POLICY WHISTLEBLOWING

AI SENSI DEL D.LGS. 24/2023

1. PURPOSE OF THE DOCUMENT

This policy defines the procedure of ROTAIR S.p.a. to be followed for reporting suspected wrongful conduct or suspected illicit acts or alleged violations (so-called whistleblowing), in accordance with Legislative Decree March 10, 2023, No. 24, implementing Directive (EU) 2019/1937 of the European Parliament and of the Council, of October 23, 2019, concerning the protection of persons who report violations of Union law and containing provisions on the protection of persons who report violations of national legislative provisions.

The objective is to provide clear operational guidelines to whistleblowers regarding the subject, content, recipients, and methods of transmitting reports, as well as the forms of protection offered in our legal system, removing factors that may discourage or hinder the use of reports (such as doubts and uncertainties about the procedures to follow and fears of retaliation or discrimination).

2. DEFINITIONS

For the purposes of this procedure, the following terms are defined as:

- "violations": behaviors, acts, or omissions that harm public interest or the integrity of the Company;
- "information on violations": information, including well-founded suspicions, concerning violations committed or that, based on concrete elements, may be committed within the Company, as well as elements regarding conduct aimed at concealing such violations;
- "report" or "reporting": the communication, written or oral, of information on violations;
- "internal report": the communication, written or oral, of information on violations, submitted through the internal reporting channel established by the Company;
- "external report": the communication, written or oral, of information on violations, submitted through the external reporting channel established by the National Anti-Corruption Authority (ANAC);
- "public disclosure" or "disclose publicly": making information on violations public through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people;
- "anonymous report": a report from which the identity of the reporting person cannot be derived;
- "reporting person" (whistleblower): the natural person who reports information on violations acquired in the context of their work;
- "facilitator": a natural person who assists a reporting person in the reporting process, operating within the same work context, and whose assistance must be kept confidential;
- "work context": work or professional activities, present or past, through which, regardless of the nature of such activities, a person acquires information on violations and within which they may risk retaliation in case of reporting or public disclosure or reporting to the Judicial or Accounting Authority;
- "reported person or involved person": the 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;
- "retaliation": any behavior, act, or omission, even only attempted or threatened, carried out due to the report, reporting to the Judicial or Accounting Authority, or public disclosure and that causes or can cause unjust harm to the reporting person or the person who made the report, directly or indirectly;
- "follow-up": the set of actions taken within the framework of the reporting channel management to assess the existence of the reported facts, the outcome of the analyses, and any measures to be taken;
- "feedback": communication to the reporting person of information related to the follow-up or feedback that is given or intended to be given to the report.

3. TYPES OF REPORTING

Those wishing to report relevant facts or behaviors under Legislative Decree No. 24/2023 can do so by:

- using the internal reporting channel established by the Company and described in Chapter 4;
- using the external reporting channel managed by ANAC (National Anti-Corruption Authority);
- through public disclosure through the press, electronic means, or means of dissemination capable of reaching a large number of people.

In addition to the above-mentioned reporting methods, it is always possible for the individual wishing to make a report to directly contact the Judicial or Accounting Authority by filing a complaint regarding relevant facts or behaviors of which they have become aware. The use of the internal channel MUST be favored as a priority.

A. External Reporting Channel managed by ANAC

The reporting person can make a report using the external reporting channel established for this purpose by ANAC [National Anti-Corruption Authority] in cases where one of the following conditions occurs:

- an internal report has been made, which, however, has not been followed up. This refers to cases where the internal channel has been used, but the party responsible for managing the channel has not taken any action within the time limits prescribed by law regarding the admissibility of the report, the verification of the existence of the reported facts, or the communication of the outcome of the internal analyses conducted. It is important to clarify, therefore, that "having a follow-up" does not mean that the expectations of the reporting person, in terms of the result of the report, must necessarily be satisfied;
- the reporting person, based on concrete circumstances and information that can be effectively obtained, and therefore not on mere speculation, has good reason to believe that, if they were to make an internal report, it would not be effectively followed up or would result in retaliatory conduct;
- the reporting person has good reason to believe that the violation may constitute an imminent or obvious danger to public interest. This refers, for example, to cases where the violation clearly requires urgent intervention by a public authority to safeguard an interest that belongs to the community, such as health, safety, or environmental protection.

The external reporting channel, like the internal channel, ensures the confidentiality of the identity of the reporting person, the involved person, and the person mentioned in the report, as well as the content of the report and related documentation.

B. Public disclosure

Without prejudice to the priority access to the internal reporting channel and the principle of good faith underlying the report, the reporting person can make a public disclosure through the press, electronic means, or means of dissemination capable of reaching a large number of people, in cases where one of the following conditions occurs:

- the reporting person has already made an internal and/or external report, or directly an external report, and no feedback has been provided within the prescribed time regarding the measures planned or taken to follow up on it;
- the reporting person has good reason to believe that the violation may constitute an imminent or obvious danger to public interest (consider, for example, a situation of emergency or the risk of irreversible damage, including to the physical well-being of one or more persons, which requires that the violation be promptly revealed and have a broad impact to prevent its effects);
- the reporting person has good reason to believe that the external report may carry the risk of retaliation or may not be effectively followed up due to the circumstances of the specific case, such as those where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the report may be colluding with the author of the violation or involved in it (consider, for example, the case where the recipient of the report of a violation, by agreeing with the person involved in the violation, does not follow up on said report in the absence of prerequisites).

4. INTERNAL REPROTING CHANNLE

4.1. Subject of the report

Reports can concern suspected improper conduct, illicit acts, or alleged violations, including:

- Administrative, accounting, civil, or criminal offenses;
- Unlawful actions as defined by Legislative Decree No. 231 of June 8, 2001;
- Violations of EU law;
- Violations of European regulations on public procurement, services, products, financial markets, prevention of money laundering and terrorism financing, safety and compliance of products, transportation safety, environmental protection, radiation protection, nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, privacy, and personal data protection, network and information system security;
- Violations of competition and state aid regulations, as well as violations related to the internal market involving acts that violate corporate tax rules or mechanisms aimed at obtaining a tax advantage that undermines the purpose or intent of applicable corporate tax regulations;
- Acts or behaviors undermining the purpose or intent of EU regulations in the aforementioned sectors.

Reports must meet the following requirements:

- Be made in good faith;
- Be detailed and based on precise and consistent factual elements;
- Relate to verifiable facts directly known by the reporting party;
- Contain all necessary information to identify the authors of the reported facts and any information useful to describe the subject of the report.

Forms of "abuse" such as manifestly unfounded reports, opportunistic reports, or reports made solely to harm the reported party, and any other improper or instrumental use of the reporting mechanism are prohibited, not considered, and may result in sanctions and/or actions before the Judicial Authority. In cases of malicious or defamatory reports, the reporting party may be called to answer for them in criminal proceedings, and a disciplinary proceeding may be initiated against them.

The following reports are not relevant and are considered unenforceable:

- Those related to personal matters concerning claims or complaints regarding relationships with colleagues;
- Those with offensive tones or containing personal insults or moral judgments aimed at offending or harming the personal and/or professional honor or dignity of the person or persons to whom the reported facts refer;
- Those based on mere suspicions or rumors regarding personal matters not constituting an offense;
- Those related to information already in the public domain;
- Those with purely defamatory or malicious purposes;
- Those of a discriminatory nature, relating to sexual, religious, and political orientations or the racial or ethnic origin of the reported party.

It is necessary for the report to be as detailed as possible. In particular, the following should be clear:

- The circumstances of time and place in which the reported incident occurred;
- The description of the incident;
- The particulars or other elements that allow the identification of the subject to whom the reported facts should be attributed.

It is also useful to attach documents that can provide evidence of the reported facts, as well as information about other individuals potentially aware of the facts.

4.2. Reporting parties

Reports concerning violations known within the context of work or collaboration with the Company can be made by:

- Employees;
- Freelancers and collaborators performing their work at the Company or providing goods and services;
- Freelancers and consultants;
- Interns, whether paid or unpaid;
-

- Shareholders and individuals with functions of administration, management, control, supervision, or representation.

Reports may concern facts or circumstances of which the reporting party became aware:

- While the employment or collaboration relationship is ongoing;
- Before the employment or collaboration relationship has started, if information about violations was acquired during the selection process or in other pre-contractual phases;
- During the probationary period;
- After the termination of the employment or collaboration relationship if information about violations was acquired during the relationship itself.

Reporting parties are ensured adequate protections as described in Chapter 6.

4.3. Reporting modalities

To ensure the effectiveness of the reporting process and provide broad and indiscriminate access to all those who want to make a report, Rotair S.p.a. provides alternative channels, specifically:

- WRITTEN reporting through an online platform accessible at the link https://rotairspa.trusty.report/

- ORAL reporting through a direct meeting scheduled within a reasonable period of 10 days. The request is to be sent to one or both of the following email addresses: l.donadio@rotairspa.com and/or l.degiovanni@rotairspa.com, accessible to the Reporting Managers, identified as Lorella Donadio and Luca Degiovanni. In these cases, with the prior consent of the reporting person, the report is documented by the Reporting Manager through recording on a device suitable for preservation and listening or by minutes. In the case of minutes, the reporting person can verify, rectify, and confirm the minutes of the meeting by their own signature.

Although anonymous reports are a viable alternative, the Company suggests reporters prefer nominative ones for the sake of the speed and effectiveness of investigations. Anonymous reports, i.e., those lacking elements to identify the author, even if delivered through the methods described above, will be treated as ordinary reports and will be processed outside the regulations dictated by Legislative Decree No. 24/2023.

The management of the internal reporting channel is entrusted to the Reporting Manager defined in the following chapter.

It is not uncommon to receive reports through channels other than the official ones mentioned above (e.g., anonymous letters sent to the attention of Management and Corporate Leadership). Any employee who receives a report outside of official channels has the responsibility and moral duty to forward it, within seven days of receipt, to the Reporting Manager (Lorella Donadio or Luca Degiovanni), giving simultaneous notice of the transmission to the reporting person.

If the designated manager is in a conflict of interest situation regarding a specific report (as the reported party or reporting party), one of the conditions for making an external report to ANAC applies (see Chapter 3).

5. MANAGEMENT OF REPORTS

Rotair S.p.a. has entrusted the management of the internal reporting channel to an autonomous Committee (hereinafter referred to as the Manager) composed of specifically trained personnel: Mrs. Lorella Donadio and Mr. Luca Degiovanni. The designated individuals ensure maximum confidentiality, data protection, and privacy.

In particular, the Manager accesses the platform channel once a report is received. The Reporting Manager generally performs the following activities:

- The reporter is issued an acknowledgment of receipt of the report within 7 days of the date of receipt. It is emphasized that this acknowledgment does not imply any evaluation of the content of the report but is solely intended to inform the reporter of the correct receipt of the report. This notice must be sent to the address indicated by the reporter in the report. In the absence of such indication and, therefore, the inability to interact with the reporter for follow-ups, the report may be considered unmanageable under whistleblowing regulations (with a record of this reason) and possibly treated as an ordinary report.
- Ongoing communication is maintained with the reporting person, who may be asked for additional information if necessary.
- Diligent follow-up is given to the received reports, in accordance with the principles of confidentiality, timeliness, and impartiality, evaluating the received report and conducting necessary checks to ascertain if a violation has actually occurred.
- Feedback is provided to the reporter within 3 months from the date of the acknowledgment of receipt or, in the absence of this acknowledgment, within 3 months from the expiration of the 7-day period from the report submission.

In the preliminary phase, the Reporting Manager evaluates, including any document analysis:

- The initiation of the subsequent investigation phase;
- The closure of Reports, as they may be:
    - Generic or inadequately detailed
    - Clearly unfounded;
- Related to facts and/or circumstances that have been the subject of specific investigative activities in the past, where preliminary checks do not reveal new information requiring further investigation;
- "Detailed and verifiable," for which, based on the results of preliminary checks, no elements supporting the initiation of the subsequent investigation phase emerge;
- "Detailed and non-verifiable," for which, based on the results of preliminary checks, it is not possible, using the available analysis tools, to conduct further investigations to verify the validity of the Report.

If the report is found to be unmanageable or inadmissible, i.e., to be closed, the Reporting Manager proceeds with archiving, ensuring traceability of the supporting reasons. One of the two individuals serving as the Manager during preliminary checks may act as a coordinator for report management.

The investigative phase aims to:

- Conduct in-depth and specific analyses to verify the reasonable validity of the reported factual circumstances;
- Reconstruct the managerial and decision-making processes based on the documentation and evidence made available;
- Provide any indications regarding the adoption of necessary remedial actions to correct possible control deficiencies, anomalies, or irregularities identified in the examined areas and business processes.

During the investigations, the Reporting Manager may request additional information or clarifications from the Reporter. If deemed useful for the investigations, the Reporting Manager may obtain information from individuals involved in the Report, who also have the right to request to be heard or to submit written observations or documents. In such cases, and to ensure the right to defense, notice is given to the involved person of the existence of the Report, while maintaining confidentiality regarding the identity of the Reporter and other persons involved and/or mentioned in the Report.

The objective of the verification phase is to proceed with specific checks, analyses, and evaluations regarding the validity of the reported facts, also with a view to formulating any recommendations regarding the adoption of necessary corrective actions in the areas and business processes involved, aiming to strengthen the internal control system.

The individuals responsible for managing the reports must ensure the necessary verifications, including but not limited to:

- Directly acquiring the necessary information for evaluations through the analysis of received documentation/information;

- Involving other company structures or specialized external entities, taking into account the specific technical and professional competencies required;
- Hearing any internal/external subjects, etc.

This investigative and verification activity is exclusively the responsibility of the Reporting Manager, including all activities necessary to follow up on the report (such as hearings or document acquisitions).

If it is necessary to enlist the technical assistance of third-party professionals or the specialist support of personnel from other company functions/directorates, it is necessary to obscure any type of data that could allow the identification of the reporting person or any other involved person, in order to comply with confidentiality obligations required by regulations.

If the involvement of internal subjects other than the Manager (other company functions) is necessary, they will also be subject to the confidentiality obligations expressly provided in this Whistleblowing Procedure.

Once the verification activity is completed, the Reporting Manager can:

- Archive the report because it is unfounded, providing the reasons;
- Declare the report founded and refer to the competent internal bodies/functions for the relevant follow-ups. In fact, the Reporting Manager has no role in assessing individual responsibilities and any subsequent measures or proceedings.

All phases of the verification activity must be correctly traced and archived to demonstrate the correct diligence in following up on the report.

The Reporting Manager must provide feedback to the reporter within three months from the date of the receipt acknowledgment or - in the absence of this acknowledgment - within three months from the date of the expiration of the seven-day deadline for this notice. In this regard, it is important to specify that it is not necessary to conclude the verification activity within three months, considering that there may be cases that require more time for verifications. Therefore, this feedback, at the end of the indicated period, can be final if the investigation is complete or interim in nature regarding the progress of the investigation, not yet concluded.

Therefore, at the end of the three months, the Reporting Manager can communicate to the reporter:

- The archive of the report, providing the reasons;
- The confirmation of the validity of the report and its transmission to the competent internal bodies;
- The activity carried out up to this moment and/or the activity that it intends to carry out.

In the latter case, it is advisable to also communicate to the reporting person the subsequent final outcome of the report investigation (archive or confirmation of the validity of the report with transmission to the competent bodies).

Reports received, related verifications and analyses, and all reference documentation are kept for the time necessary for processing the report and in any case, not exceeding 5 years from the date of the communication of the final outcome of the reporting procedure, in compliance with confidentiality obligations.

6. GUARANTEES AND PROTECTIONS

The Legislative Decree 24/2023 has introduced safeguards to protect whistleblowers, extending these protections to individuals other than the whistleblower who might, however, be subject to retaliation, even indirectly, due to their role in the reporting, public disclosure, or denunciation process and/or their particular relationship with the whistleblower or reporter, specifically:

- Facilitators;
- Individuals in the same work context as the whistleblower, the person reporting to the Judicial or Accounting Authority, or the one making a public disclosure, who are connected to them by a stable emotional or familial relationship within the fourth degree;

- Colleagues of the whistleblower or the person reporting to the Judicial or Accounting Authority or making a public disclosure, working in the same professional environment and having a regular and ongoing relationship with the mentioned person;
- Entities owned by the whistleblower or the person reporting to the Judicial or Accounting Authority or making a public disclosure, as well as entities operating in the same professional context as the aforementioned individuals.

6.1. Whistleblower protection

A. Protection of whistleblower's identity

The whistleblower's identity and any other information directly or indirectly revealing their identity cannot be disclosed without the explicit consent of the whistleblower to individuals other than those competent to receive or follow up on the reports. This protection extends to any other information or element of the report, including attached documentation, from which the whistleblower's identity can be directly or indirectly inferred. It includes ensuring confidentiality throughout all stages of the reporting process, including the potential transfer of reports to other competent authorities.

For reports transmitted through the computer platform, the confidentiality of the whistleblower's identity (as well as the content of the report) is protected as follows:

- The platform is provided by a specialized entity, third-party, and independent of Rotair S.p.A.;
- The platform adopts a "no-log" policy, meaning it does not record, in any way, direct or indirect information about the connection methods (e.g., servers, IP addresses, MAC addresses), ensuring complete anonymity in access. This particularly means that corporate IT systems cannot identify the access point to the portal (IP address), even if access is made from a computer connected to the corporate network;
- The platform ensures high security standards, employing encryption algorithms and other methods of protection against unauthorized access.

For reports transmitted through email channels, the confidentiality of the whistleblower's identity (as well as the content of the report) is protected as follows:

- The whistleblower can write to the Committee established as the Reporting Manager, at the email address of Lorella Donadio and/or the email address of Mr. Luca Degiovanni. The meeting will be managed by the Committee formed by the two individuals, as described above.

As the Data Controller, Rotair S.p.A. guarantees the adoption of adequate technical and organizational measures to ensure that the processing of personal data is carried out in compliance with the privacy regulations in force.

In the context of the disciplinary proceedings initiated by the Company against the alleged perpetrator of the reported conduct, the whistleblower's identity cannot be revealed if the disciplinary charge is based on separate and additional findings from the report, even if stemming from it.

If, however, the charge is based, in whole or in part, on the report, and the whistleblower's identity is essential for the defense of the subject accused of the disciplinary charge or the person otherwise involved in the report, it can only be used in the disciplinary proceeding with the express consent of the whistleblower to disclose their identity.

In such cases, the whistleblower is given prior notice in writing of the reasons necessitating the disclosure of confidential data. If the whistleblower refuses consent, the report cannot be used in the disciplinary proceeding, which, therefore, cannot be initiated or continued in the absence of additional elements on which to base the charge.

B. Protection of whistleblower from retaliation or discrimination

Rotair S.p.A. prohibits all forms of retaliation, defined as "any behavior, act, or omission, even merely attempted or threatened, carried out due to the report, the denunciation to the judicial or accounting authority, or public disclosure,

which directly or indirectly causes or can cause unjust harm to the whistleblower or the person who filed the report." Retaliations include, but are not limited to:

- Termination, suspension, or equivalent measures;
- Demotion or failure to promote;
- Change of duties, workplace relocation, salary reduction, modification of working hours;
- Suspension of training or any restriction on access to it;
- Negative commendations or references;
- Imposition of disciplinary measures or other sanctions, including pecuniary ones;
- Coercion, intimidation, harassment, or ostracism;
- Discrimination or any unfavorable treatment;
- Non-conversion of a fixed-term employment contract into an indefinite-term contract, where the worker had a legitimate expectation of such conversion;
- Non-renewal or early termination of a fixed-term employment contract;
- Damages, including to the person's reputation, particularly on social media, or economic and financial prejudices, including loss of economic opportunities and income;
- Early termination or cancellation of a contract for the supply of goods or services;
- Cancellation of a license or permit;
- Request for psychiatric or medical examination.

For the protection to apply:

- There must be a reasonable belief that the reported violations, disclosures, or denunciations are truthful and within the objective scope of application of the decree.
- The report or public disclosure must be made in accordance with the provisions of Legislative Decree 24/2023.
- There must be a consequential relationship between the report, disclosure, and denunciation made and the retaliatory measures suffered.

Protection against retaliation is not guaranteed when the whistleblower is criminally liable, even at the first-instance judgment, for the offenses of defamation or slander or the same offenses committed with the denunciation to the judicial or accounting authority, or their civil liability for the same title, in cases of willful misconduct or gross negligence.

C. Other protections

Another protection recognized for the whistleblower is the limitation of their liability regarding the disclosure and dissemination of certain categories of information that would otherwise expose them to criminal, civil, and administrative liabilities.

In particular, the whistleblower will not be held criminally or civilly liable for:

- Disclosure and use of official secrets (Article 326 of the Penal Code);
- Disclosure of professional secrets (Article 622 of the Penal Code);
- Disclosure of scientific and industrial secrets (Article 623 of the Penal Code);
- Violation of the duty of loyalty (Article 2105 of the Civil Code);
- Violation of provisions related to copyright protection;
- Violation of provisions related to the protection of personal data;
- Disclosure or dissemination of information about violations that harm the reputation of the involved person.

The Decree, however, imposes two conditions for the application of the aforementioned limitations of liability:

- At the time of disclosure or dissemination, there must be valid reasons to believe that the information is necessary to reveal the reported violation.

- The report must be made in compliance with the conditions specified by the Decree to benefit from protection against retaliation (valid reasons to believe the reported facts are true, the violation is reportable, and compliance with the conditions for reporting).

It should be emphasized that the limitation operates if the reasons for disclosure or dissemination are not based on mere speculation, gossip, revenge, opportunism, or sensationalism.

In any case, liability is not excluded for behaviors that:

- Are not connected to the report;
- Are not strictly necessary to reveal the violation;
- Configure an acquisition of information or access to documents in an illicit manner..

If the acquisition is configured as a crime, such as unauthorized access to a computer system or an act of computer piracy, the criminal, civil, administrative, and disciplinary responsibility of the reporting person remains intact. On the other hand, actions like extraction (copying, photographing, removal) of documents to which legal access was obtained are not punishable.

6.2. Protection of the reported party

This policy leaves the criminal and disciplinary responsibility of the whistleblower unaffected in the case of false or defamatory reporting under the criminal code and Article 2043 of the civil code.

Article 16, paragraph 3, of Legislative Decree 24/2023 establishes that protection is no longer guaranteed when the criminal responsibility of the reporting person for the crimes of defamation or slander or similar crimes committed with the report to the judicial or accounting authority is ascertained, or their civil liability, for the same reasons, in cases of gross negligence or willful misconduct. In such cases, a disciplinary sanction is imposed on the reporting or complaining person.

Forms of abuse of this policy, such as opportunistic reports made solely to harm the accused or others, and any other misuse or intentional exploitation of the institution, are also sources of responsibility in disciplinary proceedings and other competent forums.

7. DISCIPLINARY SYSTEM

The Company, for its employees, foresees and, when the conditions are met, adopts disciplinary measures against:

- Those who are responsible for any act of retaliation or discriminatory or otherwise illegitimate prejudice, directly or indirectly, against the whistleblower (or anyone who has collaborated in determining the facts of a report) for reasons connected, directly or indirectly, to the report;
- The Reported, or other parties involved in the reported facts, for established responsibilities;
- Anyone who violates the confidentiality obligations referred to in the Policy;
- Employees, as provided by law, who have made an unfounded report with gross negligence or willful misconduct.

Disciplinary measures will be proportionate to the extent and gravity of the established illicit behaviors, and for more serious cases, they may lead to the termination of the employment relationship. Regarding third parties (e.g., partners, suppliers, consultants, etc.), applicable legal remedies and actions apply.

8. PROTECTION OF PERSONAL DATA

In accordance with the minimization principle under Article 5 of Regulation (EU) No. 2016/679 (GDPR), only personal data that is relevant and necessary for the purposes of the Policy may be processed. Therefore, all personal data (of any natural person) contained in the report or otherwise collected during the investigation that is not necessary will

be deleted or anonymized. The privacy notice contains general information regarding the processing of personal data in the context of managing reports. Reports and related documentation are kept for the time necessary for the handling of the report and in any case, not beyond five years from the date of communication of the final outcome of the reporting procedure.

9. SANCTIONING POWERS OF ANAC

In accordance with Article 21 of Legislative Decree No. 24/2023, the National Anti-Corruption Authority (ANAC) imposes the following administrative pecuniary sanctions on the responsible party:

- From 10,000 to 50,000 euros when it is ascertained that the individual identified as responsible has committed retaliation;
- From 10,000 to 50,000 euros when it is ascertained that the individual identified as responsible has obstructed or attempted to obstruct the report;
- From 10,000 to 50,000 euros when it is ascertained that the individual identified as responsible has violated the obligation of confidentiality under Article 12 of Legislative Decree No. 24/2023 and described above in point 6.1.A. Sanctions applicable by the Guarantor for the protection of personal data for competence profiles based on personal data protection regulations remain in force;
- From 10,000 to 50,000 euros when it is ascertained that no reporting channels have been established; in this case, the directing body is considered responsible;
- From 10,000 to 50,000 euros when it is ascertained that procedures for the execution and management of reports have not been adopted, or that the adoption of such procedures is not in compliance with Legislative Decree No. 24/2023; in this case, the directing body is considered responsible;
- From 10,000 to 50,000 euros when it is ascertained that the activity of verification and analysis of received reports has not been carried out; in this case, the manager of the reports is considered responsible;
- From 500 to 2,500 euros, when the civil liability of the reporting person for defamation or slander in cases of gross negligence or willful misconduct is ascertained, provided that the same has not already been convicted, even in the first degree, for the crimes of defamation or slander or similar crimes committed with the report to the judicial authority.