for this reason, it is important that the smallest possible number of people know their identity.

4.2 Responsibilities of the Evaluation Group

The whistleblowing evaluation group is the person or team that takes charge of the reporting person, does not know their identity, and communicates with them for the purposes of developing any investigations and providing information. It also manages the communication channel and is responsible for providing feedback to the reporting person.

4.3 Responsibilities of the Whistleblowing Evaluation Group

This working group:

- prepares, manages and updates the references and tools used to submit reports;
- receives, records and analyzes the reports received, involving the relevant functions of the organization and forwarding each report to the supervisory bodies responsible for the relevant matters (for companies incorporated under Italian law: the Board of Statutory Auditors and the Supervisory Bodies, in accordance with applicable legislation and the Organizational Models adopted pursuant to Legislative Decree 231/2001);
- prepares specific action plans and carries out any investigative activities, subject to prior agreement with Management;
- ensures that documentation is obtained and archived for a period of five years following the conclusion of verification activities;
- suggests any legal action or reports to Management;
- supports the Privacy management area in carrying out the Data Protection Impact Assessment under Article 35 of EU Regulation 679/2016.

In accordance with Article 4(2) of Legislative Decree 24/2023 and Section 3.1 of ANAC Guidelines No. 1/2025, the person managing reports — whether internal or external — is chosen from among individuals possessing the requirement of autonomy, understood as impartiality (absence of conditioning or favoritism) and independence (ability to carry out the relevant checks without interference from the governing body), specifically trained in whistleblowing and personal data protection matters, and possessing adequate knowledge of the organization. The governing body is not granted supervisory powers over the handling of individual reports.

In accordance with Section 3.3 of ANAC Guidelines No. 1/2025, the organization identifies in advance a substitute for the manager, possessing the same requirements of autonomy, impartiality and independence, who takes over management of the report if the manager is in a conflict-of-interest situation (for example, because they coincide with the reporting person or the person involved) or in the event of prolonged absence (more than seven days). If the substitute is also in a conflict-of-interest situation, or if the organization is unable to identify a substitute, the reporting person may contact ANAC directly through the external channel, where one of the conditions set out in Article 6 of Legislative Decree 24/2023 applies.

4.4 Responsibilities of External Parties

The manager of the reporting channel, or the working group responsible for managing the whistleblowing process, may be external to the organization where there is a need to engage expert legal consultants.

5. OPERATING PROCEDURES

5.1 Introduction

5.1.1 General

This Operating Procedure, issued to implement Legislative Decree 24 of 10/03/2023, governs the process for reporting violations, suspected violations and inducements to commit violations of Italian and European law.

Employees who become aware of actual or potential violations are encouraged to report them to the organization promptly (hereinafter "Reports"). Confidentiality will be guaranteed and they will not be subject to any form of retaliation.

The purpose of this Operating Procedure is to describe and regulate the management of whistleblowing, so as to enable the organization and delegated roles to verify the validity of reports and take appropriate action.

The procedure described below must be carried out in compliance with any legal obligations that may arise from the report, in particular regarding the obligation to report to the Judicial Authority or Supervisory Authorities, and with regard to the processing of personal data, privacy protection and, where present, the Supervisory Body (pursuant to Law 231).

Pursuant to Article 4(1) of Legislative Decree 24/2023 and Section 2.1 of ANAC Guidelines No. 1/2025, the adoption of this procedure and any subsequent substantial update to it must be preceded by notice to the company trade union representatives (RSA/RSU) or, in their absence, to the territorial trade union organizations that are comparatively most representative at national level, allowing a reasonable period for any comments, it being understood that such involvement is purely consultative and non-binding.

In line with Insight 1 of ANAC Guidelines No. 1/2025, the reporting channel governed by this procedure constitutes the organization's sole internal channel, suitable for receiving both whistleblowing reports under Legislative Decree 24/2023 and reports of unlawful conduct relevant under Legislative Decree 231/2001 or violations of the Organization, Management and Control Model (MOG 231), where adopted, without prejudice to the separate information flows to the Supervisory Body required under Article 6(2)(d) of Legislative Decree 231/2001.

5.1.2 Privacy Aspects

This activity must be managed as a data processing operation and, as such, must be entered in the register of processing activities (where such a register exists).

A data protection impact assessment must be carried out to assess the secure management of data; where a DPO has been appointed, their opinion must be obtained.

Employees of the organization, personnel managing the reporting channel, and members of the whistleblowing evaluation group must:

- 1) be adequately trained according to their role, with such training repeated periodically;
- 2) be expressly authorized to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2-quaterdecies of the Italian Data Protection Code (Legislative Decree No. 196 of 30 June 2003).

Personal data that is manifestly not useful for handling a specific report is not collected and, if collected accidentally, is deleted immediately (principle of data minimization).

The rights of data subjects under Articles 15 to 22 of Regulation (EU) 2016/679 may not be exercised, or may only be exercised in a manner that protects the confidentiality of the reporting person.

Appropriate privacy information must be prepared for all potential reporting persons and published on the organization's website.

Where necessary, additional information will be provided for the specific report.

Parties that share the same reporting systems must manage that sharing through a specific document (this may require appointment as data processor or a joint-controller agreement, depending on the specific situation).

Information and data may not be retained for longer than 5 years from the date the final outcome of the reporting procedure is communicated.

Data relating to reports and all related communications must therefore be deleted, both from the communication channel and from any digital devices or paper archives used to manage whistleblowing.

Digital deletion and destruction of paper documents must be carried out in accordance with the law.

5.2 Definition of Violation

The following are defined as violations:

- 1) administrative, accounting, civil or criminal offenses that do not fall within the exclusions of paragraphs 3, 4, 5 and 6 of Article 2 of Legislative Decree 24 of 10/03/2023;
- 2) unlawful conduct relevant under Legislative Decree No. 231 of 8 June 2001, or violations of organizational models, that do not fall within paragraphs 3, 4, 5 and 6 of Article 2 of Legislative Decree 24 of 10/03/2023.

5.3 Method and Content of Reports

5.3.1 Reporting Method

A report may be made in writing or verbally (through a meeting).

The organization has implemented an adequately secured reporting software platform, deemed secure by the Impact Assessment. The software can be accessed through the company website, in the dedicated reporting area, or via the following link: https://giulianotartufi.whistlelink.com/.

The software provides guided entry of information, which is received by the channel manager.

If a report is to be made verbally, the channel manager — whose email and phone contact details are appropriately publicized within the organization and on the website — will contact the reporting person. The channel manager will arrange a meeting within 20 days of the request, with the reporting person, in the strictest privacy, so as to protect the reporting person's confidentiality. At the end of the meeting, a document confirming that the report was made will be issued.

If the reporting person decides not to disclose their identity through the communication channel, the report will only be considered if it is sufficiently detailed and contains all the information needed to verify it, regardless of whether the identity of the reporting person is known.

Please note that making a report anonymously does not provide the protections afforded to public employees under Legislative Decree 190/2012, and that anonymous reports will be given lower handling priority. It remains possible to disclose one's identity at a later stage.

Pursuant to ANAC Resolution No. 479 of 26 November 2025 (which amended Section 2.2 of ANAC Resolution No. 311/2023), the organization may treat anonymous reports received through the internal channel in the same way as ordinary reports, where their handling is provided for: in such cases they are managed according to the criteria set out above for ordinary reports, without prejudice to the obligation to record and retain the related documentation under Article 16(4) of Legislative Decree 24/2023, so as to allow traceability if the reporting person subsequently informs ANAC that they have suffered retaliatory measures as a result of the anonymous report.

5.3.2 Content of the Report

A report may not contain:

- disputes, claims or requests linked to a personal interest of the reporting person, or of the person who has filed a report with the judicial or accounting authority, that relate exclusively to their own individual employment or public-employment relationships, or to their employment or public-employment relationships with hierarchically superior figures;
- reports of violations already mandatorily governed by European Union or national instruments listed in Part II of Legislative Decree 24 of 10/03/2023, or by national instruments implementing the EU instruments listed in Part II of the Annex to Directive (EU) 2019/1937;
- reports of violations relating to national security, as well as procurement relating to defense or national security matters, unless such matters fall within the relevant derived EU law.

5.3.3 Handling of Internal Reports

The person managing the internal communication channel must:

- 1. issue the reporting person an acknowledgment of receipt of the report within seven days of the date of receipt (via a dedicated entry in the management software); this is not required for verbal reports, as it is implicit in the meeting;
- 2. inform the whistleblowing management group of the new report within 7 days of the report itself;

- 3. maintain communication with the reporting person, requesting further information from them if necessary;
- 4. diligently follow up on reports received;
- 5. provide feedback on the report within 3 months of the date of the acknowledgment of receipt or, if no such acknowledgment was issued, within 3 months of submission of the report;
- 6. make clear information available on the channel, procedures and requirements for making internal reports, as well as on the channel, procedures and requirements for making external reports. This information is displayed and made easily visible in the workplace, and made accessible to persons who, while not present in the workplace, have a legal relationship as described in point 2) of this procedure. Public- and private-sector entities that have their own website also publish the information referred to in this procedure in a dedicated section of that website.

Prior to the investigation, and in accordance with ANAC Resolution No. 479/2025 (which updated Section 3.5 of ANAC Guidelines No. 1/2025), the manager verifies that the subjective and objective requirements set out in Legislative Decree 24/2023 are met (that the report comes from an eligible person and that its subject matter falls within the scope of the decree), in order to grant the reporting person the protections provided for.

Only once compliance with these requirements has been verified does the manager initiate the internal investigation into the facts or conduct reported. If a report is manifestly unfounded due to a lack of factual elements capable of justifying verification, or is so generic in content that it cannot be understood, the manager may close it, giving reasons to the reporting person, without prejudice to the option of requesting clarifications and additional information from them.

5.3.4 Handling of External Reports

The conditions for making an external report (a report to ANAC) are:

- a) the mandatory activation of an internal reporting channel is not required in the reporting person's work context, or, even if mandatory, such a channel is not active or, even if activated, does not comply with the requirements regarding the reporting person's confidentiality;
- b) the reporting person has already made an internal report and it was not followed up;
- 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 the report itself could give rise to a risk of retaliation;
- d) the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

The National Anti-Corruption Authority (ANAC) operates an external reporting channel (link: https://servizi.anticorruzione.it/segnalazioni/#!/#%2F) that guarantees, including through the use of encryption tools, the confidentiality of the identity of the reporting person, the person involved and any person mentioned in the report, as well as the content of the report and related documentation. The same confidentiality is guaranteed even when the report is made through channels other than those indicated above, or is received by personnel other than those responsible for handling reports, to whom it is in any case forwarded without delay.

External reports are made in writing through the IT platform, or verbally through telephone lines or voice messaging systems, or, at the reporting person's request, through a direct meeting arranged within a reasonable time.

An external report submitted to a party other than ANAC is forwarded to ANAC within seven days of its receipt, with simultaneous notice of the transmission given to the reporting person.

5.4 Confidentiality, Protection and Prohibition of Retaliation

5.4.1 Confidentiality

Actions arising from a report must be handled with the utmost impartiality and confidentiality by all parties involved, in full compliance with legal and regulatory principles on the processing of personal data and privacy protection.

The organization does not tolerate threats or retaliation of any kind against the reporting person or anyone who has assisted in verifying the validity of the report.

Any threats or retaliation against the reporting person must be promptly reported to the manager of the reporting channel.

Reports may not be used beyond what is necessary to provide an adequate follow-up.

The identity of the reporting person, and any other information from which that identity may be directly or indirectly inferred, may not be disclosed, without the reporting person's express consent, to persons other than those competent to receive or follow up on reports.

- In criminal proceedings, the identity of the reporting person is protected by secrecy in the manner and within the limits set out in Article 329 of the Italian Code of Criminal Procedure.
- In proceedings before the Court of Auditors, the identity of the reporting person may not be disclosed until the investigative phase has concluded.
- In disciplinary proceedings, the identity of the reporting person may not be disclosed where the disciplinary charge is based on findings that are separate from and additional to the report, even if resulting from it.

Where the charge is based, in whole or in part, on the report, and knowledge of the reporting person's identity is essential for the defense of the accused, the report may be used for disciplinary proceedings only with the reporting person's express consent to the disclosure of their identity.

The reporting person is given written notice of the reasons for disclosing confidential data, in the case referred to in the preceding paragraph, as well as in internal and external reporting procedures under this chapter, when disclosure of the reporting person's identity and information is also essential for the defense of the person involved.

Public- and private-sector entities, ANAC, and the administrative authorities to which ANAC forwards external reports within their competence, protect the identity of the persons involved and the persons mentioned in the report until the conclusion of proceedings initiated as a result of the report, in compliance with the same guarantees provided for the reporting person.

The report is exempt from the right of access to administrative documents and from the right to transparency.

Without prejudice to the protections referred to above, the person involved may be heard or, at their request, is heard, including through a written procedure involving the submission of written comments and documents.

5.4.2 Public Disclosure

A reporting person who makes a public disclosure benefits from the protection provided for under Decree 24/2023 if, at the time of the public disclosure, one of the following conditions applies:

- a) the reporting person has previously made an internal and external report, or has made an external report directly, under the conditions and in the manner set out in Articles 4 and 7, and no feedback was provided within the time limits set out by law regarding the measures planned or adopted to follow up on the report;

- b) the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest;
- c) the reporting person has reasonable grounds to believe that an external report could give rise to a risk of retaliation, or might not be effectively followed up, due to the specific circumstances of the case, such as situations in which evidence could be concealed or destroyed, or where there is reasonable concern that the recipient of the report may be colluding with the perpetrator of the violation or involved in the violation itself.

Rules on professional secrecy applicable to journalists, with regard to protecting their sources, remain unaffected.

5.4.3 Prohibition of Retaliation

Entities or reporting persons may not be subject to any form of retaliation.

In judicial or administrative proceedings, or in any out-of-court disputes concerning conduct, acts or omissions prohibited under this article against reporting persons, it is presumed that such conduct, acts or omissions were carried out because of the report, the public disclosure or the report to the judicial or accounting authority.

The burden of proving that such conduct or acts are motivated by reasons unrelated to the report, public disclosure or complaint lies with the person who carried them out.

Where a reporting person brings a claim for damages before the judicial authority, if they demonstrate that they made a report, a public disclosure, or a complaint to the judicial or accounting authority under Decree 24/2023, and that they suffered harm, it is presumed, in the absence of proof to the contrary, that the harm was a consequence of that report, disclosure or complaint.

The following are examples of conduct that constitutes retaliation:

- a) dismissal, suspension or equivalent measures;
- b) demotion or failure to grant promotion;
- c) change of duties, change of place of work, reduction of salary, change of working hours;
- d) suspension of training or any restriction of access to it;
- e) negative performance appraisals or negative references;
- f) imposition of disciplinary measures or other sanctions, including financial ones;
- g) coercion, intimidation, harassment or ostracism;
- h) discrimination or otherwise unfavorable treatment;
- i) failure to convert a fixed-term employment contract into a permanent one, 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 reputational damage, in particular on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- l) inclusion on improper lists on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in future;
- m) early termination or cancellation of a contract for the supply of goods or services;

- n) cancellation of a license or permit;
- o) a request to undergo psychiatric or medical examinations.

5.5 Verification Activities and Actions

After receiving a report, the evaluation group must verify its validity by carrying out any activity deemed appropriate. To this end, subject to authorization from Management, the following may be included among the verification and investigative activities, by way of example:

- Legal consultations
- IT consultations
- Authorizations to search office documentation
- Private investigative activity
- Reporting to the Judicial Authority
- Administrative and accounting verification activities
- Support from the company functions to be involved (IT Department, Administration, HR, etc.)

At the conclusion of the verification phase:

- if the report is found to be unfounded and it is decided not to proceed, the channel manager must formally close the report, notifying the reporting person of the outcome of the verification;
- if the report is found to be well-founded, the evaluation group must define a specific action plan including appropriate corrective actions/measures, the persons responsible, and the implementation timeline. The reporting person must in any case be informed of the outcome of the verification;
- if a report is confirmed to be well-founded, the organization will adopt appropriate disciplinary measures and any other actions, including legal action, to protect the organization.

In operational terms, the following steps must be followed:

- a. Verify whether the reporting person falls within the category of eligible persons;
- b. Verify whether the violation falls within those that may be reported;
- c. Verify whether the report is well-founded and, where applicable, proceed with either: closing the report; or carrying out internal investigations.

Internal investigations consist of in-depth activities carried out by the organization, within its own structure, in order to:

- verify information concerning possible violations of the law and, more generally, ascertain — and where possible prevent — events that could compromise the company or its employees, and from which civil, administrative or criminal liability, or reputational damage, could arise;

The investigations involve the following steps:

- receipt of the report;
- preliminary verification of the reported facts to assess their relevance, scope and potential risks;
- definition of investigative methods and identification of any internal or external resources to be involved;
- carrying out typical investigative activities to reconstruct the reported facts and assess the extent of potential damage;

- drafting of a final report;
- identification of remedial actions (including the adoption of disciplinary sanctions).

Depending on the case, the typical methods for carrying out internal investigations are:

- Analysis of databases (e.g., chambers of commerce) and other public sources (e.g., social media) to identify possible links between the reported person and third parties.
- Collection and analysis of relevant company documents.
- Forensic analysis of devices (e.g., PC, phone, tablet) assigned to the reported person to check for evidence supporting the report (e.g., emails, messages).
- Interviews with persons who may have information relevant to proving the reported violations.

5.6 Improper or False Reports

The organization reserves the right to take disciplinary and legal action against the reporting person in the event of abuse (reports that are manifestly opportunistic and/or made solely to harm the reported person or other parties concerned by the report).

5.7 Disciplinary System and Staff Training

Pursuant to Article 21(2) of Legislative Decree 24/2023 and Insight 1 of ANAC Guidelines No. 1/2025, the disciplinary system, where provided for in the Organization, Management and Control Model under Legislative Decree 231/2001 (Article 6(2)(e)), is supplemented with specific, proportionate and graduated sanctions against anyone who: engages in, attempts, or obstructs retaliation, or obstructs a report; breaches the duty of confidentiality; or fails to carry out the verification and analysis activities for reports within their competence. A disciplinary sanction is also provided for, pursuant to Article 16(3) of Legislative Decree 24/2023, against a reporting person whose criminal liability for defamation or slander, or whose civil liability for willful misconduct or gross negligence, has been established, including by a first-instance judgment, in connection with the report, complaint or public disclosure.

In accordance with Section 5 of ANAC Guidelines No. 1/2025, the organization ensures periodic, up-to-date training: (i) for personnel responsible for managing reports, on whistleblowing and privacy regulatory matters, operating procedures, and conflict-of-interest management; (ii) for all other personnel, on the purpose of the whistleblowing framework, protected persons, reporting methods, and available channels, including by reference to the information published on the organization's website.

6. LIST OF DOCUMENTS AND OPERATIONAL TOOLS

6.1 Software used

The platform used as the internal communication channel is Whistlelink, accessible at the following link: https://giulianotartufi.whistlelink.com/.

For in-person reports (via meeting), please contact the communication channel manager at the following email: whistleblowing@giulianotartufi.it.

ATTENTION

Once a report has been completed, it is essential to record the following data (which serve as the credentials for logging back into the platform):

Case number and verification code, as shown below:

Your report has been submitted	
Case number	91940238
Verification code	otrXM7u8

Save the case number and verification code if you wish to follow up on your case.

Thank you for your report. Please make a note of the case number and verification code.

It is important to save this information so that you can log back in to follow up on your report and receive feedback. You may also log in to provide additional information.

If this information is not saved or recorded, it will no longer be possible to access the report again to view its outcome or any requests for further information.

Neither the channel manager nor the Whistlelink platform can recover these credentials.