ORGANIZING COMMITTEE OF THE SPECIAL OLPYMPICS WORLD WINTER GAMES
POLICY WHISTLEBLOWING
PURSUANT TO LEGISLATIVE DECREE 24/2023 AND LEGISLATIVE DECREE NO. 231/2001

REVISION STATUS OF THE DOCUMENT

Rev.	Date	Reason
00		First Emission

SUMMARY

1. PURPOSE OF THE DOCUMENT

The present document defines the procedure adopted by the ORGANIZING COMMITTEE OF THE SPECIAL OLYMPICS WORLD WINTER GAMES TURIN 2025 (hereinafter "Foundation"). for reports of suspected misconduct or suspected unlawful acts or alleged violations (c.d. whistleblowing), in accordance with the provisions of Legislative Decree 24/2023, concerning the protection of persons reporting infringements of Union law and containing provisions on the protection of persons reporting infringements of national legal provisions.

The objective is to provide c.d. whistleblowers with clear operational indications about the subject, contents, recipients and manners of transmission of the reports, as well as explain them the forms of protection that are offered in our system, removing factors that may discourage or hinder the use of reports (such as doubts and uncertainties about how to proceed, and fears of retaliation or discrimination).

2. DEFINITIONS

For the purposes of this procedure, it is understood as:

- «violations», any means of conduct, acts or omissions which damage the public interest or the integrity of the Foundation;
- «information on infringements»: information, including substantiated suspicions, concerning infringements committed or which, based on factual evidence, may be committed within the Foundation, as well as elements of actions taken to conceal such infringements;
- «report» or «reporting»: the communication, either written or oral, of information on infringements;
- «internal report»: the communication, either written or oral, of information on breaches, submitted through an internal reporting channel established by the Foundation;
- «external report»: the communication, either written or oral, of information on violations, submitted through the external reporting channel established by the National Anti-Corruption Authority (ANAC);
- «public disclosure» or «divulge publicly»: making information on violations publicly available through the press or electronic media or in any case by 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» (c.d. whistleblower): the natural person who reports information about infringements acquired in their work environment;
- «facilitator»: a natural person assisting a reporting person in the reporting process, operating within the same working context and whose assistance shall be kept confidential;
- «working environment»: the current or past work or professional activities through which, irrespective of the nature of those activities, a person obtains information about violations and in the context of which they could risk retaliation in case of report or public disclosure or complaint to the Judicial or Accounting Authority;
- «reported person or person involved»: the natural or legal person mentioned in the internal or external report or public disclosure as the person to whom the breach is attributed or as otherwise involved in the breach reported or disclosed publicly;
- «retaliation»: any behavior, act or omission, even if attempted or threatened, that is made as a result of the report, the complaint to the Judicial or Accounting Authority or public disclosure and that causes or may cause unfair damage, directly or indirectly, to the person who is reporting or to the person who has made the complaint;

- «follow up»: the set of actions taken in the context of the management of the reporting channel to assess whether the reported events are true, the outcome of the analyses and any action to be taken;

«feedback»: the communication to the reporting person of information related to the follow-up that is given or intended to be given to the report.

3. TYPOLOGY OF REPORTS

Those who intend to report relevant facts or behavior pursuant to Legislative Decree 24/2023 may do so by:

- using the **INTERNAL REPORTING CHANNEL** provided by the Foundation and described in Chapter 4;
- using the EXTERNAL REPORTING CHANNEL managed by ANAC (National Anti-Corruption Authority). The reporting authority may make a report using the external reporting channel established by ANAC for this purpose if one of the following conditions is met:

  - an internal report was issued, but no response was given. This refers to cases where the internal channel has been used but the entity entrusted with the management of the channel has not undertaken, within the time limits provided for by Law, any activity regarding the admissibility of the report, the verification of the occurrence of the reported facts or the communication of the results of the internal analyses carried out. It is therefore appropriate to specify that the term "follow-up" does not mean that the expectations of the reporting person, in terms of the result of the reporting, must necessarily be fulfilled;
  - the reporting person has reasonable grounds to believe that, if they report internally, on the basis of actual circumstances and information which can be acquired and therefore not on the basis of mere guesswork, the action would be ineffective or lead to retaliation;
  - the informer has reasonable grounds to believe that the breach may constitute an imminent or apparent danger to the public interest. This refers, for example, to the case where the breach clearly requires urgent action by a Public Authority to safeguard an interest that is of public concern such as health, safety or environmental protection.

  The external reporting channel, like the internal reporting channel, ensures confidentiality of the identity of the person issuing the report, the person involved and the person mentioned in the report, as well as the content of the report and its documentation.
  The report addressed to ANAC is made according to the procedures made available by the latter on its portal https://www.anticorruzione.it/-/whistleblowing.

  • through **PUBLIC DISCLOSURE** via press, electronic media or means of dissemination capable of reaching a large number of people.
  It being understood that it needs to be given priority access to the internal reporting channel and considering the principle of good faith to which the report is inspired, the whistleblower may make a public disclosure through the press, electronic means or means of dissemination capable of reaching a large number of people, where one of the following conditions is met:

- the reporting person has already made an internal and external report, namely directly external, and no response was given within the time limits on the measures planned or taken to follow up;
- the reporting person has reason to believe that the breach may constitute an imminent or obvious danger to the public interest (for example, an emergency situation or the risk of irreversible damage, including to the physical integrity of one or more persons, that require that the breach must be promptly disclosed and have a wide resonance in order to prevent its effects);

- the reporting person has reason to believe that the external reports may entail a risk of retaliation or lack of effective follow-up due to the circumstances of the particular case, such as those in which evidence may be obscured or destroyed, or where there is a reasonable fear that the person who received the report may be in cahoots with m ay be involved in the infringement (consider, for example, the case where the person receiving a report of a violation, by agreeing with the person involved in the violation itself, does not follow up on such a report in the absence of the premises).

In addition to the above mentioned reporting procedures, it is always possible for a person who wishes to make a report to contact directly the Judicial or Accounting Authority by lodging a complaint about the relevant facts or conduct of which they have come to know.

The use of the internal channel established by the Foundation and described in the following chapter **MUST** be favored as a priority channel.

4. INERNAL REPORTING CHANNEL

4.1. Subject of the report

Subject of the report might be suspected misconduct or suspected unlawful acts or alleged infringements, consisting of:

- illegal conduct relevant to the Legislative Decree 8 June 2001, No. 231, or violations of the Model of organization and management adopted by the Foundation (including violations of the Code of Ethics).

The reports shall meet the following requirements:

- be issued in good faith;
- be substantiated and based on precise and consistent factual elements;
- relate to facts that can be verified and are known directly by the reporting entity;
- contain all the information necessary to identify the perpetrators of the reported acts or conduct and any information useful for describing the subject of the report.

Forms of "abuse" such as reports manifestly unfounded, opportunistic and/or reports made with the sole purpose of damaging the reported person, and any other hypothesis of improper use or instrumental use of the reporting mechanism are prohibited, are not taken into account and may be subject to sanctions and/or actions before the Judicial Authority.

In the event of slanderous or defamatory reports, the person who has committed a malicious act may be called to account for it and disciplinary proceedings may be initiated against them.

The following reports are not relevant and should be considered as unenforceable:

- personal situations involving claims or complaints relating to relations with colleagues;
- containing offensive or personal language or moral judgments and intended to offend or damage the honor and/or the personal and/or professional decency of the person or persons to whom the reported facts relate;
- based on mere suspicions or rumors of personal facts which are not unlawful;
- related to information already in the public domain;

- with a purely defamatory or slanderous purpose;
- Discriminatory in nature, as they relate to sexual, religious and political orientations or racial or ethnic origin of the reported person.

The report must be as detailed as possible. In particular, it must be clear:

- the circumstances of time and place in which the event to which the report relates occurred;
- the description of the act;
- details or other elements that allow the identification of the person to whom the reported facts are attributed.

It is also useful to attach documents that can provide elements of substantiation of the facts reported, as well as the indication of other persons potentially aware of the facts.

4.2. Reporting persons

Reports of violations known in the context of work or collaboration with the Foundation can be issued by:

- employees and equivalent subjects such as trainees, paid and unpaid workers, workers in administration;
- self-employed persons and employees who work for the Foundation or provide goods and services;
- freelancers and consultants;
- shareholders and persons with functions of administration, management, control, supervision or representation.

The reports may relate to facts or circumstances of which the reporting person has become aware:

- when the employment or collaboration relationship is currently in force;
- when the employment or collaboration relationship had not yet commenced, whether information on breaches was acquired during the recruitment process or other pre-contractual stages;
- during the trial period;
- after the termination of the employment or collaboration if information about breaches was acquired during the relationship.

Adequate safeguards are provided for reporting persons as described in Chapter 6.

4.3. How to make a report

In order to ensure the effectiveness of the reporting process and provide broad and indiscriminate access to all those who wish to report, the Foundation provides alternative channels, specifically:

- report to the Report Manager in WRITTEN form via a computer platform (https://turin2025.trusty.report)
- report in ORAL form by a direct meeting within a reasonable period of No. 15 days. The request for a meeting should be sent to the e-mail address **avv.debernardi@avvocatozanalda.it**, or to the physical address of the Supervisory Body:

Avv. GIUSEPPE DEBERNARDI
C.so Vittorio Emanuele II, 97
10128 TORINO
Telefono 011.0379546

In such cases, the report shall be documented by the report manager either by recording it on a storage and listening device or by recording it in an oral form with the consent of the reporting person. If a minute is taken, the reporting person may verify, correct and confirm the minute of the meeting by means of their signature.
Where possible, the use of the electronic platform is preferred.

Similarly, although anonymous reports are a viable option, the Foundation suggests that informants favor to report by name, in order to speed up and make more effective investigations. Anonymous reports, that is to say without elements that allow the identification of the author, even if delivered through the above described methods, will be treated as ordinary reports and will be treated outside the legislation dictated by Legislative Decree 24/2023.

The management of the internal reporting channel is entrusted to the Reporting Manager as defined in the following chapter.
It is not unusual to receive reports through channels other than the official ones and described above (e.g. anonymous letters sent to the attention of the Management and the Foundation Executive). Any employee who should be the recipient of a report received outside official channels has the responsibility and moral duty to transmit it, within seven days from its receipt, to the manager of the reports, informing the reporting person of the transmission at the same time.

Where the manager as identified below is in a conflict of interest scenario with respect to a specific report (as reported person or reporting person) one of the conditions for making an external report to ANAC is met (see chapter 3).

5. REPORTS MANAGEMENT

The management of the internal reporting channel adopted by the Foundation is entrusted to the Supervisory Body, identified as an independent entity and with specifically trained staff. In particular, the Supervisory Body of the Foundation is composed by Lawyer Giuseppe Debernardi.

Reports received through the internal channel shall be handled with maximum confidentiality and privacy, data protection and absence of conflicts of interest. In particular, once a report is received, the report manager shall generally carry out the following activities:

- the reporter is given a reception notice of the report within 7 days from the date of receipt. It should be noted that this confirmation does not imply for the manager any assessment of the contents subject of the report, but is only intended to inform the reporter that the report has been correctly received. This notice shall be sent to the address indicated by the reporting person in the report. In the absence of such indication and, therefore, in the absence of the possibility to interact with the reporting person for follow-up, it is possible to consider the report unmanageable pursuant to the whistleblowing discipline (leaving a trace of such motivation) and, where appropriate, treat it as a regular report;
- a dialogue is maintained with the reporting person, from whom additions may be requested if necessary;

- The reports received are followed up diligently, in accordance with the principles of confidentiality, timeliness and impartiality, by assessing the report received and making the necessary checks to determine whether, on the basis of the information in possession, a breach has actually occurred;
- the report shall be followed-up within 3 months of the date of the report notice or, in the absence of such notice, within 3 months of the expiry of the 7-day period following the submission of the report.

The report manager shall first assess, including through any document analysis:

• the start of the next stage of investigation;

• the closure of the Reports, as:

- generic or not adequately substantiated;
- clearly unfounded;
- refer to facts and/or circumstances that have been the subject of specific investigations already completed in the past, where the preliminary verifications carried out do not reveal new information which would require further investigation;
- "verifiable facts" for which, in the light of the results of the preliminary verifications carried out, no elements emerge to support the start of the subsequent phase of investigation;
- "unverifiable facts" for which, in the light of the results of the preliminary verifications carried out, it is not possible, on the basis of the available analysis tools, to carry out further investigations to verify the validity of the Report.
-

In the event that the report is not applicable or inadmissible and therefore to be closed, the manager of the report must proceed to archive, ensuring the traceability of the reasons supporting his choice.

In addition, during the pre-screening process, the Manager of the report may appoint a person from among its members to act as coordinator for the management of the report.

The investigation phase of the report aims at:

- carrying out specific investigations and analyses to verify the reasonable substantiation of the reported factual circumstances;
- reconstructing the management and decision-making processes used on the basis of the documentation and evidence made available;
- providing any guidance on the implementation of necessary remedial actions to correct possible control deficiencies, anomalies or irregularities detected in the business areas and processes examined.

The Manager of the reports during the investigations may request additions or clarifications to the Reporting Person. In addition, where it is deemed useful for further information, they may obtain information from the Persons involved in the Report, who are also entitled to request a hearing or to produce written observations or documents. In such cases, also to guarantee the right of defense, the Person concerned is informed of the existence of the Report, while ensuring confidentiality on the identity of the Reporter and other persons involved and/ or mentioned in the Report.

The aim of the verification phase is that of carrying out specific verifications, analyses and assessments on whether or not the facts reported are true, also to make recommendations for the adoption of corrective actions in the business areas and processes concerned, with a view to strengthening the internal control system.

The offices or person handling reports shall ensure that the necessary checks are carried out, including but not limited to:

- directly by acquiring the information needed for assessments through analysis of the documentation/information received;
- through the involvement of other company structures or even external specialized entities in view of the specific technical and professional skills required;
- hearing of any internal/external parties, etc.

This investigation and verification activity are the exclusive responsibility of the Report Manager, including all activities necessary to follow up on the alert (for example, hearings or document acquisitions). If it is necessary to use the technical assistance of third-party professionals, as well as the specialized support of staff from other functions/ business directions, it is necessary to - in order to ensure the confidentiality obligations required by law - obscure any type of data that may allow the identification of the reporting person or any other person involved.

If it is necessary to involve other corporate functions other than the Report Manager, they will also be extended to the confidentiality obligations expressly provided for in this "whistleblowing" Policy and in the Model of organization and management, and expressly sanctioned by the internal disciplinary system.

If the report, however, is about violation of Organizational Model 231, it is advisable to work in synergy with the Supervisory Body, in respect of the confidentiality obligations.

Once the investigation activity is completed, the manager of the report may:

- archive the report as unfounded, stating the reasons;
- declare the report well-founded and contact the internal bodies/functions responsible for follow-up. The manager of the report is not responsible for any assessment of individual responsibilities and any subsequent measures or procedures.

All stages of the investigation activity must always be properly tracked and archived in order to demonstrate proper diligence in following up on the report.

The manager of the report shall provide a response to the reporting person within three months from the date of acknowledgement or - in the absence of such notification - within three months from the expiry of the seven-day deadline for that notification. In this respect, it should be specified that the verification activity does not need to be completed within three months, given that there may be cases where more time is needed for verification purposes. Therefore, it is a confirmation that, at the end of the indicated period, the verification activity may be final if the investigation is completed, or of an interim nature on the progress of the investigation, not yet completed.

Therefore, at the end of the three-month period, the manager of the report may communicate to the reporting person:

- the occurred closure of the alert, giving reasons to support the decision;
- the occurred verification of the validity of the report and its transmission to the competent internal bodies;
- the activity carried out up to that point and/or the activity they intend to carry out.

In this case, it is advisable to inform the reporting person of the subsequent final outcome of the investigation of the report (archiving or verification of the validity of the report with transmission to the competent authorities).

The reports received, their verification and analysis and all reference documentation, shall be kept for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the report procedure, in respect of the confidentiality requirements.

6. GUARANTEES AND SAFEGUARDS

Decree-Law 24/2023 introduced safeguards to protect reporting persons, which were extended to those persons other than the reporting person who, however, could be targets of retaliation, also indirectly undertaken, because of their role in the reporting process, in the public disclosure or in the complaint process and/or their particular relationship with the informer or complainant, in particular:

- to the facilitators;
- to persons from the same working environment as the reporting person, or of the persons who have lodged a complaint with the Judicial or Accounting Authority or of the persons who have made a public disclosure and who are linked to them by a stable emotional link or kinship within the fourth degree;
- to the work colleagues of the reporting person or of the person who has made a complaint to the Judicial or Accounting Authority or made a public disclosure, who work in the same working environment as that person and have a regular and current relationship with that person;
- to entities owned by the reporting person or the person who has lodged a complaint with the Judicial or Accounting Authority or which has made a public disclosure or for whom the same persons work, and to entities operating in the same working environment as the above-mentioned persons.

6.1. Safeguard of the reporting person

A. Safeguard of the identity of the reporting person

The identity of the reporting person and any other information which may directly or indirectly reveal their identity may not be disclosed without the express consent of the reporting person, to persons other than those competent to receive or follow up on reports. Accordingly, this protection also extends to any other information or element of the report, including the documentation attached thereto, from which the identity of the reporting person can be directly or indirectly deduced and has as a corollary the guarantee of such confidentiality during all stages of the reporting process, including any transfer of reports to other competent authorities.

In the disciplinary proceedings initiated by the Foundation against the alleged perpetrator of the reported conduct, the identity of the informer may not be disclosed, where the dispute of the disciplinary charge is based on separate and further investigations as compared to the report, even if they follow from it.

If, on the other hand, the dispute is based, in whole or in part, on the report and the identity of the reporter is essential for the defense of the person against whom the disciplinary charge has been challenged or of the person involved in the report, the information may be used for disciplinary purposes only with the explicit consent of the person who is the subject of the report to reveal their identity. In such cases, the person issuing the report shall be notified in advance by written communication of the reasons for which the confidential data need to be disclosed.

If the reporting person refuses to give its consent, the report may not be used in disciplinary proceedings which, therefore, cannot be initiated or continued in the absence of additional elements on which to base the dispute.

B. Safeguard of the whistleblowers from retaliation or discrimination

The Foundation prohibits any form of retaliation, understood as "any behavior, act or omission, even if only attempted or threatened, committed on account of the report, of the complaint to a judicial or accounting authority or of the public disclosure which causes or may cause direct or indirect unfair damage to the reporting person or to the person who made the complaint".

Retaliation, by way of example is considered:

- dismissal, suspension or equivalent measures;
- demotion or failure to advance;
- the change of functions, the change of place of work, the reduction of salary, the change of working hours;
- the suspension of training or any restriction on access to training;
- negative ratings or references;
- the taking of disciplinary measures or other sanctions, including pecuniary penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfavorable treatment;
- the non-conversion of a fixed-term employment contract into an open-ended employment contract, where the worker had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, especially on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
- the early conclusion or cancellation of the contract for the supply of goods or services;
- the cancellation of a license or permit;
- the request for submission to psychiatric or medical examinations.

For the protection to apply, it is necessary that:

- there is a reasonable belief that the information on violations reported, disclosed or denounced are true and fall within the objective scope of application of Legislative Decree 24/2023
- the public notice or disclosure was made in accordance with the provisions of Legislative Decree 24/2023
- there is a consequential relationship between the reporting, disclosure and complaint made and the retaliatory measures taken

The protection provided for in the event of retaliation is not guaranteed when it is established, even by a judgment at first instance, the criminal liability of the person who issued the report for defamation or slander offences or in any other way for the same offences committed by the reporting to the judicial or accounting authority, namely their civil liability, under the same title, in cases of intent or gross negligence.

C. Other safeguards

The further protection acknowledged to the reporting person is the limitation of their liability with regard to the disclosure and dissemination of certain categories of information, which would otherwise expose them to criminal, civil and administrative liability.

In particular, the reporting person will not be called upon to answer either criminally or through civil and administrative proceedings of:

- disclosure and use of official secrets (Art. 326 p.c.);
- disclosure of professional secrecy (Art. 622 P.C.);
- disclosure of scientific and industrial secrets (Art. 623 p.c.);
- breach of the duty of loyalty (Art. 2105 C.C.);
- infringement of the copyright protection provisions;
- breach of the provisions on personal data protection;
- disclosure or dissemination of information on breaches that are offensive to the reputation of the person concerned.

Decree-Law 24/2023 sets two conditions for the above mentioned limitations of liability:

- at the time of disclosure or dissemination there are reasonable grounds to believe that the information is necessary to disclose the reported breach;
- the report is made in compliance with the conditions provided for by Legislative Decree 24/2023 to benefit from protection against retaliation (there are good reasons to believe that the reported facts are true, the breach is among those reportable and the terms and conditions for accessing the report are respected).

It should be pointed out, therefore, that the limitation operates if the reasons behind the disclosure or dissemination are not based on mere insinuations, gossip, vengeful, opportunistic or scandalous purposes.

In any case, it should be considered that is not excluded liability for conduct which:

- are not linked to the report;
- are not strictly necessary to reveal the breach;
- unlawfully acquire information or access to documents.

Where the acquisition is an offence, for example illegal access to a computer system or hacking, the criminal liability and any other civil, administrative and disciplinary liability of the person who issued the report remain unaffected. It will be, on the contrary, not punishable, for example, the extraction (by copying, photography, removal) of documents to which they had lawful access.

6.2. Guarantee of the reported person

This policy does not affect the criminal and disciplinary responsibility of the whistleblower in the case of a slanderous or defamatory report under the Penal Code and art. 2043 of the Civil Code.

Art. 16, paragraph 3, of Legislative Decree 24/20023 states that protection is no longer guaranteed when it is established, even by a judgment at first instance, the criminal liability of the person who issued the report for defamation or slander, or in any other way for the same offences committed by the reporting to the judicial or accounting authority, or their civil liability under the same title in cases of willful intent or gross negligence, and the reporting person or the person making a complaint shall face a disciplinary sanction.

They are also responsible, in disciplinary proceedings and other competent bodies, for any form of abuse of this policy, such as the reports manifestly opportunistic and/ or made for the sole purpose of harming the reported

person or other subjects and any other hypothesis of improper use or intentional instrumentalization of the institution.

7 DISCIPLINARY SYSTEM

The Foundation for its own employees provides for and (if the conditions are met) adopts disciplinary sanctions against:

- those who are responsible of any act of retaliation or discrimination or otherwise unlawful, direct or indirect harm to the Reporting person (or anyone who has cooperated in the investigation of the facts subject to a report) for reasons directly or indirectly related to the report;
- the Reported person, or other persons involved in the reported events, for established responsibilities;
- anyone violating the confidentiality obligations referred to in the Policy;
- Employees, as required by law, who have made an unfounded report with intent or gross negligence.

Disciplinary measures will be proportionate to the extent and severity of the verified illegal conduct, possibly reaching, for the cases of greater gravity, the termination of employment.

Regarding Third parties (e.g. partners, suppliers, consultants etc.) the remedies and legal actions apply in addition to the contractual clauses of compliance with the Code of Ethics and any other applicable internal legislation.

8 PROTECTION OF PERSONAL DATA

The fulfilment of the obligations provided for by Legislative Decree 24/2023 involves the processing of personal data, concerning natural persons who enjoy regulatory protection as well as those involved in the activity of handling reports.
With regard to these processes, the Foundation, as Data Controller, has defined its own model for receiving and managing internal reports, identifying appropriate technical and organizational measures to ensure a level of security adequate to the specific risks arising from the processing carried out, based on a data protection impact assessment (DPIA) pursuant to art. 35 of the GDPR.
The Company will ensure that data subjects receive the information referred to in articles 13 and 14 of the GDPR, according to timeliness and adequacy criteria, giving preference to the digital mode.
In order to allow the data subjects to be fully informed about the processing carried out, on the platform and on the website of the Data Controller is made available information that explains the concrete methods of processing.
In particular, it is hereby announced that the processing of data will be carried out on behalf and by delegation of the Data Controller exclusively by the persons expressly responsible for receiving and/or managing the report.
The Data Controller will commission for the performance of the activities referred to in the preceding paragraph only properly trained subjects and who, where not legally bound by an adequate obligation of confidentiality, have undertaken to do so and in any case present sufficient guarantees on the adoption of appropriate technical and organizational measures so that the processing of Data is similar to that carried out by the Data Controller.
They are subject to the processing of all common, particular and/or judicial data contained in the report and the accompanying documentation.
The data are processed exclusively to give adequate follow-up to reports (art. 12 Legislative Decree 24/2023).
The Data Controller undertakes the responsibility not to disclose the identity of the reporting person, unless they have expressed their consent, to subjects other than those referred to in article 3 of this notice.

For further confidentiality measures to protect the reporting person, please refer to article 12 of Legislative Decree 24/2023.
The processing of data is necessary to comply with the legal obligations imposed by Legislative Decree 24/2023 (art. 6, par. 1, lett. c and ccoo. 2 and 3; art. 9 par. 2, lett. b; art. 9; art. 88 G.D.P.R.).
The Data Controller adopts strict policies to minimize the use of Data, which is only taken and used in so far as it is actually necessary for receiving and managing reports.
As regards the concrete processing methods, the Data Controller adopts technical/organizational measures, both on digital and analogic data, aimed at providing the highest possible level of protection.
In compliance with the legislation on whistleblowing and, in general, in accordance with the principles of privacy by design and default, the Data Controller has previously evaluated the impact that the processing in question has on the rights of data subjects and the protection of their data.
The data will be managed and processed exclusively by the parties indicated in article 3 of the Information Notice, which will carry out the appropriate investigations on the facts reported.
If the investigation activity requires the involvement of additional subjects, the Data Controller will endeavor to extend to them the privacy and confidentiality obligations provided for by the reference legislation.
If the report is true, the manager of the report will involve the responsible business functions so that they take appropriate measures.
Pursuant to article 14 of Legislative Decree 24/2023, reports and related documentation are processed for as long as necessary for their management and no later than five years from the date of communication of the final outcome of the reporting procedure.

10 THE ANAC'S SANCTIONING POWERS

Pursuant to art. 21 del Legislative Decree No. 24/2023, the National Anti-Corruption Authority (in short ANAC) applies to responsible the following administrative pecuniary sanctions:

- EUR 10,000 to 50,000 when it finds that the natural person identified as responsible has committed retaliation;
- EUR 10,000 to 50,000 when it finds that the natural person identified as responsible has obstructed or attempted to obstruct the report;
- EUR 10,000 to 50,000 when it establishes that the natural person identified as responsible has violated the obligation of confidentiality set out in art. 12 of Legislative Decree No. 24/2023 and described above in point 6.1.A. The sanctions applicable by the Guarantor for the protection of personal data for the profiles of competence according to the regulation on personal data remain unaffected;
- EUR 10,000 to 50,000 when it is verified that no reporting channels have been established; in this case the steering body is considered responsible;
- EUR 10,000 to 50,000 when it establishes that no procedures have been adopted for the implementation and management of reports or that the adoption of such procedures is not in accordance with what is provided for by Legislative Decree No. 24/2023; in this case the steering body shall be considered responsible;
- EUR 10,000 to 50,000 when it is established that the activity of verification and analysis of the reports received has not been carried out; in this case, the manager of the reports is considered responsible;
- EUR 500 to 2,500, when the civil liability of the person who reported the offence is established, even by a judgment at first instance, for defamation or slander in cases of intent or gross negligence, unless the person has already been convicted, also at first instance, for the offences of defamation or slander or in any other way for the same offences committed with the complaint to the judicial authority.