WHISTLEBLOWING POLICY
COMPANY PROTOCOL

TABLE OF CONTENTS

1) TERMS AND DEFINITIONS
2) LEGAL BACKGROUND TO THE PROTOCOL
3) PURPOSE OF LEGISLATION
4) PERSONS WHO CAN SUBMIT WHISTLEBLOWING REPORTS AND BENEFIT FROM LEGAL PROTECTION
5) PROTECTED PERSONS OTHER THAN THE REPORTING PERSON
6) SYSTEM OF PROTECTIONS AND SUPPORT MEASURES GRANTED TO THE REPORTING PERSON
7) OBJECTIVE SCOPE
8) HOW TO SUBMIT REPORTS IN THE ORGANISATION
9) REPORT HANDLING SYSTEM
10) CONFIDENTIALITY OBLIGATIONS CONCERNING THE IDENTITY OF THE REPORTING PERSON
11) DATA PROCESSING IN COMPLIANCE WITH PRIVACY LEGISLATION

1. TERMS AND DEFINITIONS

To facilitate consultation and understanding of this Protocol, the main terms used are defined below. The same terms are used on the platform that the Data Controller uses to handle reports.

"**ANAC**"	Italian Anti-Corruption Authority
"**GDPR**"	Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
"**Reporting person**" or **"Whistleblower"**	Person who is entitled to make a Report, pursuant to Legislative Decree No. 24 of 10 March 2023 ("Whistleblowing Decree") implementing EU Directive 2019/1937 and, in general, this Whistleblowing Protocol.
"Manager"	Manager responsible for handling reports, a person appointed by the Company to receive and handle/investigate whistleblowing reports, with an obligation to keep the information acquired confidential
"Reporting channel"	System for reporting a breach under the Whistleblowing law. Reporting channels can be of three types: internal, external (managed by ANAC) or public disclosure
Public Disclosure	With public disclosure, information on breaches is brought into the public domain through the press or online, i.e. using distribution methods capable of reaching a large number of people.
"**Collaborator"**	Person inside or outside the company, identified by the organisation and appointed by the Manager to carry out report-handling support activities.
"**Third Party"**	Person who may be involved as a witness, person informed of the facts or accused party. The third-party reports exclusively to the Manager and may provide supplementary elements useful for investigations and assessments.
"**Protected Persons other than the reporting person**"	Persons who could be subject to retaliation due to their role in the reporting or complaint process or due to a special relationship established with the reporting person, who are granted protection.
"Facilitator"	Natural person assisting the reporting person in the reporting process.
"Entities"	Enterprises, companies and/or associations
"Platform"	Tool chosen as an internal reporting channel, which allows reports to be made, in compliance with legislative requirements and maintaining absolute confidentiality.
"Breaches"	Offences and breaches falling within the scope of Legislative Decree 24/2023 and this Protocol
"Organisation"	Subject (Enterprise, Company, other type of Entity) to which the Whistleblowing Decree and this Protocol apply

2. LEGAL BACKGROUND TO THE PROTOCOL

Legislative Decree No. 24 of 10 March 2023 on "the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws" was issued to transpose *Directive (EU) 2019/1937.*

Legislative Decree 24 /2023 consolidates all the rules governing reporting channels and the protections granted to whistleblowers in public and private sectors. The Decree entered into force on 30 March 2023, and its provisions take effect on 15 July 2023 and 17 December 2023.

Under Article 10(1) of Legislative Decree No 24/2023, ANAC, after consulting the GDPR, adopted the "*Guidelines on the protection of persons who report breaches of Union law and the protection of persons who report breaches of national laws. Procedures for the submission and management of external reports," by Resolution No. 311 of 12/07/2023.*
These Guidelines are intended to provide instructions for the submission and handling of reports and to provide information and principles that affected organisations may consider when establishing their own internal organisational channels and forms. The information in this document is based on these guidelines.

3. PURPOSE OF LEGISLATION

The legislation aims to enhance principles of legality and transparency in complex organisations, by creating conditions that allow reports by company stakeholders to reveal the emergence of situations of irregularity and illegality that could be detrimental to the organisation and the general interest, removing any obstacles that prevent such situations being revealed.

MAIN ASPECTS OF LEGISLATIVE DECREE 24/2023	**The main new features of the recent regulation concern**: ➢ Extension of the subjective scope as regards the entities required to apply the legislation ➢ Indication of natural persons who can be protected when making reports, complaints or public disclosure; ➢ Identification of what is considered a breach that entitles the reporting person to protection, as well as the distinction between what is protected and what is not; ➢ The system of three reporting channels and conditions for accessing them: internal (in entities with a dedicated person or office or through an external person with specific expertise) or external (managed by ANAC) and the public disclosure channel; ➢ The different ways of submitting reports, in written or verbal form; ➢ detailed rules on confidentiality obligations and the processing of personal data received, handled and disclosed by or to third parties; ➢ clarification of what is meant by retaliation, and extension of the scope; ➢ rules on the protection of whistleblowers or persons reporting retaliatory measures offered by both ANAC and the judiciary, and more guidance on the responsibility of the reporting persons and on exculpatory measures; ➢ the introduction of special support measures for reporting persons and the involvement, for this purpose, of third sector entities that have appropriate expertise and provide their services free of charge; ➢ a review of the rules on sanctions applicable by ANAC and the introduction of sanctions by private entities into the disciplinary system adopted pursuant to Legislative Decree No. 231/2001.

4. PERSONS WHO CAN SUBMIT WHISTLEBLOWING REPORTS AND BENEFIT FROM LEGAL PROTECTION

A reporting person means a natural person who reports or publicly discloses using means designed to reach a large number of people, or reports to the legal or accounting authorities information on breaches acquired in the context of his or her work-related activities. This definition includes, inter alia, all persons who are, even temporarily, in a valid working relationship with the company (employees, consultants, freelancers, collaborators, suppliers of goods and services, agents, shareholders, persons exercising functions of

administration, management, control, supervision or representation, volunteers, trainees, whether paid or unpaid, and, subject to certain conditions, those who have not yet entered into a legal relationship with the organisation (in pre-contractual negotiations), as well as those whose relationship has ended or who are on probation.
The whistleblower must necessarily be a natural person, and therefore reports submitted by other persons, including representatives of trade unions, will not be taken into account, since the institution of whistleblowing is aimed at protecting the individual person acting on his or her own behalf, not under a trade union banner. In the latter case, reports will be shelved as they do not meet the subjective requirement laid down in the legislation.

5. PROTECTED PERSONS OTHER THAN THE REPORTING PERSON

Legislative Decree no. 24/2023 strengthens protection for whistleblowers, extending it to persons other than whistleblowers, confirming the legislator's intention to create conditions that make the institution in question an important safeguard for ensuring the legality and good standing of entities.
Protection is granted to all persons who make reports, complaints and public disclosures, as well as those who might be the targets of retaliation, even indirectly, due to their role in the reporting, public disclosure or complaint process and/or the particular relationship that links them to the reporting person or complainant, i.e.:

- **The facilitator,** meaning the natural person who assists the reporting person in the reporting process, such as a colleague in the reporting person's office, or in another office, who assists the reporting person on a confidential basis, or who holds the status of trade unionist if he or she assists the reporting person in his or her own name, without using the trade union banner (if, on the other hand, he or she assists the reporting person under the trade union banner, he or she is not acting as a facilitator, unless otherwise provided for in provisions on the consultation of trade union representatives and the repression of anti-union conduct set out in Law No 300/1970);
- **persons in the same work environment as the reporting person**, complainant or person making a public disclosure and who are bound to them by a stable emotional or familial relationship up to the fourth degree; in the Decree, the concept of “work environment” covers current or past work or professional activities, irrespective of their nature, that lead a person to acquire information on breaches and in the context of which he or she might be exposed to retaliation in the event of a report or public disclosure or a complaint to the judicial or accounting authorities; e.g. colleagues, former colleagues, collaborators; a prerequisite for the application of protection in such cases, however, is the existence of a stable emotional or relationship link up to the fourth degree with the reporting person;
- **work colleagues with a habitual and current relationship with the reporting person**, complainant or person making a public disclosure; persons who, at the time of the report, work with the reporting person (thus excluding former colleagues) and who have a relationship with the latter that is not merely sporadic, occasional, episodic and exceptional, but is current, long-term and characterised by a certain continuity that determines a relationship of “communality” or friendship;
- **entities: (a)** all or a majority of which are **owned** by third parties, by the reporting person, complainant or person making a public disclosure**; (b) where** the reporting person, complainant or person making a public disclosure **works** (Article 3(5)(d)); **c) who work in the same employment** context as the reporting person, complainant or person making a public disclosure.

6. SYSTEM OF PROTECTIONS AND SUPPORT MEASURES GRANTED TO THE REPORTING PERSON

A central pillar of the new rules is the system of protections offered to a person making a report, public disclosure or complaint regarding breaches. These protections extend to persons other than the reporting person and complainant who could be at risk of retaliation because of their role in the reporting process and/or the special relationship between them and the reporting person. The protection system covers:

➢ The **confidentiality** of the reporting person, the facilitator, the person involved and the persons mentioned in the report; the identity of the reporting person, and any other information from which that identity may be directly or indirectly inferred, may not be disclosed to persons other than those competent to receive or follow up reports without the express consent of the reporting person;

➢ **possible retaliation by the entity due to the report**, public disclosure or complaint made and the conditions for its application; the Decree provides for the protection of the whistleblower, for the prohibition of retaliation defined as "any conduct, act or omission, even if only attempted or threatened, carried out due to the report, judicial disclosure or public disclosure and which causes or may directly or indirectly cause the reporting person or the person filing the complaint unfair damage"; the following are examples of retaliation**:** **a)** dismissal, suspension or equivalent measures; **b)** demotion or non-promotion; **c)** change of duties, change of workplace, reduction of salary, change of working hours; **d)** suspension of training or any restriction on access to training; **e)** demerit notes or negative references; **f)** adoption of disciplinary measures or any other sanction, including a fine; **g)** coercion, intimidation, harassment or ostracism; **h)** discrimination or any other unfavourable treatment; **i)** failure to convert a fixed-term employment contract into a permanent employment contract, where the employee had a legitimate expectation of such conversion; **j)** non-renewal or early termination of a fixed-term employment contract**; k)** damage, including to a person's reputation, particularly on social media, or economic or financial loss, including loss of economic opportunities and loss of income **(l)** improper listing on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future; **(m)** early termination or cancellation of a contract for the supply of goods or services; **(n)** cancellation of a licence or permit; **(o)** application for psychiatric or medical examinations.

The conditions for applying protection from retaliation are as follows:
a) the person has reported, complained of or made a public disclosure based on a reasonable belief that the information on the reported, disclosed or complained of breaches is true and within the objective scope of the decree;
b) the report or public disclosure was made in compliance with the rules laid down in Legislative Decree no. 24/2023;
c) there must be a consequential relationship between the report, disclosure and complaint made and the retaliatory measures taken;
d) mere suspicions or rumours are not sufficient. Alleged retaliation, even if only attempted or threatened, must be reported exclusively to ANAC, which is tasked with ascertaining whether it is a consequence of the report, complaint or public disclosure made.
Protection also extends to cases of retaliation following a report submitted to the competent European Union institutions, bodies and agencies. If ANAC finds that retaliation has taken place, the retaliatory measure is cancelled and an administrative fine is imposed on the person who adopted the retaliatory measure/act or to whom the conduct and/or omission is attributable; in the event of dismissal, the dismissal is cancelled and the person is entitled to reinstatement in the workplace.

➢ **Limitations of liability regarding disclosure and dissemination of certain categories of information that operate under certain conditions.** The set of protections afforded by the rules to the reporting person, complainant or person making a public disclosure include limitations of liability regarding the disclosure and dissemination of certain categories of information. These limitations operate under certain conditions, in the absence of which there would be consequences in terms of criminal, civil and administrative liability. They concern: a) Offences that cannot be categorised as such in cases of dissemination of information covered by the obligation of secrecy if the exemption applies, in particular with regard to: disclosure and use of official secrets (Article 326 of the Criminal Code); disclosure of professional secrets (Article 622 of the Criminal Code); disclosure of scientific and industrial secrets (Article 623 of the Criminal Code); breach of the duty of loyalty and faithfulness (Article 2105 of the Civil Code); b) breach of the provisions on the protection of copyright; c) breach of personal data protection provisions; d) disclosure or dissemination of information on breaches that damage the reputation of the person involved. Two conditions must be fulfilled cumulatively for the exclusion

of liability to operate in cases of information dissemination: 1) that at the time of the information disclosure or dissemination there are reasonable grounds to believe that the report or dissemination is necessary to reveal the breach; 2) the report, public disclosure or complaint must be made in compliance with the conditions that the legislator has laid down in Legislative Decree No. 24/2023 as requirements for benefiting from the protections. Liability is also excluded in the event of lawful access to the reported information, or to documents containing that information, as well as the exclusion of criminal liability and any other liability, including civil or administrative liability, for the conduct, acts or omissions if they are connected with the reporting, complaint and public disclosure and strictly necessary to reveal the breach.

In order to strengthen the effectiveness of the protections provided for by the Decree, the legislator has also provided for measures that enable the reporting person to be supported by third sector entities listed by ANAC on its institutional website. They provide assistance and advice free of charge:

- on how to report;
- on the protection against retaliation granted by national and EU legislation;
- on the rights of the person involved;
- on the terms and conditions of access to legal aid.

This broad form of protection is intended to ensure that the reporting person is better able to submit a report and his or her identity is better protected, while ensuring the reported person's right of defence.

Unless otherwise provided for in the exceptions set out in Legislative Decree No. 24/2023, the person responsible for handling the report is authorised to disclose the identity of the reporting person to other persons only with their express consent

CASES OF EXCLUSION:

The protection provided in the event of retaliation does not apply if the reporting person is found guilty of criminal liability for the offences of slander or defamation or of the same offences committed with the complaint, or of civil liability for having intentionally reported false information maliciously or frivolously, even if the preliminary sentence is not final. If liability is established, a disciplinary sanction will also be imposed on the reporting person or complainant.

7. OBJECTIVE SCOPE

Legislative Decree No. 24/2023 provides that information on breaches, including well-founded suspicions thereof, of national and European Union law, affecting the public interest or the integrity of the public administration or the private entity committed within the organisation of the entity with which the reporting person or complainant is engaged in one of the legal relationships considered valid by the legislator is subject to reporting, public disclosure or complaint. Information on breaches may also relate to breaches not yet committed that the whistleblower reasonably believes could be committed on the basis of factual evidence. These may also be irregularities and anomalies (symptomatic indicators) that the reporting person believes could give rise to one of the breaches provided for in the Decree.
The legislator identifies certain types of offences to be considered and only these are relevant for a report, public disclosure or complaint to be considered eligible for purpose of the regulations.

The legislature has categorised the following types of breaches:

➢ Breaches of national regulations:

This category includes criminal, civil, administrative or accounting offences other than those specifically identified as breaches of Union law as defined below. Secondly, the breaches under consideration include:

- predicate offences within the scope of Legislative Decree No. 231/200132;
- breaches of the organisational and management models provided for in Legislative Decree No. 231/2001 above, which are also not categorised as breaches of Union law as defined below.

Such breaches do not constitute predicate offences within the scope of Legislative Decree No. 231/2001 and relate to organisational aspects of the entity that adopts them.

➢ Breaches of Union legislation:

- Offences committed in breach of Union legislation listed in Annex 1 to Legislative Decree No. 24/2023 and all national implementing provisions (even if these are not expressly listed in the said Annex). The reference to the legislative provisions set out in Annex 1 is to be understood as a dynamic reference as it naturally has to be adapted to changing legislation.
  In particular, these offences relate to the following areas: public procurement; services, products and financial markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and animal feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and the security of networks and information systems.
  Examples include environmental offences such as the discharge, emission or other release of hazardous materials into the air, soil or water, or the unlawful collection, transport, recovery or disposal of hazardous waste.
- Acts or omissions that are harmful to the financial interests of the European Union (Article 325 TFEU fight against fraud and illegal activities affecting the financial interests of the EU) as identified in EU regulations, directives, decisions, recommendations and opinions.
  Examples include fraud, corruption and any other illegal activity related to EU expenditure.
- Acts or omissions relating to the internal market that negatively affect the free movement of goods, persons, services and capital (Article 26(2) TFEU). These include breaches of Union competition and State aid rules, breaches of the rules of corporate tax or arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.
- Acts or conduct that defeat the object or purpose of Union law in the areas indicated above. These include, for example, abusive practices as defined by the case law of the Court of Justice of the European Union.
  An example would be an undertaking operating in a dominant market position. The law does not prevent such an undertaking from gaining a dominant position on a market on its own merits and abilities, nor does it ensure that less efficient competitors remain on the market. However, such an undertaking could, by its conduct, undermine effective and fair competition in the internal market by resorting to abusive practices (adoption of predatory pricing, targeted discounts and cross selling) in breach of the rules of free competition.

However, an evidence-based, case-by-case check must be carried out (e.g. by looking at sector regulations and similar cases examined by case law) in order to determine whether such acts or omissions can be categorised as breaches covered by Legislative Decree No. 24/2023.

Evidence of conduct aimed at concealing breaches may also be the subject of reporting, public disclosure or complaint. One example is the concealment or destruction of evidence that a breach has been committed.

Complaints, claims or requests that are purely in the personal interest of the reporting person or a person who has filed a complaint with the judicial authority that relate exclusively to his or her individual work or public employment relationships or to relationships with people in hierarchically senior roles cannot be reported.

Information on breaches eligible for reporting or complaint does not include information that is clearly unsubstantiated, information that is already fully in the public domain, or information acquired solely on the basis of rumours or unreliable hearsay (gossip).

The report must be as detailed as possible so that the facts can be assessed by the persons competent to receive and handle reports, as well as by ANAC.

ANONYMOUS REPORTS → Reports from which the identity of the reporter cannot be established are considered anonymous. Anonymous reports, where substantiated, are treated like ordinary reports.
The organisation keeps the anonymous reports received, and the relevant documentation, for no longer than five years from the date of receipt, so that they can be traced if the reporting person or the person who filed a complaint informs ANAC that he or she has suffered retaliatory measures as a result of that anonymous report or complaint. A subsequently identified anonymous reporting person or complainant who has informed ANAC that he or she has suffered retaliation is entitled to benefit from the protection that the Decree guarantees against retaliatory measures.
The IT platform adopted for handling whistleblowing reports also allows reports to be submitted anonymously; these reports can be supplemented at a later stage with the identity of the reporting person.

8. HOW TO SUBMIT REPORTS IN THE ORGANISATION

INTERNAL CHANNEL
To comply with the law, and given that whistleblowing is a corporate compliance tool, the Organisation offers a reporting **system** based on the **DigitalPa S.r.l. '*LEGALITY WHISTLEBLOWING*'** platform**.**

This online channel was chosen due to the following attributes:
- Compliance with data protection obligations under the GDPR;
- Total anonymity, in the event of anonymous reporting, even during the post-reporting communication phase;
- DATA ENCRYPTION (any content and data uploaded can only be read by the reporting person and the whistleblowing manager);
- Activation of read receipts for any messages from the whistleblowing manager, allowing the flow to be easily monitored;
- Possibility of implementing multilingual systems;
- Access rights defined for users and profiles on a need-to-know basis;
- 24-hour access for reporting from devices and applications;
- Channel accessible to all stakeholders eligible to report;
- Facilitated registration and request processing times;
- Secure transmission of files and documents;
- The system is simple and intuitive to use and ensures technical and regulatory compliance with current guidelines on the subject. It provides prompt updates on new versions of the application and the legislative framework;
- Compliance with all the required characteristics.

For specific information on using the platform, see the ***Whistleblower's Operating Guide*** on the platform.

EXTERNAL CHANNEL
Access to the external channel - **ANAC** - is permitted only under certain conditions expressly provided for by the legislator, which are as follows:
a) the obligatory internal channel is not active, or is active but does not comply with the legislator's requirements concerning subjects and the report submission procedure;
b) the person has already made an internal report but it has not been followed up**;**
c) the reporting person has reasonable grounds to believe that an internal report would not be effectively followed up, or that it could lead to a risk of retaliation;
d) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest. The external channel activated by ANAC guarantees, including through the use of encryption tools, confidentiality regarding the identity of the reporting person, the person involved and the person mentioned in the report, as well as the content of the report and related documentation. Click

on the link to the dedicated page of ANAC's institutional website to access the whistleblowing service (https://www.anticorruzione.it/-/whistleblowing).

OTHER OPTIONS

Public Disclosure. Public disclosure is permissible under the following conditions: **a)** an internal report to which the organisation has not provided a response within the specified time frame has been followed up by an external report to ANAC which, in turn, has not responded to the reporting person within a reasonable time frame; **b)** the person has already made an external report to ANAC directly, but ANAC has not provided a response as to the measures envisaged or adopted to follow up the report within a reasonable time frame; **c)** the person makes a public disclosure directly because he or she has reasonable grounds for believing (based on concrete circumstances and not on mere inferences) that the breach may represent an imminent or obvious danger to the public interest; **d)** the person makes a public disclosure directly because he or she has reasonable grounds for believing that an external report may involve a risk of retaliation or may not be effectively followed up.

Report to the judicial authority. Legislative Decree No. 24/2023 also offers protected persons the option of approaching the judicial authorities to file a complaint of unlawful conduct that they have become aware of in a public or private work-related context.

9. REPORT HANDLING SYSTEM

The whistleblowing manager is the person with operational responsibility for receiving and taking charge of the reports (**within 7 days**), assessing that the reports are eligible, initiating the relevant investigation, maintaining contact with the whistleblower, and providing him or her with feedback **within three months** of the date the report was received.
He or she is legally entitled to process the personal data of the reporting person and, where appropriate, to know his or her identity.
The whistleblowing manager can call upon the support of a dedicated working group to carry out his verification and analysis activities if the corporate organisation has established such a group; the working group is made up of individuals whose competences are cross-cutting with regard to the organisation's main duties. The Organisation appoints the members by means of a special act, and they receive personal data processing instructions from the manager. The group members, who may be classified as collaborators, can view the reports but not the reporting person's identification data.
They are, however, subject to the same confidentiality constraints as the manager.
For all specifications on requirements and activities related to the role of the manager, please see the **specific guide drawn up by the organisation.**

The organisation has introduced a specific and detailed PROCEDURE covering all the information, steps and salient details of the management system adopted. This aims to remove factors that could hinder or discourage its use, such as doubts, uncertainties or fears of retaliation or discrimination.

At least once a year, the Management calls a meeting of its managers in order to assess the adequacy and effectiveness of the planned whistleblowing system. Collaborators and people working in roles that are not directly involved but who can provide input for the assessment may also be invited to take part in this review. Any statistical reports produced by the platform, any relevant cases and any difficulties encountered, will be analysed during the review so that any necessary changes or additions can be made to the procedure.
No personal or confidential information should be mentioned in the context of the review, only procedural and managerial observations.

10. CONFIDENTIALITY OBLIGATIONS CONCERNING THE IDENTITY OF THE REPORTING PERSON

In compliance with the fundamental principles of personal data protection, such as limitation of purpose and data minimisation, the Decree expressly states that reports may not be used over and above what is necessary to provide adequate follow-up.

The identity of the reporting person and any other information from which his or her identity may be inferred, directly or indirectly, may not be disclosed to persons other than those competent to receive or follow up the reports without the express consent of the reporting person.

CONFIDENTIALITY OF THE REPORTING PERSON IN A JUDICIAL CONTEXT
In **criminal proceedings**, the identity of the reporting person is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.
This provision provides for the obligation of secrecy over actions performed in the preliminary investigation *"until the defendant can have knowledge of them and, in any case, no later than the closure of the preliminary investigation"* (notification of which is provided for in Article 415-bis of the Code of Criminal Procedure).
Afterwards, the judicial authority may disclose the identity of the reporting person for use in the proceedings.

CONFIDENTIALITY OF THE REPORTING PERSON IN DISCIPLINARY PROCEEDINGS
Within the framework of **disciplinary proceedings** initiated by the Organisation against the alleged perpetrator of the reported conduct, the identity of the reporting person may not be disclosed, where the alleged disciplinary charge is based on investigations that are separate from and additional to the report, even if instigated as a consequence of it. If the charge is based, in whole or in part, on the report and knowledge of the identity of the reporting person making the report is indispensable for the accused's defence, the report can only be used for the purposes of disciplinary proceedings **if the reporting person expressly consents to his or her identity being disclosed**.
The Decree then expressly sets out **two options** in which **prior written notice of the reasons for the need to disclose the** identity of the reporting person and the **reporting person's prior express consent** are required in order to reveal the identity of the reporting person**.**

- The identity of the reporting person is **indispensable for the defence of the person charged with the disciplinary offence**
- The identity of the reporting person is **also indispensable for the defence of the person involved**

Breach of the confidentiality obligation is punishable by ANAC.

11. DATA PROCESSING IN COMPLIANCE WITH PRIVACY LEGISLATION

Personal data must be processed in accordance with and in compliance with the EU Privacy Regulation 679/2016; responsibility for the correct processing of personal data lies with the Data Controller, the company has set up its own personal data processing system (company privacy policy), which can be consulted at the relevant office. The main points of the whistleblowing law are set out below.

Storage times *(see Article 14 of Legislative Decree 24/2023)*
Internal and external reports, and related documentation, are stored for as long as necessary to process the report and, in any case, **no longer than five years from the date on which the final outcome is notified.**
In the event of legal proceedings, the storage period may be extended until the case is concluded.
If data or information must be stored to comply with other regulations, reference will be made to the regulations in question.

Formalisation of roles and positions
When entrusting activities to managers and collaborators, data processing assignments must always be formalised, whether the assignments are internal under Article 29 GDPR or external under Article 28 GDPR. When appointing individuals, checks must always be carried out to ensure that they have the necessary skills and have received the required training.

Data controllers, and therefore data processors and persons authorised to process personal data, are required to comply with the fundamental principles summarised below:

- Process data in a lawful, correct and transparent manner
- Collect data for the sole purpose of handling and following up reports, public disclosures or complaints
- Ensure that data are adequate, relevant and limited to what is necessary for the purposes for which they are processed
- Ensure that data are accurate and up-to-date
- Store data for as long as necessary to process the specific report
- Ensure the data are processed in such a way as to guarantee the security of personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction and damage
- Respect the principles of privacy by design and privacy by default
- Carry out a data protection impact assessment
- Provide possible data subjects with advance information on the processing of personal data by publishing or handing over the privacy policy
- Ensure the register of processing activities is updated
- Ensure that reporting channels do not allow tracing
- Ensure, where possible, that the activity of authorised personnel is traceable in compliance with safeguards protecting the reporting person.