ORGANISATION: ANCI SERVIZI SRL

(hereinafter 'organisation')

POLICY / PROCEDURE for WHISTLEBLOWING REPORTS

(Policy/Procedure VERSION NO.1 / 2023)

CONTENTS

* * *

1. INTRODUCTION

The 'Whisteblowing' policy/procedure is adopted by the organisation (along with the chosen IT tools) with the aim of:

(i). complying with the provisions of **Legislative Decree No. 24 of 2023** (hereinafter also referred to as the "**WB Decree**") concerning the protection of persons reporting breaches of Italian or European Union regulations (so-called whistleblowing directive) of which they become aware in the context of their work, which are detrimental to the public interest or the integrity of a public or private organisation, and

(ii) governing aspects relating to whistleblowing Reports, by various parties, including those referred to below, namely: employees and managers / persons exercising administrative (directors), management, control and supervisory functions / freelance professionals, consultants, self-employed workers / employees / co-workers of companies / suppliers of goods or services that perform works in favour of our Organisation / volunteers / shareholders / trainees, including unpaid ones, and

- in compliance with the regulations on data protection and the protection provided by law for Whistleblowers, Reported Persons and other parties involved in a Whistleblowing Report: aspects relating to Whistleblowing Reports, which will be detailed in this Whistleblowing policy/procedure, include inter alia, by way of example:

- parties entitled to submit whistleblowing reports (whistleblowers);
- parties who enjoy the protection provided for in Legislative Decree no. 24/2023;
- the prerequisites for internal reports and conditions for admissibility;
- the internal or external party entrusted with the management of reports and the respective powers and obligations;
- the specific methods chosen by the company for using the internal reporting channel (IT platform, voice messaging, etc.);
- the need for adjustments for the processing of personal data/privacy.

Moreover, the WB Decree provides that, for private sector organisations falling within the scope of Decree 231/01 **the Organisational Models pursuant to Legislative Decree 231/01 must be updated and provide, in order to comply with the new regulations, "internal reporting channels, prohibition of retaliation and a disciplinary system" .**

Therefore, our Organisation is also updating the current Organisational Model 231/01.

For anything not expressly indicated in this "Whisteblowing" policy/procedure, reference is made to Legislative Decree no. 24 of 2023, the ANAC Guidelines, published by Resolution no. 311 of 2023, and to the Rules and Operating Instructions available on the ANAC institutional website.

2. REFERENCE LEGISLATION and ORGANISATIONAL MODEL PURSUANT TO LEGISLATIVE DECREE 231/01

- Legislative Decree No. 24 of 2023 implementing *"Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws"*.
- EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on *"the protection of individuals with regard to the processing of personal data and on the free movement of such data"*.
- Legislative Decree No. 231 of 8 June 2001 concerning the *"Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of 29 September 2000"*
- Directive (EU) 2019/1937:
- ANAC Resolution No. 311 of 12 July 2023 on the *"Guidelines on the protection of persons who report breaches of national laws. - Procedures for the Submission of External Reports"*
- European Regulation 2016/679 (GDPR);
- Privacy Code (Legislative Decree. 196/2003 and subsequent amendments);

The references also include the Organisational Model adopted by the organisation.

As has been pointed out by a number of organisations that have dealt with 'whistleblowing' in various capacities, the scope of application of the regulations is very complex and rests on a variable system of obligations and protective measures, which change according to: i) the subject of the breach; ii) the public/private nature of the whistleblower; iii) the size of the private organisation and the extent to which the rules set out in Decree 231 apply to it.

3. RECIPIENTS

Our Organisation is among those that must comply with the WB Decree, as it **has already adopted the Organisational Model pursuant to Legislative Decree. 231/01.**

Those who can make a Report (Whistleblowers) are:

employees and managers / persons exercising administrative (directors), management, control and supervisory functions / freelance professionals, consultants, self-employed workers / employees, co-workers of companies / suppliers of goods or services that perform works in favour of our Organisation / volunteers / shareholders / trainees, including unpaid ones.

Reporting by such persons may be carried out:

-. when a legal relationship is ongoing;

-. during a probationary period;

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

-. after the dissolution of a legal relationship if the information on breaches was acquired before the dissolution of the relationship.

4. FRAMEWORK/SCOPE AND PURPOSE

The Whistleblowing policy/procedure, along with the IT Platform that will be adopted for whistleblowing and the indication of the whistleblowing manager to be appointed by the organisation, are intended to govern the process of transmission, receipt, analysis and management of Whistleblowing Reports, including the filing and subsequent deletion of these and related documentation, with the described methods and timeframes and in compliance with the WB Decree.

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

The purpose of the Whistleblowing policy/procedure under review will be to adequately inform all recipients of the Whistleblowing regulations set forth by Legislative Decree No. 24 of 2023.

Pursuant to Legislative Decree No. 24 of 2023, complaints, claims or requests linked to a personal interest of a Whistleblower or a person who has made a complaint to the Judicial Authority cannot be the subject of Reports: therefore, Reports of this kind fall outside the scope of the Whistleblowing Policy/Procedure.

5. SUBJECT OF A REPORT and BREACHES

Breaches that can be reported are those that harm the public interest or the integrity of a public or private organisation and **consist** of:

-. (i). unlawful conduct that is relevant under Decree 231/01 or

-. (ii) breaches of the 231/01 Organisational Model adopted by the Organisation

Reports must relate to situations, facts, circumstances which the Whistleblower became aware of directly at work by reason of an employment relationship or collaboration and, therefore, also include information that was acquired during and/or as a result of the performance of working duties, albeit in a random/fortuitous manner.

Reports may be made even if an employment relationship is subsequently terminated, where information was acquired during the course of the relationship, as well as where a relationship has not yet begun and information on breaches was acquired during the selection or other pre-contractual stages.

6- CONTENT AND CHARACTERISTICS OF A REPORT AND ANONYMOUS REPORTING

-. CONTENT AND CHARACTERISTIC OF A REPORT

A Whistleblower is required to make a Report in accordance with this Whistleblowing policy/procedure (preferably **in writing using the guided form on the IT Platform**), and shall act in good faith and provide all relevant information for enabling the necessary checks and verifications to be carried out to ascertain whether the reported facts are well-founded.

-. ANONYMOUS REPORTS

Anonymous Reports that are received can be equated with ordinary reports.

Anonymous Reports can only be taken into account where these are adequately substantiated, and recorded and kept by the Whistleblowing Manager, to ensure they can be traced when a Whistleblower, or the person making the complaint, informs ANAC that he/she has suffered retaliation as a result of that Anonymous Report or complaint.

In the event of anonymous Reports, where a whistleblower is subsequently identified and has suffered retaliation, the protection measures for retaliation provided for in Legislative Decree No. 24 of 2023 shall apply.

7. LEGAL REPORTING CHANNELS

Legislative Decree No. 24 of 2023 provides for various reporting channels - including the internal reporting channel in our Organisation - which are created following prior notification to trade unions.

The Organisation will activate the following internal reporting channels that will be directed to the Whistleblowing Manager. In summary, a Report may be submitted in one of the following ways:

a). via the IT Platform (written channel).

b). by voice messaging via the IT platform (verbal channel).

The IT Platform is the preferred channel for making a Report (preferably in writing), since it will have encryption mechanisms that best guarantee the security and technological confidentiality of the Reporting process and allow the identity of Whistleblowers and Reported Persons, as well as the content of Reports and related documentation, to remain confidential.

The Whistleblowing Manager will be the external party appointed by the organisation, who is entrusted with the Management of the channel and Whistleblowing Reports, given that the management of the channel may be delegated to an "external party" to the organisation.

In terms of the data protection legislation, the party managing Whistleblowing Reports shall: (i) be authorised to process personal data, (ii) ensure independence and impartiality; (iii) receive appropriate professional training on whistleblowing regulations, including with reference to specific cases.

8-. INTERNAL REPORTING CHANNEL

8. Internal reporting channel

The Company has provided for an internal reporting channel to be used by whistleblowers to send information on breaches. The creation of this channel allows for more effective prevention and detection of breaches. This choice is guided by the principle of fostering a culture of good communication and corporate social responsibility, as well as the improvement of the organisation.

The internal reporting channel allows for reporting to be made in writing or verbally through the "@Whistleblowing" platform' which is available using the following link

https://digitalroom.bdo.it/Assocalzaturifici

By accessing the platform, whistleblowers can also use a voice messaging system to request a direct meeting with the person responsible for managing whistleblowing reports.

The internal reporting channel guarantees the confidentiality of the identity of whistleblowers, facilitators (if applicable), any persons involved or mentioned in reports, as well as the content of reports and relevant documentation that is submitted, including supplementary documentation.

8.1 Party responsible for the management of the channel ("channel manager")

The management of the internal channel is entrusted to Mr Niccolò Scardaccione, Tax Code SCRNCL81P18C933X, born in Como on 18.09.1981 and with offices in Viale Luigi Majno 9, 20122 Milan, an external party satisfying the requirements of autonomy, independence and specific training.

The party in charge of managing the channel and whistleblowing reports has exclusive jurisdiction with regard to the acquisition of reports and access to the platform.

8.2 Characteristics of the internal reporting channel

The Company's internal whistleblowing channel is managed through the web-based "Whistleblowing" platform, which is accessible from all devices (PCs, Tablets, Smartphones).

Data entered into the platform are segregated in the logical partition dedicated to the Company and subjected to a scripting algorithm before being stored. Security in transport is guaranteed by secure communication protocols.

Once a report is submitted (in an anonymous form or otherwise), the platform will issue the whistleblower with a randomly and automatically generated 12-character alphanumeric code, which cannot be reproduced and can be used by the whistleblower at any time to check the status of his/her report and interact with the whistleblowing manager through a messaging system.

In the event of a non-anonymous report, a whistleblower's details ("user data") will not be accessible to the channel manager. The channel manager may, at his or her discretion, view these fields ("visible fields") only after motivation has been provided and appropriately traced on the platform.

A report can only be viewed and managed by the channel manager. The
manager has unique access credentials which expire every 3 months. The
password policy complies with international best practice.

Data Retention is governed by predefined deadlines with automatic reminders sent to the channel manager for data to be deleted.

The company BDO, which provides the platform service, is ISO27001 certified.

The processing of personal data always take into account and complies with the obligations laid down in the GDPR and in Legislative Decree. 196/2003 and as amended.

8.3 Characteristics of whistleblowing reports and anonymous reports

Reports must be as detailed as possible in order to allow the analysis of the facts by persons with the jurisdiction to receive and handle reports. In particular, the following must be clear:

- the time and place at which the reported event occurred;
- the description of the facts;

- the personal details or other elements enabling the identification of the party the reported facts are attributable to.

Information on reported breaches must be truthful. This does not apply to mere conjecture, rumours, information that is in the public domain, incorrect information (with the exception of genuine errors), information that is manifestly unfounded or misleading, or merely harmful or offensive. A whistleblower does not need to be certain the reported facts have actually occurred or of the identity of the perpetrator.

Ideally a whistleblower will provide documents to substantiate reported facts and provide the names of other persons who are potentially aware of the facts.

Anonymous reports, where these are substantiated, are equated with ordinary reports and thereby handled within the scope of this procedure, including with regard to the protection of whistleblowers (where the latter are subsequently identified) and retention obligations.

8.4 Operational procedure for handling a report

The whistleblower sends a report via the dedicated internal channel.

The whistleblower activates the report through the above link, in writing by filling in a guided form, or verbally through a voice messaging system. In the event of a face-to-face meeting, the channel manager shall ensure this takes place within a reasonable timeframe (10-15 days), with the meeting ideally not taking place in company premises.

In the event of the whistleblower making a report verbally at a meeting with the channel manager, this report shall, with the consent of the whistleblower, be documented by the channel manager either by recording it on a device that is suitable for storage and voice playback or by drafting minutes. In the latter case, the whistleblower can verify, correct and/or confirm the minutes of the meeting by signing these.

Receipt of a report by the channel manager initiates the report management process. The channel manager then follows the steps set out in the relevant flow chart.

Within 7 days of receiving a report, the channel manager shall notify the whistleblower that the report has been received and is being processed.

The person in charge of handling the report then proceeds with an initial check on the correctness of the procedure used by the whistleblower and the content of the report, both with reference to the scope defined in this procedure (relevance of the content of the report) and its verifiability, on the basis of the information provided. If a report is not relevant, the channel manager formalises the outcome of the check and communicates this to the whistleblower within a reasonable timeframe (no more than three months) and files the report. The channel manager promptly informs the internal contact person, in accordance with the principle of confidentiality, so that the information can then be shared with the Company.

If additional information is required, the channel manager will contact the whistleblower through the platform. If the whistleblower does not provide the requested additional information within 3 months of the respective request , the channel manager shall file the report and notify the whistleblower and the internal contact person accordingly.

After verifying the relevance of the report and acquiring all the necessary information the channel manager informs the Supervisory Board in accordance with the principle of confidentiality.

At the end of the investigation, the channel manager prepares a final report in order to provide the whistleblower with feedback. Feedback shall be provided to the whistleblower within three months of the receipt confirmation date or upon the expiry of the seven-day period from the submission of the report. Only in exceptional cases, when the complexity

of the report requires this, or in view of the whistleblower's response time, having promptly informed the whistleblower before the deadline, where there is an appropriate justification, the channel manager may continue the investigation for as long as is necessary and provide the whistleblower with periodic updates.
Within the scope of its operational autonomy, the Supervisory Board assesses the relevant outcome and, if a report is well-founded, initiates the necessary communications to the holders of disciplinary power for the organisation to apply any applicable penalties. Any consequent measures are applied in accordance with the provisions of the penalties system set out in the organisation's 231/01 Organisational Model.
In the event of defamation or slander, as ascertained by a conviction, even at the first instance of judgement, the organisation will take action against the whistleblower using the penalties system.
Please note that, from the receipt of a report until its closure, any person with a conflict of interest shall refrain from taking decisions to ensure compliance with the principle of impartiality.

8.5 Transmission of reports to the wrong recipient

In the event of a report being transmitted to a person other than the designated person, the recipient shall send this to the competent person in no more than seven days, notifying the whistleblower accordingly and ensuring a chain of custody of the information in accordance with obligations of confidentiality and those set out in paragraph 8.2. The organisation shall adopt disciplinary penalties in the event of non-compliance with the obligation to forward whistleblowing reports.
In the event of a report being inadvertently sent to a non-designated person, the whistleblower must demonstrate this was solely due to negligence and there was no personal interest involved in this erroneous transmission.

8.6 Retention of documentation on internal reporting

Internal reports and all accompanying or supplementary documentation are retained, with an appropriate digital chain of custody, for the timeframe required to process a report.
In any case, documentation shall be kept for a period not exceeding five years from the date of the communication of the final outcome of the whistleblowing procedure.
In all cases referred to the procedure for retaining internal reports and related documentation shall comply with EU and Italian guarantees on the processing of personal data and the measures in place on confidentiality rights.

9. EXTERNAL REPORTING CHANNEL AND PUBLIC DISCLOSURE

With reference to our Organisation, as an entity operating in the private sector, with a 231 Organisational Model in place and less than 50 workers, an external reporting and public disclosure are not feasible.

This is without prejudice to the possibility of reporting to ANAC any retaliation suffered as a result of a Report

10-. PROTECTION MEASURES AND REPORTING OF RETALIATION

the WB Decree is concerned with protecting Whistleblowers through:

-the obligation to keep their identity confidential;

- prohibiting retaliatory actions against them as a result of a report, including: (i) the possibility of informing ANAC of retaliation one believes to have suffered as a result of a Report; (ii) the provision that renders invalid any acts taken in breach of the prohibition of retaliation, that may also be enforced before courts of law.

- exclusions of liability in the event of the disclosure (or dissemination) of breaches covered by the obligation of secrecy (except in the case of classified information, professional and medical secrecy and secrecy of court deliberations, for which the application of the relevant legislation remains unprejudiced) or which relate to the protection of copyright or personal data protection or information on breaches that may bring offence to the reputation of involved or reported persons, where:

-. at the time of the disclosure (or dissemination) there are reasonable grounds for believing that disclosure is necessary to reveal the breach, and

-. the conditions set out in (a) and (b) below are satisfied;

-. exclusions of liability -unless the act constitutes a criminal offence - for the acquisition of or access to information on breaches;

The Organisation shall protect Whistleblowers in good faith; therefore, the protection measures listed above apply to Whistleblowers and Connected Persons provided that:

-. a) at the time of a Whistleblowing Report, a Whistleblower has reasonable grounds to believe that the information about the reported breaches is true and falls within the scope of the breaches covered by the Whistleblowing policy/procedure;

-. b) the Report is made in accordance with the policy/procedure and the WB Decree.

The protection measures listed above also apply for anonymous Reports, where a Whistleblower is subsequently identified.

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

- dismissal, suspension or equivalent measures;
- demotion or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction on access to training;
- negative appraisals or references;
- the adoption of disciplinary measures or other penalties, including fines;
- discrimination or unfavourable treatment;
- non-renewal or early termination of a fixed-term employment contract;
- early termination or cancellation of a contract for the supply of goods or services;

Actions taken in breach of the prohibition of retaliation are invalid.

The declaration of invalidity for retaliatory acts, likewise, lies with the judicial authority.

ANAC is responsible for the management of notifications of retaliation in the public and private sectors.

Once a Whistleblower proves that he or she has made a Report in compliance with the law and that he or she has been subjected to conduct deemed retaliatory, the onus is on the Employer to prove that such conduct is not related in any way to the Report.

To this end, the alleged perpetrator must provide all elements to demonstrate the absence of retaliatory action against the Whistleblower.

Protection also applies to facilitators, persons in the same work environment as the Whistleblower, and the Whistleblower's work colleagues.

The means through which a Whistleblower - or any other party indicated above - may notify ANAC of retaliation are described in a dedicated section of ANAC's website.

The Organisation shall apply appropriate disciplinary penalties where retaliatory action has been shown to have taken place against a Whistleblower or persons involved in a Whistleblowing Report.

11. PROTECTING THE CONFIDENTIALITY OF WHISTLEBLOWERS

The identity of Whistleblowers and any other information from which their identity may be inferred directly or indirectly shall not be disclosed to persons other than those designated to receive or follow up Reports, without the express consent of Whistleblowers themselves.

In the following two cases, as expressly provided for by the WB Decree, in order to reveal the identity of a Whistleblower, aside from the latter's express consent,

a written statement is required detailing the reasons for this disclosure:

-. during disciplinary proceedings where the disclosure of the identity of the Whistleblower is essential for the defence of the person accused of the disciplinary offence;

-. during proceedings initiated after internal or external Reports where the disclosure of the identity of the Whistleblower is essential including for the defence of the person involved.

If a Whistleblower does not accept the disclosure of his or her identity, the Report cannot be used in the context of the disciplinary proceedings.

Within the context of disciplinary proceedings, the identity of a Whistleblower cannot be disclosed where an accusation of disciplinary offences is based on separate and additional findings to the contents of the Report, even where such findings were made subsequently to the Report. Where an accusation is based, entirely or in part, on a Report and knowledge of the identity of the Whistleblower is essential for the accused person's defence, the Report may only be used for the purposes of disciplinary proceedings where the Whistleblower expressly consents to his/her identity being disclosed.

Moreover, to ensure the complete protection of confidentiality, access to documents relating to Reports and investigation activities shall be granted exclusively to the Whistleblowing Manager.

The prohibition to disclose the identity of Whistleblowers applies to the name of the latter and to all elements of the Report, including attached documentation.

The protection of confidentiality is extended to the identity of persons involved and persons mentioned in a Report until the conclusion of the proceedings initiated as a result of a Report, with the same guarantees provided for Whistleblowers.

Where a Report is received electronically, the protection will consist in an IT Platform that is accessible only to the Manager and which uses an encryption protocol offering enhanced protection of the confidentiality of the identity of Whistleblowers, the content of Reports and attached documentation.

The IT Platform uses a guided computerised procedure to allow for the drafting and sending of Whistleblowing Reports featuring all the elements and information based on the instructions contained in Legislative Decree no. 24 of 2023 and the ANAC Guidelines.

In accordance with the provisions of the prevailing legislation, this IT platform will allow the Organisation to ensure complete protection of the confidentiality of the identity of Whistleblowers, the content of Reports and attached documentation, as it provides for the immediate encryption of Reports through the use of an encryption protocol and instruments to ensure incorruptibility.

The IT platform will be accessible directly through the appropriate section of the organisation's institutional website.

12. EXCLUSION OF WHISTLEBLOWER PROTECTION

The relevant protections are not guaranteed for Whistleblowers in the event of Reports containing false information that is provided intentionally or with gross negligence.

Such conduct may also give rise to disciplinary proceedings or legal action against Whistleblowers.

13. PROTECTION OF REPORTED PERSONS

A Reported Person is a natural or legal person referred to in a Report as being responsible for an alleged infringement or illegal conduct.

The protection of the identity of the person mentioned in a Report must be guaranteed by the Organisation, Whistleblowing Manager, ANAC, and by the administrative authorities to which Reports are forwarded within the scope of their jurisdiction, until the conclusion of proceedings that are initiated as a result of a Report, and with the same guarantees provided for Whistleblowers.

Reported persons may also be heard, at their request, by means of a written procedure through the acquisition of written comments and documents. Reported persons do not have the right to be informed of a Report concerning them, unless disciplinary proceedings are initiated against them based entirely or in part on such Report.

Moreover, Reported person may not ask for the name of Whistleblowers, except in the cases expressly provided for by the law.

14. DISCIPLINARY SYSTEM

In compliance with current legislation, individual National Collective Labour Agreements and internal provisions, in the event of bad faith (slanderous or defamatory) Reports or unlawful or irregular conduct, the Organisation will issue disciplinary penalties:

- against individuals who are responsible for any retaliatory actions or discrimination or unlawful prejudice, be it direct or indirect, against a Whistleblower (or anyone who has cooperated in the investigation of facts that are the subject of a Report) for reasons connected, directly or indirectly, with a Report;
- against a Reported person, for breaches he/she is found to have committed;
- against anyone who breaches confidentiality obligations;
- against employees, as provided by law, who make an unfounded Report intentionally or with gross negligence.
- against employees not complying with the obligation to send Reports to the competent person within 7 days , following incorrect receipt of the report, giving notice of the transmission to the whistleblower and ensuring a chain of custody for information that complies with confidentiality obligations and those set out in paragraph 8.2.

Disciplinary measures will be proportionate to the nature and seriousness of unlawful conduct, and may involve dismissal in the most serious cases.

With regard to third parties (partners, suppliers, consultants, agents, etc.), the remedies and actions provided by law shall apply over and above the contractual clauses on compliance with the Code of Ethics adopted by the Organisation.

15. PENALTIES

Pursuant to the WB Decree, a person who is responsible for any of the following conduct is subject to financial penalties from the ANAC:

-. retaliatory action in relation to Reports;
-. obstructing or attempting to obstruct a Report being made;

-. breach of confidentiality obligations under the policy/procedure and the WB Decree;

- failure to establish Reporting channels according to the requirements of the WB Decree;

-. failure to adopt a policy/procedure for making and handling Reports or failure to comply with the WB Decree;

-. failure to check and analyse Reports that are received.

For all the conduct listed above, the disciplinary penalties provided for in Model 231 shall also be applicable.

In addition, a disciplinary penalty can also be issued against a Whistleblower where:
(i) he/she is found to be guilty, including with a judgement of first instance, of offences of defamation or slander or for the same offences which were committed with a complaint to the judicial or accounting authorities or
(ii) he/she is found to have civil liability, for the same reason, in the event of intentional conduct or gross negligence.
The disciplinary penalties provided for in Model 231 shall also be applicable in such cases.

16. PROTECTION OF PERSONAL DATA - PRIVACY: EVALUATION AND INFORMATION

In the course of the proceedings, the Data Controller (as defined in Article 4, EU Regulation 2016/679) is the Organisation. In connection with the entry into force of the 'Whistleblowing' regulations, one of the tasks of the Data Controller involves adapting the data protection regulations to the current legal provisions.
The data protection policy on whistleblowing Reports will be published on the corporate website and posted on the company notice board.
Internal and external Reports and related documentation are kept for as long as necessary for the processing of Reports, and in any case for no longer than five years from the date of the communication of the final outcome of the Reporting procedure, in compliance with the confidentiality obligations set out in European and Italian legislation on the protection of personal data.
Pursuant to the provisions of the personal data legislation, Legislative Decree No. 24 of 2023 and the ANAC Guidelines, the Data Controller, Data Processors and persons authorised to process personal data are also required to comply with the following fundamental principles:

- process data in a lawful, fair and transparent manner vis-à-vis the data subjects (“lawfulness, fairness and transparency”).
- collect data only for the purpose of managing and following up Reports;
- ensure that data are 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 data subjects for as long as necessary for the processing of a specific Report and in any case no longer than five years from the date of communication of the final outcome of the Report procedure (“limitation of retention”).
- ensure the updating of the register of processing activities
- ensure the prohibition of tracing Reporting channels

- ensure, where possible, the tracing of the activities of authorised personnel in compliance with the safeguards protecting Whistleblowers, in order to avoid the misuse of data relating to a Report; the tracing of any information that could lead to the identity or activity of the Whistleblower being revealed must be avoided.
- process data in a manner that ensures appropriate security of personal data, including protection, through appropriate technical and organisational measures, to prevent unauthorised or unlawful processing and accidental loss, destruction or damage ("integrity and confidentiality"). In the context in question, which is characterised by high

  risks for the rights and freedoms of data subjects, the use of encryption tools within the internal and external reporting channels is deemed n appropriate measure for implementing by design and default the principle of integrity and confidentiality.

17. TRAINING AND VISIBILITY OF THE WHISTLEBLOWING POLICY/PROCEDURE

Whistleblowers and the Persons involved shall be provided with appropriate information pursuant to Articles 13 and 14 of the GDPR. The Data Protection Policy is made available through:

-. publication on the whistleblowing page of the institutional website;

-. link (to the above page) inserted in the Online Portal;

-. Emailed to all employees and co-workers.

Whistleblowing training is also included in staff training plans