



## PROCEDURE FOR THE MANAGEMENT OF WHISTLEBLOWING REPORTS

Legislative Decree 10 March 2023, N. 24

## **PREMISE**

The legal framework of so-called "whistleblowing" was introduced into the national legal system by Article 1, paragraph 51, of Law No. 190 of November 6, 2012, titled "Provisions for the Prevention and Suppression of Corruption and Illegality in Public Administration." This law added Article 54-bis to Legislative Decree No. 165 of March 30, 2001, concerning "General Rules on Employment for Public Administration," which provides protections for public employees who report misconduct that they learn of through their work.

This framework was first expanded by Decree Law No. 90 of June 24, 2014, converted into Law No. 114 of August 11, 2014, titled "Urgent Measures for Simplification, Administrative Transparency, and Efficiency in Judicial Offices." This decree amended Article 54-bis and designated the Italian National Anti-Corruption Authority (ANAC) as a recipient of such reports. Subsequently, ANAC issued Determination No. 6 of April 28, 2015, titled "Guidelines on the Protection of Public Employees Reporting Illicit Activities (c.d. Whistleblowing)," highlighting the need to extend the protection to employees of private-law entities under public control and economic public entities, as well as to consultants, collaborators in any capacity, and collaborators of companies providing goods or services to public administration entities.

A further modification occurred with the enactment of Law No. 179 of November 30, 2017, concerning "Provisions for the Protection of Persons Reporting Crimes or Irregularities of which They Have Become Aware in a Public or Private Employment Relationship." This law, comprising three articles, stipulates the following:

- Enhanced protections for public employees reporting misconduct (first article);
- Extension of protections to employees or collaborators reporting misconduct within private entities subject to Legislative Decree No. 231/2001 or Article 11 of Law No. 300 of September 29, 2000 (second article);
- Establishment of an exemption from liability (Articles 326, 622, 623 of the Criminal Code) in cases where the whistleblower discloses official, company, professional, scientific, or industrial secrets, or violates the duty of loyalty under Article 2105 of the Civil Code (third article).

The whistleblowing framework was comprehensively reorganized through Legislative Decree No. 24 of March 10, 2023 (henceforth "Decree"), which implemented EU Directive 2019/1937 of the European Parliament and Council of October 23, 2019, on the protection of individuals who report violations of Union law. The Decree not only strengthens protections for individuals making reports, complaints, or even public disclosures (the latter being newly introduced) but also extends protections to individuals other than the whistleblower who may support the reporting party.

Below are the main innovations introduced by Legislative Decree No. 24/2023:

- Extension of the personal scope of application to private entities;
- Expansion of the categories of individuals entitled to protection for reports, complaints, or public disclosures;
- Broadening of the range of violations subject to protection and a clear distinction between what is and is not protected;

- Regulation and establishment of three reporting channels: internal (within entities), external (managed by ANAC), and public disclosure through the press or social media;
- Provisions for both written and oral reporting methods;
- Rules regarding confidentiality obligations and the handling of personal data received, managed, and shared with third parties;
- Clarification of what constitutes retaliation;
- Specification of protective measures for whistleblowers and those claiming to have been retaliated against;
- Provision of support measures for whistleblowers that may be made available by third-sector entities with adequate competencies and at no charge;
- Revision of the sanction system applicable by ANAC and private law entities.

Following the issuance of the Decree, ANAC issued Guidelines aimed primarily at providing guidance for the submission and management of external reports addressed to the Authority itself. However, these Guidelines also include interpretive and application guidelines relevant to the other institutions and protections under the Decree, which have been considered in updating this Procedure to reflect the new regulatory framework.

## 1. Objectives of the Document

This Procedure regulates the methods and related process for managing reports of unlawful conduct by employees, independent consultants or collaborators, employees or collaborators of companies, suppliers of goods and services, or entities performing work on behalf of Tecnocap S.p.A., in compliance with the Organization, Management, and Control Model under Legislative Decree No. 231/2001 adopted by the Company, and in conformity with the regulations on the protection of individuals who report violations of national provisions pursuant to Legislative Decree No. 24 of March 10, 2023.

## 2. Objectives of the Process

The aim of this document is to encourage collaboration among those working within Tecnocap S.p.A. in order to identify possible unlawful conduct relevant under Legislative Decree No. 231/2001 and/or violations of the Organization, Management, and Control Model adopted, while ensuring the protection of those who report crimes or irregularities that come to their attention in the course of their employment, as provided for by Legislative Decree No. 24/2023.

## 3. Definitions

In this Procedure, the following terms are defined as follows:

- **Tecnocap S.p.A. or Tecnocap or Company:** Tecnocap S.p.A., headquartered in Cava de' Tirreni (SA), via Starza s.n.c., registered in the Salerno Companies Registry, with Tax Code and VAT number 02865960658.
- **ANAC:** Italian National Anti-Corruption Authority.
- **Oversight Body or OdV:** the body endowed with independent powers of supervision and control, responsible for overseeing the functioning and observance of the Organization, Management, and Control Model adopted by Tecnocap S.p.A., as well as its updating.

- **Report Manager:** dedicated body for receiving reports and conducting verification and analysis of the reports received (preliminary investigation). The Report Manager is formally designated and consists of the OdV.
- **Model:** the Organization, Management, and Control Model under Article 6, paragraph 1, letter a) of Legislative Decree No. 231/2001, adopted by Tecnocap S.p.A.
- **Whistleblowing (reporting of misconduct):** the system for protecting employees or collaborators who report unlawful conduct (Article 2, paragraph 1, letter a) of Legislative Decree No. 24/2023), intended to regulate the process of reporting crimes, violations of the Model and/or the Code of Ethics, or other irregularities by an individual who becomes aware of them through their employment relationship, with specific legal protections for the whistleblower, even in cases where retaliatory or discriminatory measures are taken against them as a result of the report.
- **Whistleblowing Report:** a report submitted by a qualified individual (whistleblower) concerning unlawful conduct of which the whistleblower has become aware through their employment or collaboration relationship.
- **Unlawful Conduct:** violations defined by Article 2, paragraph 1, letter a) of Legislative Decree No. 24/2023.
- **Sensitive Activity:** an activity or area of the Company where there is a risk, even potential, of commission of crimes applicable to it and included in the list of predicate offenses under Legislative Decree No. 231/2001.
- **Instrumental Activity:** an activity or area of Tecnocap S.p.A. where financial instruments and/or substitutes are managed that may, when combined with directly sensitive activities, support the commission of one of the crimes covered by Legislative Decree No. 231/2001, thus serving as a means of commission.
- **Whistleblower (reporting person):** the person who reports, discloses, or reports to the judicial or accounting authority violations of national or European Union regulatory provisions that harm public interest or the integrity of Public Administration or a private entity, which they have become aware of in a public or private work context.

This norm includes within the notion of whistleblower both Tecnocap S.p.A. employees, independent consultants, employees of companies providing goods or services or performing work for the Company, volunteers, trainees (paid or unpaid), shareholders, and individuals in administrative, management, oversight, or representative roles, even when such roles are de facto, who report unlawful conduct, crimes, or irregularities that they have become aware of due to their work relationship. Reporting may occur:

a) when the legal relationship is ongoing; b) during a probationary period; c) when the legal relationship has not yet begun, if information about violations was obtained during the selection process or other pre-contractual stages; d) after the termination of the legal relationship, if information about violations was acquired before the relationship ended.

- **Facilitator:** an individual who assists the reporting person in the reporting process, working within the same employment context, and whose assistance must remain confidential.
- **Recipients:** individuals covered by this Procedure, including a) employees of Tecnocap S.p.A.; b) partners, suppliers, consultants, collaborators, shareholders, and, in general, anyone with an interest relationship with the Company.

- **Whistleblowing Channels:** channels adopted by Tecnocap S.p.A. for the submission and management of whistleblowing reports, published directly on Tecnocap S.p.A.'s institutional website in the dedicated "Whistleblowing" section.

#### 4. References

For the purposes of this document, the following references are considered:

- Law No. 190 of November 6, 2012, "Provisions for the prevention and suppression of corruption and illegality in Public Administration."
- Legislative Decree No. 231 of June 8, 2001, "Regulation on the administrative liability of legal entities, companies, and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of September 29, 2000."
- Legislative Decree No. 24 of March 10, 2023, "Implementation of EU Directive 2019/1937 of the European Parliament and Council, of October 23, 2019, on the protection of persons reporting breaches of Union law and provisions for the protection of persons reporting violations of national legislative provisions."
- ANAC Resolution No. 469 of June 9, 2021 (Guidelines adopted by the Authority and amended with the President's Communication of July 21, 2021): "Guideline Framework for the protection of whistleblowers reporting crimes or irregularities they became aware of in the course of their employment relationship, pursuant to Article 54-bis of Legislative Decree No. 165/2001."
- Directive (EU) 2019/1937, "Directive of the European Parliament and Council of October 23, 2019, on the 'Protection of persons reporting breaches of Union law' (published in OJ L 305, 26.11.2019, pp. 17–56)."
- EU Regulation 2016/679 of the European Parliament and Council of April 27, 2016, on the protection of natural persons regarding personal data processing, as well as the free circulation of such data, repealing Directive 95/46/EC.
- Confindustria Guidelines: Guidelines issued by Confindustria in 2002, subsequently updated in 2004, 2008, 2014, 2021, and 2023. These Guidelines provide associations and companies with methodological guidance on how to build an appropriate Model to prevent offenses and serve as a defense against liability and penalties provided for by Legislative Decree No. 231/2001.

#### 5. Phases

##### 5.1 Definition of Scope: 'Object' and 'Requirements' of the Report

The subject of a report includes unlawful conduct, which encompasses various offenses such as criminal, civil, and administrative violations, irregularities in management or organization activities of Tecnocap S.p.A. to the extent that such irregularities are indicative of breaches of the Model and/or the Code of Ethics.

Generally, unlawful conduct subject to protection includes:

- Behavior, acts, or omissions harming public interest or the integrity of Public Administration, which consist of administrative, accounting, civil, or criminal offenses that are not included in items 3), 4), 5), and 6) of Art. 2, paragraph 1, of Legislative Decree No. 24/2023.
- Cases related to Sensitive Activities identified in the Model, where conduct is carried out in the interest or for the benefit of the Entity, as well as all conduct relevant under Legislative Decree No. 231/2001.
- Offenses within the scope of EU or national acts listed in the annex to Legislative Decree No. 24/2023, or national acts that implement EU acts listed in the annex to Directive (EU) 2019/1937, though not specified in the annex to Legislative Decree No. 24/2023, covering sectors like public procurement, financial services, product and market safety, environmental protection, nuclear safety, food safety, public health, consumer protection, privacy protection, and network and information system security.
- Acts or omissions harming the financial interests of the European Union under Article 325 of the Treaty on the Functioning of the European Union (TFEU), as specified in relevant EU secondary legislation.
- Acts or omissions concerning the internal market under Article 26, paragraph 2, of the TFEU, including violations of EU competition rules, State aid rules, and tax evasion schemes aimed at obtaining a fiscal advantage undermining the objective of the applicable tax regulations.

There is no exhaustive list of unlawful conduct, offenses, or irregularities that may constitute the subject of whistleblowing. Examples include:

- Violations of the Model
- Violations of the Code of Ethics and codes of conduct
- Repeated failure to meet administrative deadlines
- Accounting irregularities
- False declarations
- False certifications
- Violations of environmental, workplace safety, and control regulations
- Violations of internal or external personnel hiring procedures
- Violations of procurement regulations
- Actions that could damage the Company's reputation
- Abuse of power
- Illegitimate appointments or nominations
- Conflicts of interest
- Mismanagement of any public resources and potential financial harm.

Reported unlawful conduct must concern situations, facts, or circumstances that the reporter became directly aware of due to the employment or collaboration relationship, which may include information obtained by virtue of their office or knowledge acquired incidentally through work responsibilities.

It is not necessary for the employee or external collaborator to be certain of the occurrence or the perpetrators of the reported events. A reasonable suspicion, based on their knowledge, that an "unlawful" event as described above has occurred, is sufficient.

In this context, it is advisable that reports are as detailed as possible, providing sufficient elements to allow the administration to carry out necessary verifications, as indicated in paragraph 5.2 below.

Reports based on mere suspicions, rumors, or knowingly false information are not eligible for protection, as it is essential to consider the interests of third parties named in the report and avoid inefficient or costly internal inspections. Likewise, protection does not apply to disclosures of information that is already entirely public or to baseless news and rumors. This protection also does not extend to employees who violate the law to collect information, clues, or evidence of wrongdoing in the workplace.

The report must aim to safeguard Tecnocap S.p.A.'s integrity. Thus, the reported incident must show elements indicating an injury, obstacle, or alteration of the correct and impartial conduct of an activity or service, including the Company's reputation.

## **5.2 Scope Definition: Content of the Report**

The whistleblower should provide all relevant details to facilitate appropriate verification of the facts reported. The report should clearly include the following essential elements: a) Identification of the reporting individual, including their position or role within the organization; b) A clear and complete description of the reported facts; c) Time and place circumstances of the reported facts; d) Identification information for individuals involved or responsible for the reported facts; e) Details of other individuals who can corroborate the reported facts; f) Reference to any documents that may substantiate these facts; g) Any other information that may confirm the reported facts.

Tecnocap S.p.A. provides whistleblowing channels enabling the submission of comprehensive reports in compliance with ANAC and Confindustria Guidelines.

The whistleblower's identity and the content of the report are protected under Legislative Decree No. 24/2023, including anonymous reports, with the same protections as identifiable reporters.

## **5.3 Forms of Whistleblower Protection**

### **A) Protection of the Whistleblower's Identity and Report Confidentiality**

Tecnocap S.p.A. must ensure confidentiality of the whistleblower's identity and all elements of the report. Confidentiality is especially strict when the whistleblower's identity is known. Measures include:

- Confidentiality requirements for report handlers, the Report Manager, and IT experts (e.g., system administrators).
- Adoption of an internal reporting channel ensuring confidentiality.
- When the report is forwarded to third parties, such as the Judiciary, whistleblowers are informed in advance.
- GDPR (679/2016) rights (Articles 15-22) are limited for the reported individual if these rights compromise the confidentiality of the whistleblower's identity.
- Breach of confidentiality obligations by report handlers and IT experts can result in disciplinary action and other liabilities.

The whistleblower's identity is protected except in cases of slander, defamation, civil liability, or where anonymity is legally non-opposable.

## **B) Protection from Retaliation or Discriminatory Measures**

No form of retaliation or discrimination against the whistleblower is allowed for reports made under this Procedure, including direct or indirect actions affecting work conditions due to the report.

Retaliatory or discriminatory measures include sanctions, demotions, dismissals, transfers, and any other actions or omissions that could have a retaliatory effect.

An employee alleging discrimination or retaliation due to a report may communicate it to ANAC, which verifies if retaliation is related to the report and, in the absence of proof from Tecnocap S.p.A. showing that the measure was unrelated to the report, may impose an administrative fine. Retaliatory or discriminatory acts taken against the whistleblower by the Company are null.

A reversal of the burden of proof is established (Art. 17 of Legislative Decree No. 24/2023), where the party imposing a measure must prove that it was motivated by reasons unrelated to the report.

## **C) Extension of Protection**

Protective measures also apply to:

- The facilitator, who, as an individual, assists the whistleblower in the reporting process and operates within the same work context, with the requirement that this assistance remains confidential;
- Individuals within the same work context as the whistleblower, the person who submitted a report, or the person who made a public disclosure, who have a stable, close emotional or family relationship (up to the fourth degree) with them;
- Colleagues of the whistleblower or the person who submitted a report or made a public disclosure, working in the same work context and having a regular and ongoing relationship with that person;
- Entities owned by the whistleblower or the person who submitted a report to the Judicial or Accounting Authority or made a public disclosure, or where these individuals work, as well as entities operating in the same work context.

## **D) Protection of Whistleblowers for Disclosure on Just Grounds of Confidential Information**

The whistleblower is also protected in cases where they disclose, for just cause, information or facts covered by official, corporate, or professional secrecy, or if they breach a duty of loyalty. In such cases, an exemption clause is established from liability for the offenses covered in Articles 326, 622, and 623 of the Criminal Code. This protection is granted if the whistleblower acts to safeguard the integrity of Tecnocap S.p.A. In summary, the disclosure must solely aim to reveal actions, acts, or omissions that harm public interest or the integrity of the company and not for other purposes (e.g., vindictive or opportunistic motives).

## **E) Conditions for Protection and Whistleblower Responsibilities**

Protection of the whistleblower as outlined in points A), B), and C) does not apply in cases where the report contains false information provided with intent or negligence. Consequently, the protection established by this Procedure and applicable national regulations is not guaranteed to the whistleblower if their criminal or civil liability is determined in cases of slanderous or defamatory reporting under the Criminal Code and Article 2043 of the Civil Code, which states, “any intentional or negligent act that causes unjust harm to another obligates the offender to compensate for the damage.” Disciplinary or other relevant proceedings may also arise in cases of abuse of this Procedure, such as reports that are clearly opportunistic and/or solely intended to harm the reported party or others, or if it is found that the whistleblower knowingly disclosed false information (i.e., a ‘malicious report’) or used the Procedure improperly.

## **5.4 The Process of Managing Reports**

### **5.4.1 Submitting an Internal Report: Reporting Channels**

The internal report can be submitted by the whistleblower to the Supervisory Body (OdV) of Tecnocap S.p.A., Avv. Daniela Rocchi (the sole recipient of reports), with the guarantees associated with whistleblower protection according to the provisions of this Procedure. Reports can be submitted as follows:

1. *Postal Submission:* The report is enclosed in two sealed envelopes, with the whistleblower’s identification details and a form of ID in the first envelope, and the report’s content in the second. Both envelopes should then be placed in a third sealed envelope marked “confidential/personal for OdV” and sent via post to Avv. Daniela Rocchi, via Tevere, n. 46 - 00198, Rome.
2. *Email Submission:* To the OdV’s email address, Avv. Daniela Rocchi at [d.rocchi@rpcpenalisti.it](mailto:d.rocchi@rpcpenalisti.it).

For reporting, a form for reporting unlawful conduct is available per Legislative Decree of March 10, 2023, No. 24, on Tecnocap's official website in the Whistleblowing section. Reports received through these means are logged and recorded in a confidential registry by the Report Manager.

Should a report be received by an individual other than the OdV (e.g., a direct supervisor, manager, etc.), the recipient must inform the sender that the report should be sent to the OdV of Tecnocap S.p.A., and forward the report to the OdV within seven days of receipt.

If the whistleblower is a public official, sending the report to the aforementioned individuals does not exempt them from the duty to report criminally relevant facts or cases of financial damage to the appropriate Judicial Authority.

### **5.4.2 Acquiring the Internal Report and Preliminary Examination**

Reports submitted by the whistleblower are acquired by the OdV through whistleblowing channels and are subject to a preliminary review within fifteen days from the date of receipt. The OdV is responsible for the analysis and verification of received reports as the report’s administrative user. During the preliminary examination, the OdV conducts an initial assessment to determine whether the report qualifies as whistleblowing.

Internal whistleblowing channels are designed to ensure the confidentiality of the whistleblower's identity and the content of the report and related documentation. For this purpose, the administrative user accesses the received report and manages its receipt, preliminary review, and investigative phase.

Reports received through channels other than the internal reporting channels established by the company are evaluated by the OdV for competence and managed accordingly. Similarly, reports are subject to a preliminary examination as indicated above.

To ensure confidentiality of the whistleblower's identity, the content of the report, and related documentation regarding reports received through the aforementioned internal channels, access to the documentation of received reports and investigations is restricted to the OdV.

### **5.4.3 Investigative Phase**

This procedural phase follows the submission of the report:

- Within seven days of submission, the designated person must issue an acknowledgment of receipt to the whistleblower and, if necessary, request additional information;
- Within three months from the date of acknowledgment of receipt, a response must be provided to the whistleblower;
- A report submitted to an incompetent party must be forwarded to the correct recipient within seven days.

Once the preliminary review is complete, the investigative phase begins within fifteen working days from the date of receipt of the report. The investigation must be concluded within sixty days from the start date.

During the investigation phase, the OdV verifies and analyzes the received reports, specifically:

- Evaluating the presence of essential requirements concerning the whistleblower and the content of the report (see sections 5.1 and 5.2);
- Verifying the validity of the reported circumstances impartially and confidentially, performing any necessary actions. The investigation consists of document review and analysis rather than verification of the actual occurrence of reported events;
- Engaging in dialogue with the whistleblower, if necessary, to obtain clarifications, documents, or additional information;
- Requesting additional information from any other parties who can provide insight into the reported events. For this purpose, relevant department heads and anyone able to contribute to the review may be consulted;
- Utilizing, if necessary, the assistance of relevant departments and/or competent professionals external to the company, depending on the subject matter of the report.

If, following the investigation, the OdV:

- Finds evidence of clear and manifest lack of grounds, the report is filed with adequate justification.

- Finds credible elements in the reported facts, the OdV immediately contacts the relevant internal bodies or external entities/institutions to Tecnocap S.p.A. to conduct investigations on the reported facts, each according to its area of expertise. The OdV is not responsible for determining individual accountability or conducting legitimacy or merit assessments of the company's acts and measures being reported, as this would risk infringing on the roles of designated company entities or judicial authorities.

In transmitting reports to third parties, the confidentiality of the whistleblower will always be protected. All investigative activities conducted and their respective outcomes must be thoroughly documented, especially in regard to the decisions made.

#### **5.4.4. Submitting an External Report**

Articles 6 and 7 of Legislative Decree no. 24/2023 regulate the conditions and methods by which the whistleblower may initiate an external report under any of the following circumstances:

- if in the specific work context, the activation of an internal reporting channel is not mandatory, or if the channel is inactive or not designed in accordance with regulatory requirements;
- if the whistleblower has already submitted an internal report, but it has not been acted upon or concluded with a final negative outcome;
- if the whistleblower has reasonable grounds to believe that, if they were to make an internal report, it would not be effectively followed up on (e.g., if the ultimate authority in their work context is involved in the violation), or if making such a report could present a risk of retaliation;
- if the whistleblower has reasonable grounds to believe that the violation in question may pose an imminent or clear danger to the public interest.

An additional case for external reporting occurs if the supervisory body (OdV) responsible for managing the report faces a conflict of interest regarding a specific report, as either the subject or the reporter. In the first instance, the OdV notifies the whistleblower to file an external report with ANAC; in the second instance, the OdV itself proceeds accordingly.

The procedures for external reporting to ANAC are defined by ANAC and published on their website, [www.anticorruzione.it](http://www.anticorruzione.it), in a dedicated, easily identifiable, and accessible section. This website provides information including:

- an explanation of whistleblower protection measures;
- ANAC contact details (phone number, mailing address, and email, both standard and certified) for submitting an external report;
- instructions for using the external reporting channel;
- guidance on how ANAC may request further information from the whistleblower, the deadlines for responding to an external report, and the types of responses ANAC may provide to an external report.

#### **5.4.5. Public Disclosures**

Another reporting option is outlined in Article 15 of Legislative Decree no. 24/2023, quoted in full as follows: "1. The whistleblower who makes a public disclosure benefits from the protection provided by this decree if, at the time of the public disclosure, any of the following conditions apply: a) the whistleblower has previously made an internal and external report, or has directly made an external report under the conditions and methods stipulated by Articles 4 and 7, and has received no response within the timeframe established by Articles 5 and 8 regarding the measures planned or implemented to address the report; b) the whistleblower has reasonable grounds to believe that the violation may pose an imminent or clear danger to the public interest; c) the whistleblower has reasonable grounds to believe that making an external report could result in a risk of retaliation or may not be effectively followed up on, due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a reasonable fear that the recipient of the report may be complicit with the violator or involved in the violation itself. 2. The regulations on journalistic professional secrecy regarding the news source remain unaffected."

The whistleblower will benefit from the same protective measures provided by Legislative Decree no. 24/2023, which forms an integral part of this Procedure for the use of the internal/external channel, only if:

- they have previously made an internal or external report and received no response within the stipulated timeframe;
- they have reasonable grounds to believe that the violation could pose an imminent or clear danger to the public interest;
- they have reasonable grounds to believe that making an external report could present a risk of retaliation or may not be effectively followed up on, given the specific circumstances of the case, such as where evidence might be concealed or destroyed, or where there is a reasonable fear that the recipient may be complicit with or involved in the violation.

#### **5.4.6. Personal Data Processing**

All personal data contained within the report, as well as data collected or obtained during the process, will be processed in compliance with data protection laws, specifically Regulation EU 679/2016 (GDPR) and company policies on data processing.

In accordance with Article 13, paragraph 2 of Legislative Decree no. 24/2023, it is established that personal data that are clearly not relevant to the processing of a specific report will not be collected, or if collected accidentally, will be immediately deleted.

The “Whistleblowing” section on the official website of Tecnocap S.p.A., where this Procedure is published, also contains the privacy notice pursuant to Article 13 of the aforementioned EU Regulation.

Violations of the obligations provided in this Procedure constitute disciplinary infractions for non-compliance with service directives, without prejudice to the possibility of more severe disciplinary actions for serious violations.

All documentation related to each report, whether in paper or electronic format, must be adequately archived and maintained by the OdV for a period of five years from the date on which the whistleblower is informed of the outcome of the handling and processing of the report, except in cases where applicable regulations allow for a longer retention period.