ORGANIZATION: TINTSETA SRL Single - Member Company (hereinafter “institution”)

POLICY / PROCEDURE for “WHISTLEBLOWING” REPORTS

(Policy/Procedure VERSION N.1 / 2023)

SUMMARY

*** * ***

1. INTRODUCTION

The "Whistleblowing" policy/procedure is adopted by the organization (together with the IT tools chosen) with the aim:
(i) to comply with the provisions of Legislative Decree no. 24 of 2023 (hereinafter, also "WB Decree") and concerning the protection of people who report violations of national or European Union regulatory provisions (so-called whistleblowing directive) of which they become aware in the work context, harmful to the public interest or the integrity of the public administration or private institution (the "Reports"), as well as
(ii) to regulate elements relating to the so-called Reports. Whistleblowing, by various subjects also referred to below, namely: employees and managers, subjects who carry out administrative functions (administrators), management, control and supervision, freelancers, consultants, self-employed workers, employees, collaborators of the organisation, suppliers of goods and/or services who carry out works in favour of the organisation, volunteers, shareholders, interns, including unpaid ones and
- in compliance with the legislation on privacy and the guardianships provided by law for the Reporter, the Reported Party and the other subjects involved in the Report: among the aforementioned elements relating to the so-called Reports whistleblowing, which will be indicated in this Whistleblowing policy/procedure can now be indicated for example:

- the subjects entitled to submit the Reports (Reporters);
- subjects who benefit from the protection measures provided for by Legislative Decree 24/2023;
- the prerequisites for proceeding with internal reporting and the related eligibility conditions;
- the person, internal or external, who is entrusted with the management of the Reports and the related powers and obligations;
- the concrete methods chosen by the company for using the internal reporting channel (IT platform, voice messaging, etc.);
- the need for adjustments to the processing of personal data/privacy.

For anything not expressly indicated in this "Whistleblowing" policy/procedure, please refer to Legislative Decree no. 24 of 2023, to the ANAC Guidelines, published with Resolution no. 311 of 2023, as well as the Regulation and operating instructions available on the ANAC institutional website.

2. REGULATORY REFERENCES

- Legislative decree n. 24 of 2023 on the "implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, concerning the protection of people who report violations of Union law and containing provisions concerning the protection of people who report violations of national regulatory provisions"
- EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the "protection of natural persons with regard to the processing of personal data, as well as the free flow of such data"

- Directive (EU) 2019/1937
- ANAC Resolution n. 311 of 12 July 2023 containing the "Guidelines on the protection of people who report violations of national regulatory provisions." - Procedures for the submission of external reports"
- European Regulation 2016/679 (GDPR)
- Privacy Code (Legislative Decree 196/2003 and subsequent amendments).

3. RECIPIENTS

Our institution is among those that must comply with the WB Decree.

Those who can make a Report (Reporters) are:

employees and managers, individuals who perform administrative functions (administrators), management, control and supervision, freelancers, consultants, self-employed workers, employees, collaborators, suppliers of goods and/or services who carry out works for the organisation, volunteers , shareholders, interns, including unpaid ones.

Reporting by these subjects can be made:

-. when the legal relationship is ongoing;

-. during the probationary period;

-. when the legal relationship has not yet begun, if the information on the violations was acquired during the selection process or in other pre-contractual phases;

-. after the dissolution of the legal relationship if the information on the violations was acquired before the dissolution of the relationship itself.

4. SCOPE / FIELD OF APPLICATION AND PURPOSE

The Whistleblowing policy/procedure, together with the IT platform adopted by the reporting body and the indication of the reporting manager appointed by the body (the "Manager"), have the purpose of regulating the process of transmission, reception, analysis and management of the Reports, including the archiving and subsequent deletion of the same and related documentation, with the methods and timing indicated and what is necessary to comply with the WB Decree.

The scope of application coincides with that described by Legislative Decree no. 24 of 2023 and concerns the violations provided for in the aforementioned WB Decree.

The purpose of this Whistleblowing policy/procedure is to adequately inform all recipients of the whistleblowing regulations dictated by Legislative Decree no. 24 of 2023.

Pursuant to Legislative Decree no. 24 of 2023, disputes, claims or requests linked to a personal interest of the Reporter or of a person who has made a report to the judicial authority cannot be the subject of a Report: therefore, Reports of this type will not be dealt with by the Whistleblowing policy/Procedure.

5. SUBJECT OF THE REPORT and VIOLATIONS

The violations that can be reported are those that harm the public interest or the integrity of the body or public administration and which consist of illicit conduct, situations, facts and circumstances of which the Reporter has become directly aware in the working context due to the employment or collaboration relationship and, therefore, also includes information that has been acquired on the occasion and/or due to the performance of work tasks, although randomly..

In particular, the subject of the Reports are behaviours, acts or omissions harmful to the public interest, the integrity of the administration or institution, relating to:

- administrative, accounting, civil or criminal offences;
- violation of the organisation's administration and management of the institution;
- offences in the context of community or national acts relating to procurement, services and financial products, as well as for example - transport -safety, environmental protection and public health;

- acts or omissions disadvantageous to the financial interests of the EU or the internal market.

Reports can be made even if the employment relationship has subsequently ended, if the information was acquired during its performance, as well as if the relationship has not yet begun and the information on the violations was acquired during the selection or in other pre-contractual phases.

6- CONTENT AND CHARACTERISTICS OF THE REPORT and ANONYMOUS REPORTS

-. CONTENT AND CHARACTERISTIC OF THE REPORT

The whistleblower (Reporter) is required to make the Report in accordance with the provisions of this Whistleblowing policy/procedure (**preferably using the written form and the guided form within the IT platform**), to act in good faith and to provide all the useful elements to allow the necessary checks and investigations to be carried out to verify the validity of the facts which are the subject of the Report.

-. ANONYMOUS REPORTS

The anonymous reports received can be treated as ordinary reports.

The anonymous reports received can only be taken into consideration if adequately detailed, they are recorded and stored by the Reporting Manager, thus making it possible to trace them, in the event that the Reporter, or whoever filed the report, communicates to ANAC that he or she has suffered retaliatory measures cause of that anonymous report or complaint.

In cases of anonymous reporting, if the reporting person was subsequently identified and suffered retaliation, the protection measures for retaliation provided for by Legislative Decree No. 24 of 2023 are applied.

7. REPORTING CHANNELS *EX LEGE*

Legislative Decree no. 24 of 2023 provides for various reporting channels, including the specifically set-up internal one for the institution(i.e. IT Platform).

The internal reporting channels are established having given information to the trade unions.

The organization has activated the internal reporting channels indicated below, intended for the Reporting Manager.
In summary, the Report can be presented in the following alternative ways:
a). sending via the IT platform (channel in written form).
b). sending with voice messaging via IT platform (oral channel).
The IT platform will represent the preferential channel for reporting (preferably in written form), given that it will be equipped with encryption mechanisms that better guarantee security and technological confidentiality of the reporting process and which allow the identity of the reporting party and the reported party to be kept confidential as well as of the content of the Report and the related documentation.
The Reporting Manager is the internal or external entity appointed by the organization and to which the management of the channel and the reporting is entrusted, the possibility of entrusting the management of the channel to an "external entity" to the organization being recognised.
In terms of privacy legislation, the person (i.e. Manager) who manages the Reports must: (i) be authorized to process personal data, (ii) ensure independence and impartiality; (iii) receive adequate professional training on the discipline of whistleblowing, also with reference to concrete cases.

8-. INTERNAL SIGNALLING CHANNEL

8. Internal signalling channel
The body has provided an internal reporting channel that the Reporter must use to transmit information on violations. The establishment of this channel allows for more effective prevention and detection of violations. This choice responds to the principle of promoting a culture of good communication and corporate social responsibility as well as improvement of one's organization.
The internal reporting channel involves written or oral methods through the “My Whistleblowing” platform accessible https://areariservata.mygovernance.it/#!/WB/TINTSETA
By accessing the platform, the whistleblower can also request a direct meeting with the person responsible for managing the report.
The internal reporting channel guarantees the confidentiality of the identity of the reporter, the facilitator (where present), the people involved and in any case mentioned in the Report as well as the content of the same and the related documentation forwarded or integrated.

8.1 Person responsible for managing the channel (so-called "channel manager")

The management of the internal channel is entrusted to:
- Cassina Roberto, CF CSSRRT57T17C933I, born in Como (CO) on 12/17/1957
- Galli Cristina, CF GLLCST86S52I441B, born in Saronno (VA) on 12/11/1986

subjects in possession of the requirements of autonomy, independence and specifically trained.
The person responsible for managing the channel and the report acts exclusively with regard to the acquisition of the report and access to the platform.

8.2 Characteristics of the internal signalling channel

The organisation's internal reporting channel is managed via the web-based "Whistleblowing" platform, accessible from all devices (PC, Tablet, Smartphone).

The data entered into the Platform is segregated in the logical partition dedicated to the institution and subjected to a scripting algorithm before being archived. Safety transport is guaranteed by secure communication protocols.

Reporters, after registering, can choose whether to make an anonymous or non-anonymous report. The system allows, thanks to the data provided during registration, to send in real time, even in the case of anonymous reporting, notifications via e-mail to the reporting parties on the progress of the reporting (for example: correctly sent, received, new comment, outcome of the investigation) inviting them to connect to be an active part of the process of evaluating the alleged offence. This allows for effective and efficient management of the report; in fact, you do not have to wait for the whistleblowers to connect to the platform in order to notify them of the relevant information relating to their reports.

In case of anonymous reporting, the reporting person's data will not be accessible to the managers of the reporting. The email addresses of the whistleblowers will NEVER be available either to the company or to the managers of the report.

To take charge of a report, one of the managers simply needs to click on the report and open it.

A closed or rejected report can be reopened by managers at any time.

The entity's reporting managers have unique credentials for access, which expire every 3 months.

The password policy complies with international best practices.

The company ZUCCHETTI Spa, which provides the service for using the Platform, is ISO27001 certified.

The processing of personal data must always take into account and comply with the obligations established by the GDPR and Legislative Decree 196/2003 and subsequent amendments.

8.3 Characteristics of the report and anonymous reports

It is necessary that the Report is as detailed as possible in order to allow the analysis of the facts by the parties competent to receive and manage the reports. In particular, the following must be clear:

- the circumstances of time and place in which the event which is the subject of the Report occurred;
- the description of the fact;
- the personal details or other elements that allow the identification of the person to whom the reported facts can be attributed.

Information about reported violations must be truthful. We do not consider such simple suppositions, unreliable indiscretions (so-called rumours), as well as news in the public domain, incorrect information (with the exception of genuine error), clearly unfounded or misleading or if merely harmful or offensive. However, it is not necessary for the reporter to be certain of the actual occurrence of the facts reported and of the identity of the author of the same.

It is also useful for the reporting party to provide documents that can provide elements of justification for the facts being reported, as well as the indication of other subjects potentially aware of the facts.

Anonymous Reports, where detailed, are treated as ordinary Reports and in this case considered within the scope of this procedure also with reference to the protections of the Reporter, if subsequently identified, and the conservation obligations.

8.4 Operational procedure for managing the Report

The Reporter transmits the Report via the dedicated internal channel.

The Reporter activates the Report through the link indicated above, in written mode, through a guided form, or in oral mode via a voice messaging system. In the case of a direct meeting, the channel manager guarantees that the meeting will take place within a reasonable time (10-15 days), preferring that the hearing takes place in premises other than the company ones.

If the Reporter makes the Report orally through a meeting arranged with the channel manager, the same, with the prior consent of the reporter himself, is documented by the channel manager with recording on a device suitable for storage and vocal reproduction or through the drafting of a report. In this last case, the Reporter can verify, rectify and/or confirm the minutes of the meeting by signing them.

The reception of the Report by the person responsible for the channel starts the Report management process. The channel manager proceeds with its "processing" according to a predefined process flow chart.

Upon reception of the Report, the responsible party communicates an acknowledgment of receipt to the reporting party within 7 days of receiving the report and taking charge of the Report.

The person responsible for managing the Report proceeds with an initial verification of the correctness of the procedure followed by the Reporter and of the content of the Report both in reference to the scope of application defined by this procedure (so-called inherence of the content of the Report) and to its verifiability in based on the information provided. If the Report is not relevant, the channel manager formalizes the outcome of the check and communicates it to the Reporter within a reasonable time (no later than 3 months) and archives the Report. The channel manager promptly informs the internal contact person, ensuring compliance with the principle of confidentiality, who shares the information with the organisation.

If it is necessary to acquire additional elements, the channel manager will contact the Reporter via the Platform. If the Reporter does not provide additional information within 3 months of the request for integration, the channel manager will proceed with archiving the Report, notifying the Reporter and informing the internal contact person.

The channel manager, having verified the relevance of the Report and having acquired all the elements, informs the management, supervisory and control body of the institution, in compliance with the principle of confidentiality.

At the end of the investigation, the channel manager prepares a final report in order to proceed with feedback to the Reporter. The response to the Reporter must be sent within three months from the date of acknowledgment of receipt or from the expiry of the seven-day period from the submission of the Report. Only in exceptional cases, if the complexity of the Report requires it, or in consideration of the Reporter's response times, the channel manager, having promptly informed the Reporter before the deadline, with appropriate justification, will be able to continue the investigation phase for the necessary time and give the reporter periodic updates.

The management, supervision and control body of the institution, within its operational autonomy, evaluates the outcome received and, if the report is well founded, initiates the necessary communications to the holders of disciplinary power for the application of any sanctions by the institution.

In the event of defamation or slander, ascertained with conviction even at first degree, the organization proceeds with sanctioning proceedings against the Reporter.

It is specified that, from reception of the Report until its closure, any person who finds himself in a situation of conflict of interest must refrain from making decisions in order to guarantee compliance with the principle of impartiality.

8.5 Transmission of Reports to the wrong recipient

If the Report is transmitted to a different person from the one responsible for receiving it, the person receiving it has the obligation to transmit it within seven days to the competent person, giving notice of the transmission to the reporting person and guaranteeing a chain of custody of the information compliant with confidentiality obligations. and those referred to in paragraph 8.2. The organization adopts disciplinary sanctions in case of failure to comply with the transmission obligation.

In the case of involuntary transmission of the Report to a person different from the one entitled to receive it, the Reporter must demonstrate mere negligence and the absence of a personal interest in the erroneous transmission.

8.6 Retention of Internal Reporting documentation

Internal reports and all related attached or integrated documentation are kept, with a specific digital chain of custody, for the necessary time to process the report itself.

In any case, the documentation is kept only for a period of time identified as a maximum of five years starting from the date of communication of the final outcome of the reporting procedure.

In all the cases mentioned, it is necessary that the procedure for storing internal reports and related documentation complies with community and national guarantees on the processing of personal data as well as with the established measures on the right to confidentiality.

9. EXTERNAL REPORTING CHANNEL AND PUBLIC DISCLOSURE

With reference to the institution, as an institution belonging to the private sector, the use of the external channel and public disclosure are not practicable.

The possibility of reporting to ANAC any retaliation suffered following the Report remains unaffected.

10. PROTECTION MEASURES AND REPORTING OF RETALIATION

The WB Decree is concerned with protecting the Reporter with:

-. the obligation to keep your identity confidential;

-. the prohibition of retaliatory acts against you following a Report, including: (i) the possibility of communicating to ANAC the retaliation you believe you have suffered following a Report; (ii) the provision of nullity of acts undertaken in violation of the prohibition of retaliation, to be enforced also in court;

-. exclusions of liability in the event of disclosure (or dissemination) of violations covered by the obligation of secrecy (except in the case of classified information, professional and medical secrecy and secrecy of the deliberations of the judicial bodies, for which the application of the relevant legislation remains unchanged) or relating to the protection of copyright or the protection of personal data or information on violations that offend the reputation of the person involved or reported, if:

-. at the time of disclosure (or dissemination) there are well-founded reasons to believe that it is necessary to reveal the violation and the conditions referred to in the following points a) and b) exist;

-. exclusions of liability, unless the fact constitutes a crime, for the acquisition of information on violations or for access to them.

The institution protects the Reporter in good faith; therefore, the protection measures listed above apply to the Reporter and Connected Parties provided that:

- a) at the time of the Report, the Reporter has reasonable grounds to believe that the information on the reported or reported violations is true and falls within the scope of the violations referred to in the Whistleblowing policy/procedure;
- b) the Report is made in compliance with the provisions of the policy/procedure and the WB Decree.

The protection measures listed above also apply in the case of anonymous reporting, if the reporting party has subsequently been identified.

Examples of retaliatory behaviour or discriminatory measures include, but are not limited to:

- dismissal, suspension or equivalent measures;
- demotion or failure to promote;
- the change of functions, the change of place of work, the reduction of salary, the modification of working hours;
- the suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including pecuniary ones;
- discrimination or otherwise unfavourable treatment;
- failure to renew or early termination of a fixed-term employment contract;
- the early termination or cancellation of the contract for the supply of goods or services;

Acts taken in violation of the prohibition on retaliation are void.

The declaration of nullity of retaliatory acts is also up to the Judicial Authority.

The management of retaliatory communications in the public and private sectors is the responsibility of ANAC.

Once the Whistleblower proves that he or she has made a Report in compliance with the law and that he or she has suffered behaviour deemed retaliatory, the onus is on the Employer to prove that such behaviour is in no way connected to the Report.

To this end, it is essential that the alleged perpetrator provides all the elements from which to deduce the absence of the retaliatory nature of the measure adopted against the Whistleblower.

The protection also applies to the facilitator, to people in the same work context as the Reporter, to the Reporter's work colleagues.

The methods through which the Reporter - or another person among those indicated above - can communicate retaliation to the ANAC are defined by the latter and indicated on the ANAC website, in a dedicated section.
The institution will apply the appropriate disciplinary sanctions in the event that retaliatory measures against the Reporter or the people involved in the Report are ascertained.

11. PROTECTION OF THE REPORTER'S CONFIDENTIALITY

The identity of the Reporter and any other information from which it can emerge, directly or indirectly, cannot be revealed without the express consent of the reporting person to persons other than those competent to receive or follow up on the Reports.
In two cases expressly provided for by the WB Decree, to reveal the identity of the Reporter, in addition to the express consent of the same, a written communication of the reasons for such disclosure is also required:
-. in disciplinary proceedings where the disclosure of the identity of the Whistleblower is essential for the defence of the person against whom the disciplinary charge is contested;
-. in proceedings initiated following internal or external reports where such disclosure is also indispensable for the purposes of the defence of the person involved.
If the Reporter does not agree to the disclosure of his identity, the Report cannot be used as part of the disciplinary proceedings.
As part of the disciplinary proceedings, the identity of the Whistleblower cannot be revealed where the contestation of the disciplinary charge is based on investigations that are distinct and additional to the Report, even if consequent thereto.
If the dispute is based, in whole or in part, on the Report and knowledge of the identity of the Reporter is indispensable for the defence of the accused, the Report will be usable for the purposes of disciplinary proceedings only in the presence of the express consent of the Reporter to the disclosure of their identity.
Furthermore, in order to guarantee maximum protection of confidentiality, access to the documentation relating to the Reports and the investigation activities is allowed only to the manager of the Reports.
The prohibition on revealing the identity of the Reporter refers not only to the name of the Reporter, but also to all elements of the Report, including the documentation attached to it.
The protection of confidentiality is extended to the identity of the people involved and the people mentioned in the Report until the conclusion of the proceedings initiated based on the Report, in compliance with the same guarantees provided in favour of the Reporting person.
In the case of receipt of the Report using IT methods, the protection provided takes the form of the preparation of an IT platform that uses an encryption protocol suitable to guarantee strengthened protection of the confidentiality of the identity of the Reporter, the content of the Report and the documentation attached thereto. , accessible only to the Manager.
The IT platform allows, through a computerized guided compilation procedure, to make and send a whistleblowing report complete with elements and information according to the indications contained in Legislative Decree no. 24 of 2023 and in the ANAC Guidelines.
This IT platform, in accordance with the provisions of current legislation, allows the institution to guarantee maximum protection of the confidentiality of the Reporter's identity, the content of the Report itself and the related attached documentation, as it provides for the immediate encryption of the Report through the use of tools and an encryption protocol that ensure its inalterability.
The IT platform can be accessed directly via the specific section of the institutional website.

12. EXCLUSION OF THE PROTECTION OF THE REPORTER

The Reporter is not guaranteed the protections provided if the Report contains false information, made with malice or gross negligence. Such behaviour may also give rise to disciplinary proceedings or legal action against the reporter himself..

13. PROTECTION OF THE REPORTED

The Reported Person is the person referred to in a Report as responsible for the alleged infringement or illicit conduct, who may be a natural or legal person.
The protection of the identity of the person mentioned in the Report must be guaranteed by the subjects of the organisation, by the Manager, by the ANAC, as well as by the administrative authorities to whom the Reports are sent as they fall within their competence, until the conclusion of the proceedings initiated due to the Reporting and in compliance with the same guarantees provided in favour of the Reporting person.
The reported person can be heard or is heard, at his request, also through a paper procedure through the acquisition of written observations and documents. This person does not have the right to be informed of the Report concerning him, except in the case in which disciplinary proceedings are initiated against him based in whole or in part on the Report.
Furthermore, the Reporting will not be able to request to know the name of the Reporter, except in the cases expressly provided for by law.

14. DISCIPLINARY SYSTEM

In compliance with current legislation, the individual National Collective Labor Agreements and internal provisions, if reports in bad faith (slanderous or defamatory) or illicit or irregular behaviour emerge, the organization will adopt disciplinary sanctions:

- towards those who are responsible for any act of retaliation or discrimination or in any case of illegitimate prejudice, direct or indirect, towards the Reporter (or anyone who collaborated in ascertaining the facts which are the subject of a Report) for directly related reasons or indirectly, to the Report;
- towards the Reported Party, for the responsibilities ascertained;
- towards anyone who violates confidentiality obligations;
- towards employees, as required by law, who have made an unfounded report with intent or gross negligence.
- towards employees who have not complied with the obligation to transmit within 7 days to the competent person, in the event of incorrect receipt of the report, giving notice of the transmission to the reporting person and guaranteeing a chain of custody of the information compliant with the obligations of confidentiality and those of referred to in paragraph 8.2.

Disciplinary measures will be proportionate to the extent and seriousness of the illegal conduct ascertained, and, in the most serious cases go as far as termination of the employment relationship.
With regard to third parties (partners, suppliers, consultants, agents, etc.), the legal remedies and actions apply in addition to the contractual clauses in compliance with the Code of Ethics adopted by the institution.

15. SANCTIONS

Pursuant to the WB Decree, anyone who is responsible for one of the following conduct is subject to financial sanctions by the ANAC:
-. carrying out retaliation in relation to Reports;
-. obstacle or attempted obstacle to making the Report;
-. violation of the confidentiality obligations established by the policy/procedure and the WB Decree;
-. failure to establish reporting channels according to the requirements set out in the WB Decree;
-. failure to adopt a policy/procedure for making and managing reports or failure to comply with the WB Decree;
-. failure to verify and analyze the Reports received.
Furthermore, the imposition of a disciplinary sanction against the Whistleblower is envisaged when it is established that: (i) even with a first degree sentence, criminal liability for the crimes of defamation or slander or in any case for the same crimes committed with reporting to the judicial or accounting authority or
(ii) civil liability, for the same reason, in cases of willful misconduct or gross negligence.

16. PERSONAL DATA PROTECTION – PRIVACY: ASSESSMENT AND INFORMATION

During the procedure, the Data Controller (as defined by art. 4, EU Regulation 2016/679) is the institution.
In relation to the entry into force of the "Whistleblowing" regulation, the tasks of the Data Controller include that of adapting the privacy regulation according to the current provisions of the law.
The privacy policy relating to whistleblowing reports is published on the IT platform.
The internal and external Reports and the related documentation are kept for the time necessary to process the Report and in any case no later than five years from the date of communication of the final outcome of the Report procedure, in compliance with the confidentiality obligations set out in the legislation European and national on the protection of personal data.
Based on the provisions of the legislation on personal data, of the Legislative Decree. n. 24 of 2023 and the ANAC Guidelines, the Data Controller, the Data Processors and the persons authorized to process personal data are also required, for example, to respect the following fundamental principles:

- process the data in a lawful, correct and transparent way towards the interested parties ("lawfulness, correctness and transparency").
- collect data only for the purpose of managing and following up on Reports;
- ensure that the data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- keep the data in a form that allows the identification of the interested parties for the time necessary to process the specific Report and in any case no later than five years from the date of communication of the final outcome of the Report procedure ("retention limitation").
- ensure the updating of the register of processing activities
- guarantee the prohibition of tracking of reporting channels
- guarantee, where possible, the tracking of the activity of authorized personnel in compliance with the guarantees protecting the Reporter, in order to avoid the improper use of data relating to the Report; The tracing of any information that could lead to the identity or activity of the Reporter must be avoided.
- carry out the processing in a way that guarantees adequate security of personal data, including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage ("integrity and confidentiality"). In the context in question, characterised by high risks for the rights and freedoms of the interested parties, the use of encryption tools within the internal channels and the external reporting channel is generally considered an adequate measure to implement, since by design and by default, to the principle of integrity and confidentiality.

17. TRAINING and VISIBILITY OF THE WHISTLEBLOWING POLICY/PROCEDURE

Suitable information must be provided to the Reporters and the People involved pursuant to the articles. 13 and 14 of the GDPR.
The Privacy information is made available through:
-. publication on the web page of the institutional website dedicated to whistleblowing;
-. link below inserted in the IT Platform;
-. sending via email to all employees and collaborators.
Training on whistleblowing is also included in staff training plans.

GO TO THE WEBSITE:
https://areariservata.mygovernance.it/#!/WB/TINTSETA