WHISTLEBLOWING PROCEDURE (WHISTLEBLOWING)

		SIGNATURE (digital or analogue)
CREATED	ADACTA TAX & LEGAL AVV. LUCA DE MURI	
CONTROLLED	ADACTA TAX & LEGAL AVV. LUCA DE MURI	
APPROVED	CDA represented by MANAGING DIRECTOR (DOTT. FEDERICO PELLINI)	PELLINI CAFFE' S.p.A. Il Consigliere Delegato
VERSION	2.0	
DATE	11/03/2026	
VERSION NOTES	• Added clarifications on certain types of reportable Breaches • Inserted new Violation related to anti-money laundering / self laundering • Inserted coordination between the ODV231 and other Case Managers in the case of a single reporting channel • Inserted additions regarding the replacement of temporarily incapacitated Case Managers • Integrations regarding internal assignment of report management • Integrations regarding conflict of interest and coordination of the clause with the possibility of external reporting to ANAC • Clarifications regarding the alternation of oral reporting channels • Integrations for the case of receipt of reports sent by the reporter by e-mail • Supplements for the case of receipt of the report by more than one person, some of whom are not competent • Supplements on the consequences of the inadmissibility of the report	

	• Supplements regarding the assessment of the existence of the preconditions for the protection of the whistleblower • Clarifications on information flows from the Case Manager to senior bodies • Clarifications on feedback to the Whistleblower within 3 months from the date of the report • Clarification on whistleblowing training • Supplement on lessons learned • Clarification on whistleblower's dialogue with ETS - third sector entities • - Integration on the time limit for deletion of personal data after 5 years from the final decision	

Summary

1. PURPOSE AND SUBJECT MATTER

The purpose of this Whistleblowings Management Policy (hereinafter, the "**Policy**" or "**Procedure**") is to define and establish an adequate and efficient model for the operation of the Internal Information System (or "**Whistleblowings Management System**") that enables the receipt and processing of notifications of acts or omissions that may constitute Sectoral Violations, in accordance with:

- the relevant legislation 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 (hereinafter, the "**Whistleblowing Directive**"), and
- to Legislative Decree 24/2023, and
- to the ANAC Guidelines

The Procedure aims to facilitate the correct implementation of EU law (legal certainty) and, therefore, to ensure the "**well-being**" of the Company. The objective is the '**transparency**' of private action, which is the road to a truly virtuous company. The Company also handles Whistleblowings to **avoid incurring detrimental effects** related to Violations (e.g. negative publicity on the market).

The purpose of this Policy is to **ensure professional, confidential, impartial handling and adequate protection of the rights of the persons concerned** throughout the process of making, handling, processing, investigating and resolving Reports made through the Company's Internal Reporting Channel.

This Policy **governs** the roles, processes and tools for the functioning of the Company's Internal Reporting Channel, in such a way as to **regulate matters relating to the communications made by Whistleblowers, as well as their management and resolution** by the System Manager.

The procedures for the processing, investigation and resolution and, in general, the management of the Reports received pursuant to this Procedure shall be governed by the utmost **objectivity and independence**, establishing in this Procedure the corresponding mechanisms in order to avoid the concurrence of possible conflicts of interest.

Furthermore, the rights to be informed of the actions or omissions attributed and the presumption of innocence of the Persons Concerned are guaranteed by this Procedure.

2. DEFINITIONS AND SCOPE OF APPLICATION

2.1. Definitions

For the purposes of this Procedure, the following definitions apply:

ANAC - Autorità Nazionale Anticorruzione (or **Competent Authority**)	*Independent Italian administrative authority designated to (i) receive External Reports and (ii) perform the functions provided for by the Directive, including responding to the Whistleblower, in particular with regard to the Follow-up given to the Reports, and imposing any sanctions, in the cases provided for by the applicable legislation*

Sectorial Acts	*Regulatory acts identified in **Appendix A** of this Procedure*
Reporting Channels	*Channels for making Reports, made available to the Whistleblower, respectively, by the Company, in the case of Internal Reporting, or by the ANAC in the case of External Reporting;* *Internal Reporting Channels are in turn defined as Internal or External depending on whether they are managed directly by the Company or by third parties authorised by it*
Reporting Committee	*Collegial body made up of any additional Case Managers designated from time to time by the Company*
Work context	*Work or professional activities, present or past, carried out in the context of Legal Relations, through which, regardless of the nature of such activities, a person acquires information on Violations and in the context of which he/she could risk being retaliated against in the event of a Whistleblowing or Public Disclosure or a report to the Judicial Authority*
Whistleblowing Decree	*Legislative Decree 24/2023 implementing the Whistleblowing Directive in Italy*
Public Disclosure	*Placing information on Breaches in the public domain through the press or electronic media or in any case through means of dissemination capable of reaching a large number of people (e.g. radio, television, blogs, Internet, automated e-mail campaigns)*
Whistleblowing Directive	*EU Directive 2019/1937 on the protection of persons who report breaches of Union law*
Third Sector entities	*Entities that have entered into agreements with ANAC to provide the specific Support Measures under their competence pursuant to the Whistleblowing Decree. They never take on the role of Facilitator.*
Facilitator	*A natural person who assists a Whistleblower in the Whistleblowing process, operating within the same work context and whose assistance must be kept confidential, including a trade unionist if he/she assists the Whistleblower in his/her name and on his/her behalf, without using the trade union's initials*
Case Manager	*Person(s) designated under this Procedure to receive the Report and/or carry out the further activities for the management of the Report provided for in this Procedure*
GDPR	*EU Data Protection Regulation 679/2016*
Violation Information	*Information, including reasonable suspicion, concerning:* *(i) Violations committed or which, on the basis of concrete evidence, could be committed in the organisation with which the Whistleblower or the person making the complaint to the judicial or accounting authority has a legal relationship; and* *(ii) information concerning any conduct aimed at concealing such Violations*

Whistleblowing Privacy Policy	*Information communicated pursuant to articles 13-14 of the GDPR by the Company to the Interested Parties*
ANAC Guidelines	• *ANAC Guidelines on the protection of persons who report violations of Union law and the protection of persons who report violations of national laws - Procedures for the submission and management of external reports (approved by resolution No. 311 of 12 July 2023 - Outline of new guidelines on whistleblowing 07 November 2024), and* • *Regulations for the management of external whistleblowing and for the exercise of ANAC's sanctioning power in implementation of Legislative Decree 24/2023 (approved by Resolution No. 301 of 12 July 2023).*
Protection measures	*Measures provided for in **paragraph 2** of **Appendix B** of this Procedure*
Support measures	*Measures provided for **in paragraph 6** of **Appendix B to** this procedure*
Organisational Model 231	*Organisational, Management and Control Model possibly adopted by a Company in Italy, pursuant to Legislative Decree No. 231/2001, as amended*
Supervisory Board 231 (or "**SB 231**")	*Supervisory Body appointed by the Company in relation to the Organisational Model 231*
Involved Person (or **Reported Person**)	*Natural or legal person to whom is attributed, through or during the course of the Report or Public Disclosure or Complaint to the Judicial Authorities, the responsibility in any capacity whatsoever of the Violation reported or publicly disclosed or denounced*
Portal/Software	*The third party cloud portal, accessible on the Internet at https://pellinicaffewb.integrityline.com, including user usable functionalities and its secure database*
Procedure	*This document*
Procedures	*The set of directives, instructions, protocols and written procedures provided for and implemented by the Company in order to prevent Violations, and/or to reduce their consequences or recurrence*
Legal relationship	*Legal relationship between the Whistleblower and the organisation in which a Violation has been committed or may be committed;* *The legal relationship may be direct or indirect (i.e. through a third party having a direct legal relationship with the Company).*
Reporting Register	*Software in which to register reports*
Redress	*Communication to the Whistleblower of information on the follow-up given or intended to be given to the Report, including the acknowledgement of receipt of the Report*

Retaliation	*Any conduct, act or omission, even if only attempted or threatened, carried out by reason of the Report or of the denunciation to the judicial authority or of the Public Disclosure and which causes or may cause to the person making the Report or having made the Report, directly or indirectly, an unjust damage*
Administrative sanctions	*Administrative pecuniary sanctions applicable by ANAC against non-compliance under the Whistleblowing Decree*
Disciplinary sanctions	*Disciplinary sanctions applicable by the Company in the event of non-compliance with the provisions of this procedure*
Whistleblower	*Natural person, who makes the Report or Public Disclosure of Information on Violations acquired in the context of his or her own work context*
External Reporting	*Disclosure of Information on Breaches by the Whistleblower submitted through the Reporting Channel activated by ANAC*
Internal Reporting	*Communication of Information on Breaches, submitted through the Reporting Channels made available by the Company*
Follow-up	*Action taken by the Case Manager or the Reporting Committee to assess the existence of the facts reported, the outcome of the investigation and any measures taken*
Internal Information System	*Portal/Software*
Company	*Company indicated in Art. 3.2.1*
Persons in the Private Sector	*Subjects, other than those falling within the definition of Public Sector Subjects*
Public Sector Subjects	• *Public Administrations referred to in Article 1(2) of Legislative Decree No. 165/2001* • *Public Economic Bodies* • *Bodies governed by public law referred to in Art. 3, co. 1, lett. d), Legislative Decree 50/2016,* • *Public service concessionaires,* • *Publicly controlled companies referred to in Art. 2, co. 1, lett. m) of Legislative Decree 175/2016, even if listed,* • *In-house companies referred to in Art. 2, co. 1, lett. o) of Legislative Decree 175/2016, even if listed*
External Parties	*Reporting Parties other than Internal Parties*
Internal Persons	*Whistleblowers defined as internal in this procedure*
Protected Persons	*The persons set out in **paragraph 1 of Appendix B** of this Procedure, who may benefit from the Safeguards.*
TFEU	*Treaty on the Functioning of the European Union*
Safeguards	*The set of Protection and Support Measures provided in favour of Protected Persons under applicable law*

231 Violations	*Acts or omissions which harm the public interest or the integrity of the Company and which consist of* *a) unlawful conduct relevant under Legislative Decree 231/2001 (i.e. the committing of predicate offences or the reasonable danger of committing predicate offences, provided for by Legislative Decree 231/01 on the administrative liability of companies (so-called "231 offences")* *b) violations of the rules of conduct/procedures/protocols issued by the Company and/or any violation of the Organizational Model 231,* *o* *c) that frustrate the object or purpose of the regulations set out in Legislative Decree 231/2001, including any attempts to conceal such violations,* *which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly also other than the Company, for example a supplier of the same) with which the Whistleblower has a legal relationship, including any conduct aimed at concealing such violations;*
Violations of Sectorial Acts	*Behaviours, acts or omissions which harm the public interest or the integrity of the Company and which consist of offences falling within the scope of the Sectorial Acts identified in* ***Appendix A****, which have occurred or which are very likely (on the basis of concrete elements) to occur in the organisation (possibly even other than the Company, e.g. a supplier of the same or a contact person of an auditing firm of the same) with which the Whistleblower has a legal relationship, including any conduct aimed at concealing such violations, regardless of whether* *- the employment relationship with the Company has ended in the meantime (so-called former employee), or that* *- the facts were learnt during the selection process (e.g. candidate) or in other phases of pre-contractual negotiations with the Company, irrespective of whether, under national law, Whistleblowing Violations are administrative, criminal or purely civil violations (e.g. risk of damages).*
Violations of Internal Regulations	*Behaviours, acts or omissions which damage the integrity of the Company and which consist of Breaches of the specific Internal Regulations of the Companies indicated in Appendix A of this Procedure*

2.2. Subjective Scope of Application

2.2.1. The present procedure, subject to approval by the competent Board of Directors. applies to the company **PELLINI CAFFÈ S.P.A.** with registered office in Via I Maggio 8 - 37012 - BUSSOLENGO (VR), VAT No. 09048540158 (hereinafter also only the "Company").

2.2.2. In relation to each Company, this procedure applies:

- To the persons who make i) Internal and/or External Reports or ii) Public Disclosures or iii) Complaints to the Judicial Authorities, **in relation to Sectorial Violations**;
- To other Protected Persons;
- To other categories of Interested Parties whose data are processed in connection with Reports handled by the Company.

2.2.3. Whistleblowers may belong to the following categories:

ID	Subject Category	Subject Nature
A	Company **employees**, including casual workers, regardless of their position within the Company, the legal nature of their relationship and the area of activity or hierarchical level	Internal whistleblower
B	Paid and unpaid **volunteers and trainees** working for the Company	Internal whistleblower
C	Self-employed workers, including self-employment relationships that have a special discipline pursuant to Article 2222 of the Italian Civil Code (work contract) (including **freelancers and consultants** working for the Company, *such as intellectual professions for which registration in special registers or lists is required, such as psychologists, architects, surveyors, etc.*). as well as **Holders of a collaboration relationship** referred to in Article 409 of the Italian Code of Civil Procedure, who carry out their work activities at the Company, by which is meant ✓ those of private subordinate employment, even if not inherent to the exercise of a business activity *(e.g. domestic work, home work*) ✓ agency, commercial representation relationships; and ✓ other collaborative relationships resulting in the provision of continuous and coordinated work, mainly personal, even if not of a subordinate nature *e.g. lawyers, engineers, social workers, who provide their work for the Company by organising it autonomously (para-subordinate relationship)*	External whistleblower
D	**Employees and collaborators**, who work **for third parties Public or private sector entities that provide goods or services or carry out works in favour of the Company**	External whistleblower
E	**Freelance professionals and consultants** who work for the Company	External whistleblower
F	**Shareholders** (natural persons)	External whistleblower
G	**Members of the administrative and/or management** or representative **body** of the Company, including non-executive	Internal whistleblower

	members (e.g. directors without or with delegated powers), even when such functions are exercised on a de facto basis	
H	**Members of the** Company's **control or supervisory body** (e.g. Auditors, Auditors or Auditing Company, DPO - Data Protection Officer)	Statutory Auditor: Internal whistleblower Auditor or contact person of auditing company, DPO: External whistleblower

2.3. Objective scope

The Whistleblower is obliged to communicate well-substantiated Violation Information based on precise (adequately detailed) and concordant facts, and not facts of generic, confusing and/or blatantly defamatory or slanderous content.

Reports may also be anonymous, i.e. they may not mention the identity of the reporter or allow the identity of the reporter to be reconstructed or found. They will be examined, provided they comply with the above requirements.

They will not be taken into consideration, and will result in exclusion from the Safeguards provided for by this Procedure:
a) **disputes, claims or requests linked to a personal interest of the Whistleblower** or of the person who has filed a complaint with the judicial authorities or has made a Public Disclosure **that relate exclusively to his/her individual employment relationships, or inherent to his/her employment relationships with hierarchically superior figures**
(e.g. reports concerning labour disputes, discrimination between colleagues, interpersonal conflicts or involving only the Whistleblower and another worker or the persons to whom the Report or Public Disclosure or complaint relates), and

b) **information contained in Reports that have already been rejected** by any Internal Reporting Channel or by the ANAC, and

c) **information already fully available to the public** or which constitutes mere **hearsay**, and

(d) information that relates to **acts or omissions not expressly covered** by this Procedure.

This is without prejudice to:

- the application of the provisions on a) the exercise of the right of workers to consult their representatives or trade unions, b) protection against unlawful conduct or acts carried out as a result of such consultations, c) the autonomy of the social partners and their right to enter into collective agreements, and d) the repression of anti-union conduct (e.g., by way of example but not limited to, Article 28 of Law 300/1970, as amended. - Workers' Statute), and
- the application of the provisions of criminal procedure (**if the Whistleblower has information about a criminal offence, he may always lodge a complaint with the** competent **criminal authority**).

All Reports sent through the Internal Reporting Channel must be made in good faith. This means that, at the time of submission, the Whistleblower must have reasonable and sufficient grounds to believe that the information provided is true, accurate and has not been obtained through potential violations (e.g. criminal offences).
In this sense**, malicious or grossly negligent reporting may give rise to the relevant sanctions by the Company**, without prejudice to the civil and criminal liabilities that may arise therefrom.

3. REGULATION OF ACTIVITIES

3.1. Generalities

Whistleblowing is:

a) **obligatory**, on the part of **Internal Parties** (NB. by virtue of the **general duties of loyalty, diligence and good faith** connected to the legal relationship with the Company, to be understood as expressly reaffirmed herein)

b) **obligatory**, on the part of the **External Parties who are contractually obliged** towards the Company to report;

c) **optional**, on the part of **Persons External to** the Company who are not contractually obliged towards the Company to report.

3.2. Object of the Report

In order to facilitate and allow the due verification and preliminary investigation activities by the Company, also in order to ascertain whether the Report is well-founded, the Report must contain at least the **following information**

- **identity** of the Whistleblower (name, surname, number of a valid identity document), unless he/she intends to remain anonymous;
- **relationship with the Company** (candidate, employee/collaborator, director, shareholder, supplier/consultant, partner, etc.) and, if applicable, position/qualification/company position of the Whistleblower;
- as clear, detailed and complete **a description** as possible **of the facts** that are the subject of the Report;
- **the circumstances of time and place** in which the facts were committed, if known;
- **identity** of the **person to whom the Violation is attributed** (so-called "Person Involved") or useful elements for identifying him/her (area/position/qualification/assignment), if known;
- indication of any **other persons who can report** on the facts that are the subject of the Report;
- indication of any **documents** that may confirm the truthfulness of the facts that are the subject of the Report;
- description of the **reasons** connected with the work activity carried out that made the reported facts known;
- any other **information** that may provide useful **evidence of the existence of the facts** reported;

- if applicable, a **means of communication with** the Whistleblower other than the Portal/Software (e-mail address, telephone or other) so that the Case Manager can communicate with the Whistleblower.

If, after assessing the content of the Report, it turns out to lack the minimum mandatory requirements for its proper assessment, the Case Manager will proceed to request the corresponding information and/or documentation from the Whistleblower through the communication methods indicated by the latter, proceeding as per Chapter 3.5.2 in the event that the necessary information is not available for the opening of the investigation phase.

3.3. Types of Reporting

3.3.1. Internal Reporting Channels

The Internal Reporting Channels must be activated **after compulsorily informing the trade union representatives (RSA/RSU).** Any comments made by the trade union have the value of a non-binding opinion.

Internal Reporting Channels are divided into Internal and External, depending on whether they are managed directly by the Company or, respectively, by third parties authorised by it.

3.3.1.1. Communication of the Report

The following Internal Reporting Channels may be used by the Whistleblower:

✓ INFORMATIONAL:

a) **Portal/Software**, accessible at **https://pellinicaffewb.integrityline.com**.

✓ *ORAL (at the request of the Whistleblower or if deemed useful and possible by the Case Managers in compliance with the Whistleblower's wish to remain anonymous*): **Personal/direct meeting** with one or more Case Managers, also through a possible remote session by videoconference.

The Case Managers ensure in this case, **subject to the consent** of the Reporting Subject, that

- the meeting takes place **within a reasonable time** from the date of the said request, and
- a complete and accurate **record** of that meeting is **kept on a durable medium** that **allows access** to the ViolationInformation.

The Case Manager is obliged to **document** the meeting by **keeping detailed minutes** of it.
The Case Manager has the right and obligation to **verify, rectify and approve the minutes** by his/her signature.

NB1: In the event that the Company decides at any time to activate any oral reporting channels other than and/or in addition to the direct personal meeting (e.g. voice messaging, telephone lines, etc.), it is understood that the oral channels will be reciprocal and not cumulative with respect to the direct meeting. Only in such a case, the Case Manager will have discretion as to which oral channel to use towards the Reporting Officer.

NB2: The use of e-mail (ordinary or certified) must be considered in itself inadequate to guarantee the confidentiality of the Whistleblower's identity, given the peculiar system of logs connected to it.

3.3.2. Communicating the Alert to erroneous subjects

Report to erroneous person

If a person other than the competent Case Manager (e.g. a secretary) receives a Report, he/she must forward it to the competent Case Managers, within 7 (seven) days from its receipt, complete with any supporting documentation received, not retaining any copy and refraining from taking any independent initiative for analysis and/or investigation, and guaranteeing at all times the confidentiality of the same.

Failure or delay on the part of the first recipients of the Report to communicate it to the competent Managers constitutes a serious breach of this Procedure, as such punishable by disciplinary sanctions.

Reporting to more than one internal person

In the event that the Report is sent, at the same time, to several persons, all internal to the Company, the Report must be considered as a Report sent to a non-competent person. Therefore, the person(s) in charge of receiving such Reports should forward them, within 7 days from their receipt, to the competent internal subject, simultaneously notifying the Whistleblower.

Reports also sent to several external subjects

If, on the other hand, the Report is sent not only to the internal person in charge of handling it, but also to more than one person outside the institution, the Whistleblower should be asked for clarification of the circumstances that led to the Report, in order to ascertain whether the Whistleblower intended to proceed directly to public disclosure.

In such a case, given that there are no conditions for considering that the Internal Reporting was carried out correctly (since the Whistleblower chose not to address only and exclusively the internal person competent to handle the report), it is necessary to understand whether the Report can be qualified as a Public Disclosure and to ascertain whether or not one of the conditions laid down in Article 15 of the Whistleblowing Decree itself is met.

3.3.3. External Reporting and Public Disclosure

3.3.3.1. External Reporting

The Whistleblower may make an External Report (i.e. to ANAC) only if, at the time of its submission, one of the following **conditions is met**:

a) there is no mandatory activation of any Internal Reporting Channel within its working context, or

b) the Internal Reporting Channel, even if theoretically envisaged as mandatory by the Company, **is not in** fact **active or, even if activated, does not comply with** the regulatory indications;

c) the Internal Reporting already carried out by the Whistleblower **has not been followed up**;

d) the Whistleblower has **well-founded reasons to believe** that, if he/she were to make an Internal Report, it would not be effectively followed up, or that the Report might give rise to the **risk of retaliation**; "well-founded reasons" should be understood as the presence of concrete factual elements, and not merely and generically feared, supporting the expectation of suffering Retaliation;

e) the Whistleblower has well-founded reasons to believe that the Violation may constitute an **imminent or obvious danger to the public interest**.

The External Report to the ANAC is made

- **in writing** through the Reporting Channel activated by ANAC
  (for more information on the contacts and instructions on the use of the External Reporting Channel, on the confidentiality regime applicable to External Reports, on the process for handling External Reports and any Retaliation, please consult the ANAC Guidelines available on the website https://www.anticorruzione.it/-/whistleblowing), or
- **orally** through (i) **telephone lines** or (ii) **voice messaging systems** or, (iii) at the request of the Whistleblower, through a **face-to-face meeting** set within a reasonable time.

3.3.3.2. Public disclosure

The Whistleblower **may** make a Public Disclosure of the Breach, benefiting from the Protections afforded by law, only if the following conditions are met (the '**Public Disclosure Conditions**')

- **the Report** (internal and external, or directly external) **has first been made**, but:
  - ✓ **no acknowledgement of receipt has been sent to the Whistleblower**, within the period of **7 working days** from the date of the Reporting, or
  - ✓ **appropriate action has not been taken** in response to the Report **within the period of 3 months** from the date of the acknowledgement of receipt of the Report;

or when

- the Whistleblower has **reasonable grounds** to believe that:
  - ✓ the Breach may constitute an **imminent or obvious danger to the public interest**, such as where there is an emergency situation or a risk of irreversible harm (including danger to the physical integrity of a person); or
  - ✓ in the case of an External Report, there is **a risk of retaliation or there is little likelihood of an effective Follow-up** due to the circumstances of the case, such as where evidence may be concealed or destroyed or there is reason to believe that the Authority receiving the Report may be colluding with the author of the Violation or involved in the Breach.

3.4. Case Managers

3.4.1. Generalities

The Board of Directors is the body responsible for the appointment, as well as the removal or dismissal, of the Case Manager, who, in turn, is responsible for the management and processing of Repors that enter the Internal Reporting Channel.

The Case Manager may be a natural person or a collegiate body that may delegate to one or more of its members (natural person) the powers to manage and process individual Reports.

The Case Manager is the designated EXTERNAL CASE MANAGER (currently: Avv. Luca De Muri), without prejudice to the powers of further Case Managers in accordance with the provisions of this Procedure.

In the remainder of this Procedure, the reference to the "**Case Managers**" or to the " **Reporting Committee**" is to be understood as being limited to the sole Case Manager, in the event that the latter remains such according to the rules laid down herein.

In the event that the initially designated sole Case Manager operates the eventual Instructional Delegation provided for by Article 4.6.2.1.d, or in the event of the designation of more than one Case Manager, they act collectively as the "**Reporting Committee**" and any reference to the Case Manager must be understood as referring to the "**Reporting Committee**".

The Case Manager acts in a **functional position that is autonomous and independent from the rest of the corporate functions and from any hierarchical or functional subordination that may exist**.

Without prejudice to the generality of the foregoing, it is therefore strictly forbidden for anyone to exert pressure, send instructions, attempt to condition or hinder in any form whatsoever, and in general try to compromise the autonomy, impartiality and independence of the Case Manager.

The Case Manager must be **specifically trained** for such management.
In particular, it is essential that the choice falls on a person who has all the knowledge and skills for an effective management of the Report.
Preferably, this should be a person with a good knowledge of legal, ethical and integrity issues and who has been adequately trained in the processing of personal data and whistleblowing.

The Whistleblower Manager must be guaranteed adequate knowledge of the Company's functional organisation chart.

If the Case Manager is temporarily absent or unable to perform his or her duties (due to holidays, illness, accident), he or she must inform the other members of the Whistleblowing Committee, or in the case of a one-man Case Manager, the HR Manager. In the case of holidays, moreover, if the Reporting Portal does not allow the Case Manager to be notified automatically of receipt of the Report within the strict deadline of 7 days from the date of the Report, and the Case Manager cannot be temporarily replaced by other Case Managers, he/she shall give formal notice to potential Case Managers on the home page of the Portal/software, indicating the duration of the holiday.

3.4.2. <u>Budget</u>

The body of the Company competent to appoint the Case Managers provides for the allocation to them of an **annual budget**, to be used for the performance of the tasks assigned. The amount of the budget is deemed to be automatically renewed from year to year, unless otherwise quantified by the competent body.

3.4.3. <u>Tasks</u>

The Case Manager **is responsible** for:

a) **receiving and taking charge of Reports**;

b) **carrying out the Screening** (content analysis and admissibility assessment) of the Reports;

c) **providing the Reporting Officer with the Notice of Receipt of the Report within 7 days from the date of the** Report, unless this would compromise the confidentiality of the Report or the identity of the Reporting Officer, or the Reporting Officer has waived the right

to make use of the communications relating to the investigation; maintaining contact with the Reporting Officer for subsequent communications;

d) **diligently follow up** the Report;

e) determine, in coordination with area company contact persons if necessary, the advisability or necessity of taking immediate action to **prevent** (stop or mitigate) **further damage**;

f) conduct or arrange for the **proper investigation** of the reported facts, in accordance with the rules and principles set out in this Procedure;

g) **decide on the outcome (merits) of the Reports**, on the basis of the results of the investigation within the time limit prescribed by law; extend the termination period for reasons of complexity;

h) **propose the appropriate measures for the resolution of the Breach, as well as, where appropriate, the disciplinary measures** to be taken, with the possibility of delegating this power to another competent body;

i) **communicate the outcome of the Report to the relevant persons** within the deadline laid down in this Procedure (unless, in the case of the Whistleblower, he/she has waived the right to avail him/herself of the communications relating to the investigation);

j) in general, **maintain contact with the Whistleblower** throughout the follow-up to the Report;

k) take care of the proper **filing and storage** of Reports;

l) liaise with the Privacy Function and other corporate functions, where necessary or requested, to **meet the compliance requirements of the processing of personal data** covered by Reports ;

m) make available **clear information on the Reporting Channels**, **procedures** and **prerequisites** for making Internal and External Reports, by means of the specific methods provided for in this Procedure and/or further identifiable; for this specific purpose, the HR Function is henceforth delegated to act also on behalf of the Case Manager;

n) **manage the Internal Reporting Channels, guaranteeing the necessary protection requirements** of the system for managing and storing data on Reports, also by limiting access to them, also **by making use of the competences and activities of the** corporate **IT and/or Privacy Functions**, without prejudice to the responsibilities and powers of the latter deriving from the corporate delegation system;

o) **resolve any doubts and requests for clarification** concerning the provisions of this Procedure;

p) keep the Reporting Register up-to-date;

q) ensure the adoption of appropriate measures to **prevent and avoid possible retaliation** against the Whistleblower and other Protected Persons. In order to perform the above-mentioned tasks, and where it deems it necessary, the Case Manager may be assisted by an external consultant or even delegate to the latter some of the above-mentioned functions. In this respect, the Case Manager must obtain a confidentiality agreement from the external collaborators involved in the management and resolution of the report.

Likewise, he should obtain the same from internal collaborators, when he considers it useful or necessary.

3.5. Examination of Reports

3.5.1. Screening

Following receipt of the Report, the Case Manager **takes it in hand** and carries out a **preliminary assessment**, aimed at ascertaining that the Report:

a) **concerns facts constituting a type of Violation** included among those listed in ***Appendix A***,

b) originates from **Whistleblowers belonging to one of the categories set out** in this Procedure,

c) contains the **minimum mandatory information** required by the Whistleblowing Decree,

d) does not contain **Information** that already upon summary examination appears to be **manifestly false or unreliable**,

e) does not contain **Information** that already on summary examination appears **to be the result of an offence committed by the Whistleblower**,

f) does not appear, even on summary examination, to have been made by the Whistleblower in **bad faith**, i.e. with the intention of harming the Company or third parties connected to it,

g) **does not contain any significant new information** on Breaches **with respect to a previous Report** for which the relevant decision-making procedure has been completed,

and therefore whether the Report is deemed to be **admissible** (the "**Screening**").

The results of the Screening must be documented.

The Case Manager will have to issue a decision on whether or not the Report is admissible.

If the Case Manager assesses that the Report **is not procedural:**

- **must refrain from pursuing an Alert further,**
- issues a decision to **dismiss** the Report on grounds of unfeasibility under the Whistleblowing Decree, **giving reasoned written notice:**
- **to the Whistleblower**, unless the Whistleblower has waived the right to receive communications;
- **to the Board of Auditors**.

In the event that the Case Manager during the Screening detects the possible absence of the conditions required by the Whistleblowing Decree to guarantee the Whistleblower the protection and support regime to which he/she is normally entitled, he/she will give written notice thereof, not only to the Whistleblower, but also to the Involved Subject and to the other competent internal subjects, as better indicated in Chapter 4.7.1 below.

Alternatively, **if the documentation is missing or defective in any way**, the Case Manager may not file the Report but, if he considers it necessary, request information from the Whistleblower.

Similarly, the Case Manager may, with the consent of the Whistleblower, transfer the Report to a corporate function which may be competent to treat the Report as an ordinary Report according to

corporate policies (e.g. a Report from a customer, a Report on a conflict of interest of a member of the Board of Directors).

Where the Report **is manifestly unfounded and there are, in the opinion of the Case Manager, reasonable grounds for believing that it was obtained through the commission of a criminal offence**, in addition to inadmissibility, the Company assesses whether to send the Public Prosecutor's Office a detailed report of the facts alleged to be an offence (such a report is an obligation if the offence is prosecutable ex officio).

The Whistleblower must immediately transmit the information to the CEO (provided that there is no conflict of interest, in which case the transmission is made directly to the different competent body on the basis of the company "s system of delegated powers) for any decision on whether or not to immediately transmit it

- to the Public Prosecutor's Office **when the facts may be suspected of constituting a criminal offence**, or
- to the European Public Prosecutor's Office **when the facts concern the financial interests of the European Union**.

Finally, the Case Manager must forward the communication without delay to the authority, body or third party body that may be considered competent *ratione materiae* to handle the Report.

3.5.2. Conflict of interest

If the Case Manager considers the existence of a **conflict of interest** with respect to the Report received (*e.g. if the subject matter of the Report concerns Violations attributable, even indirectly, to one of the members of the Case Manager himself/herself, or to persons who are relatives or linked by a stable affective bond, etc.*), he/she must:

- inform the Reporting Officer of the nature of the conflict of interest;
- refrain from dealing with the Report, and shall therefore not have access to the information deriving from the actions carried out in the management of the Report (unless he/she is an Involved Person); and
- immediately devolve the handling of the Report to another Case Manager(s) not in conflict of interest, within the Reporting Committee, or, in the absence of such Case Manager(s) not in conflict of interest, to the additional person to be designated and appointed without delay by the competent Board of Directors. In the event of a conflict of interest of the competent Board of Directors, the designation of the Whistleblower Manager will be made by the HR Manager, after hearing the Chairman of the Board of Auditors.

  In the event that no Case Manager with no conflict of interest can be identified, the Whistleblower will be entitled to make an External Report (i.e., direct to the ANAC).

3.5.3. Acknowledgement of receipt and acknowledgement to the Whistleblower

3.5.3.1 Acknowledgement of receipt

Within the strict deadline of 7 calendar days from the reception of the Report, the Case Manager communicates to the Reporting Subject an acknowledgement of receipt of the Report, by an appropriate means to ensure the confidentiality of the message.

The acknowledgement of receipt may be omitted if:

a) the Whistleblower has expressly objected, or
b) there is reason to believe that confirmation of receipt of a written Report would compromise the confidentiality of the identity of the Whistleblower, or
c) the Whistleblower has not provided an address to which the acknowledgement can be sent and cannot be reached anonymously via the Portal/Software.

In case c) the report received must be declared inadmissible by the Case Manager.

3.5.3.2 Acknowledgement

The subsequent acknowledgement to the Reporting Subject on the **outcome of the Report** must be provided within a period of **3 months**, starting:

- **from the date of the acknowledgement of receipt of** the Report, or,
- if the initial acknowledgement of receipt has not been sent to the Reporting Subject (e.g. because the Reporting Subject has remained anonymous despite being guaranteed the possibility of receiving the acknowledgement through the Portal/Software, or because he/she has expressly waived the right to receive the said notice), **from the expiry of 7** calendar **days** from the date of receipt of the Report.

NB: In cases of **particular complexity** requiring an extension of the investigation period, this may be extended, by decision of the Case Manager, up to a maximum of a further three (3) months, in which case the **Reporting Officer must be informed of** the extension within the first 3 months.

NB: The aforementioned period of three months is not, by law, binding on the Whistleblower. Any exceptions, however, must be reasonably justified by the Case Manager.

3.6. <u>Investigation</u>

3.6.1. <u>Generalities .</u>

Every Report assessed as admissible must be investigated to verify its merits.

The results of the Preliminary Screening are used by the Case Manager to determine the scope of the investigation (see e.g. Section 8.3 ISO 37008) and to define an investigation plan (see e.g. Section 8.4 ISO 37008).

If the Case Manager assesses that the Report **is admissible** (in particular, that **it falls within the scope of this Procedure,** as it relates to Breaches of Sectorial Acts), it is up to him/her to

a. assess whether the Report **falls within the competence *ratione materiae* of other bodies or functions on the basis of mandatory provisions of the law** (e.g. Board of Statutory Auditors or Auditing Firm/Auditor in administrative, fiscal, accounting and balance sheet matters subject by law to their control, RSPP, DPO, ODV231) and therefore, **on the basis of a decision** to be taken in agreement with such bodies and functions;

b. transfer the management of the Follow-up to such bodies or functions, or share with such bodies or functions the management of the Follow-up, with the consequent assumption by them of the status - concurrent or exclusive, as the case may be - of Case Manager and of the consequent duties and responsibilities, subject to acceptance of this Procedure;

c. (in the case of their competence *ratione materiae* under this Procedure ~~or~~ under the corporate system of delegation of powers in force, e.g. privacy delegate, etc.) coordinate the management of the Follow-up with such bodies

or functions, subject to acceptance of this Procedure, **with the Case Manager retaining the original duties and responsibilities**.

In particular, such forwarding must take place at the first useful meeting or, if the urgency is recognised, without delay.

d. assess that the further handling of the Report **does not fall within the competence - under mandatory provisions of law or the delegation system** - **of any other corporate body or function**, and consequently:

- ✓ **proceed with further** investigative **tasks** (investigation, etc.), or
- ✓ **identify, by agreement with the competent Board of Directors, a different person competent** in relation to the Report**,** transferring **the management of the Follow-up** , including the final decision on the merits of the Report, subject to acceptance of this Procedure, with simultaneous notification of the transfer to the Whistleblower. **The different person identified must meet the requirements set out in this Procedure**,
- ✓ Assess the appropriateness of **taking immediate measures to prevent further harm** and, if necessary, implement them.

3.6.2. <u>Investigation</u>

3.6.2.1 General

Once the Report has been admitted for processing, the Reporting Committee proceeds with the investigation of the facts that are the subject of the Report, carrying out all the acts, procedures and checks necessary and aimed at verifying the truthfulness of the facts that are the subject of the Report, in compliance with the principles and rules set out in this Procedure.

To this end, he/she shall, by way of example but not limited to:

a) verifies whether the Company has adopted adequate Procedures to protect against the risk of the Violationthat is the subject of the Report;

b) if he deems it necessary or appropriate, requests and receives further information, clarifications, and/or the production of deeds and documents from the Reporting Officer - if known - or from other persons (e.g. department heads or any other internal or external person) in possession of useful information for the preliminary investigation, in particular, reasonably concerning the processes at risk of Breach;

c) has direct and timely access to the Company's Board of Directors and control bodies (e.g. Board of Statutory Auditors, auditing firm or auditors, Data Protection Officer if designated, etc.);

d) where deemed necessary, may **delegate in writing to one or more** (internal/external) **persons** with adequate skills the performance of the above-mentioned **investigative tasks sub a-b-c)** - within the limits of the powers vested in the delegate in accordance with the corporate delegation system in force (the "**Investigative Delegation**") and subject to the delegate's commitment to comply with this Procedure.
In this case, the delegating Case Manager **retains** the power to:

- Evaluate the results of the preliminary investigation and **make the final decision on the merits of the Report**, and

- Make an **assessment**, as far as possible on the basis of the results of the preliminary investigation, as to the **possible existence of wilful misconduct or gross negligence on the part of the Whistleblower and/or of any Involved Persons** (as a **non-binding opinion** addressed to the function or body competent to manage the disciplinary or sanctioning proceedings against the Whistleblower or the Involved Person).

It is understood that the person to whom the Case Manager intends to delegate the aforesaid activities shall report to the Case Manager any situations in advance of his workload that may cause the risk of a non-diligent Follow-up of the Reporting by the delegate *in pectore.*

3.6.2.2 Professional defence

The Whistleblower shall assess the advisability of consulting with the competent functions of the Company in order to evaluate whether it would be useful to entrust a mandate to a lawyer to conduct the investigation, in the light of the legal principle of the so-called legal privilege[1] which protects the confidentiality of communications between the assisted party and his lawyer, preventing them from being compulsorily disclosed to third parties (e.g. the Public Prosecutor) or used against the assisted party in judicial or investigative proceedings.

3.6.3. Obligations to cooperate

The personnel and any other internal and/or external contact person of the Company are required to **cooperate loyally and with the utmost diligence** in the investigative activities carried out by the Case Manager.

The internal personnel supporting the investigative activities must have signed the prior appointment as authorised persons pursuant to Article 29 of the GDPR.

3.6.4. Collection, storage, analysis and review of electronic data

The collection, storage, analysis and review of data in electronic format by the Case Manager must comply with the rules of law on computer checks on employees and electronic evidence, under penalty of, inter alia, unusability in labour and civil law proceedings of electronic evidence.

3.6.5. Interviews

It is recommended that the Case Manager conduct interviews in accordance with the relevant good practices (e.g. Section 8.9 ISO 37008).

3.6.6. Rights of the Involved Person

During the course of the investigation, the Person Concerned must be informed of the Report with a brief account of the acts or omissions attributed to him/her and has the right to be heard at any time.
This communication must be made at a time and in a manner deemed appropriate by the Case Manager, according to prudent discretion, to ensure the proper conduct of the investigation.

[1] The protection is enshrined
- by Art. 103 of the Code of Criminal Procedure (secrecy of lawyer-client communications)
- by Art. 200 of the Code of Criminal Procedure (secrecy of lawyer-client communications)
- by professional secrecy (arts. 622 and 623 of the criminal code) and by the lawyer's deontological duty of confidentiality
- from the right of defence and cross-examination.

This information may be withheld during the hearing of the Involved Person if it is considered that its prior disclosure may facilitate the concealment, destruction or alteration of evidence.

Without prejudice to the right to lodge written complaints, the investigation shall include, where possible, an interview with the Person Involved, in which, always in full respect of the presumption of innocence, he/she is invited to explain his/her version of the facts and to provide the evidence he/she deems appropriate and relevant.

In order to guarantee the right of defence of the Involved Person, he/she shall have access to the file (without revealing information that could identify him/her) and may be heard at any time. He/she must also be informed of the possibility of being assisted by a lawyer.

In addition, the investigator must listen to all the persons concerned and any witnesses, and must carry out all the procedures he or she deems necessary (examining documentation, obtaining information from external sources, etc.). The intervention of the witnesses and persons concerned shall be strictly confidential.

The investigator may also obtain any information and documentation he deems appropriate from any area or department of the organisation to corroborate the investigation.

Of all the acts of investigation and, in particular, of the explanations or declarations provided by the persons involved in the investigation of the Report, a written record shall be drawn up (provided that their prior consent has been obtained), which shall be duly signed by the Persons Involved in order to certify its content and the conformity of their declarations.
In the event that the presence of the Involved Person during the investigation period may jeopardise the conduct of the investigation or the strict observance of the guiding principles of the procedure set out in this Procedure, the Involved Person may be granted, on the proposal of the investigator and by the competent corporate function, paid leave from work, without loss of pay, in order to ensure that the necessary investigative activities can be carried out without interference that could be detrimental to the person under investigation. Paid leave will be granted for the time necessary to carry out the investigative activities, but may in no case extend beyond the duration of the investigative process.

If the Case Manager deems it appropriate, the presence of external legal advisers is allowed at hearings and/or statements of the parties concerned, witnesses, etc.

3.6.7. Information flows to senior bodies

In order to guarantee the Whistleblower's autonomy, the Board of Directors is prohibited from deciding whether and how to follow up the Whistleblowing, requesting information, supervising the investigation carried out and/or taking decisions on the merits of the Whistleblowing, and the Case manager.

3.6.8. Finalisation of the investigation

An investigation cannot be considered substantially complete if it does not reach the following results

- the Case Manager is prepared to make findings supported by evidence, and these findings are sufficient for the Board of Directors to make a decision on the incident of non-compliance;
- the Case Manager is able to fully account for its work product;
- the result of the investigation provides a sufficient basis for initiating the necessary corrective action.

3.6.9. Reporting Decision and Investigation Report

Upon completion of all investigative actions, the Case Manager prepares a written report containing at least the following content (the '**Investigation Report**'), which is intended to be limited to the defined scope of the investigation:

- A statement of the relevant facts (descriptive information about the Report) together with the Report identification code and the date of registration.
- The actions taken to verify the plausibility of the facts and the limitations and constraints encountered during the investigation.
- The conclusions reached in the investigation and the evaluation of the proceedings and supporting evidence.
- The actions taken (if any).

3.6.10. Corrective measures

The Investigation Report **may also contain any proposals for potential corrective measures or improvements** to be implemented on the basis of the results of the investigation to minimise the impact of the Breaches (so that the root causes of the Breaches are appropriately, sufficiently and effectively addressed) and to **improve the internal controls of** the Company's **compliance programme** and/or proposed disciplinary measures.

The Company function(s) assigned to the policies or procedures corresponding to the Violation must design a **remediation plan based on the Investigation Report**.

If requested, the Case Manager should report to the Company's compliance function to assist in the development of an interim remediation plan. The plan should clearly state the compliance gaps or vulnerabilities and the objective(s) the measures are intended to achieve.

3.7. Actions following the Report

After issuing the Report of Investigation, the Case Manager makes one of the following decisions.

3.7.1. Unfoundedness of the Report with Malice or Gross Negligence

In this case, the Case Manager rejects the Report and proceeds to dismiss it.

If the Case Manager discovers elements that, in its prudent judgement, point to bad faith or gross negligence on the part of the Whistleblower, it shall communicate this without delay in writing

a) to the Whistleblower, expressly warning him/her of the consequences of the law (absence of Safeguards);
b) to the Person Involved; and
c) to the Head of the functional area to which the Whistleblower belongs, as well as to the HR Department of the Employer (e.g. for the assessment of the application of possible sanctions against the Whistleblower).

3.7.2. Report confirmed by the investigation

If, at the outcome of the investigation, the Case Manager finds that the facts reported are **well-founded in substance**, he issues a documented decision to accept the Report.

The communication may contain, where appropriate, the relevant proposals for action and/or proposal of disciplinary measures against any Involved Person.

The decision must be **communicated**, **without delay:**

a) to the Whistleblower, unless the Whistleblower has waived it or the communication is anonymous;

   in the case of an external Whistleblower, the communication must be sent:

   - ✓ to the pro-tempore legal representative of the third organisation to which the Whistleblower himself/herself belongs (or, if the Case Manager consider that the Whistleblower is in a position of conflict of interest with respect to the Violation decided, to the Head of the different functional area of the third organisation that appears competent to receive such communication), and
   - ✓ to the Head of the internal functional area that has contractual relations with that third party organisation;

b) to the Whistleblower;

c) to the Head of the functional area affected by the Breach, for the assessment and implementation of the appropriate remedial actions;

d) to the Delegated Function, for the assessment and implementation of possible consequent disciplinary sanctions;

e) to the Board of Directors, which approved this Procedure,

f) to the members of the Board of Statutory Auditors.

The aforementioned communication may be delayed in the event that, in the opinion of the Case Managers, it **may hinder** further **investigations or judicial proceedings** (e.g. administrative, criminal) for the protection of the rights of the Company and/or of third parties, after the preliminary investigation has been carried out.

3.7.3. <u>New Violations</u>

If, as a result of the investigation**, other facts are discovered that may constitute new irregularities** (whether or not falling within the scope of the Whistleblowing Decree) allegedly committed by the same Whistleblowing Person or by other persons, the Case Manager **shall, ex officio, open a new file** (in which case the related Follow-up will take place, in the first case, outside this Procedure in accordance with the applicable corporate procedures on internal investigations), and in the second case, in accordance with this Procedure) or, if it is related to what is being investigated in the current Whistleblowing file, **to the extension of the investigation file** itself, if it deems it more discretionary (in which case the related Follow-up will take place in accordance with this Procedure only if it appears necessary for a unitary treatment of the matter).

3.7.4. <u>Administrative, civil or criminal proceedings</u>

The Case Manager, if he considers that, although there is no initial indication that the facts may constitute a criminal offence, or that there may be grounds for initiating administrative or civil proceedings, this indication results from the course of the investigation,

a) if already competent on the basis of the company's system of delegated powers, independently initiates such action against any Involved Person and/or further responsible third party, otherwise
b) informs without delay the internal person competent under the company delegation system to authorise or initiate such an action; that person then assesses whether to initiate the action;
c) in the event that the latter person has a conflict of interest in relation to the report, the Case Manager will consult with the HR Function to identify the most appropriate function or person to receive and implement the request to initiate the aforementioned administrative, civil or criminal proceedings, who is not himself in a conflict of interest.

The Company will consider whether it should make a self-report to the Authorities, for example to reduce liability or to exonerate itself or to protect any of its own rights that may have been violated; in order to assess the legal consequences, it may consider seeking professional legal advice, in line with point 4.6.2.2 of this procedure.

The Whistleblower must immediately transmit the information to the Board of Directors (provided that there is no conflict of interest, in which case the transmission is made directly to the different competent body on the basis of the company's delegation system) for any decision on the latter's immediate transmission:

- to the Public Prosecutor's Office **when the facts may be suspected of constituting a criminal offence**, or
- to the European Public Prosecutor's Office **when the facts concern the financial interests of the European Union**.

3.7.5. Report confirmed by verifications carried out, but indeterminate in terms of damage suffered or insufficient evidence gathered

In such cases (*examples: reports in the media; cyber-fraud, cartels in public tenders, conflicts of interest and other circumstances or conduct not easily detectable by internal controls, etc.*), additional investigation activities should be assessed, with an indication of the professional expertise needed (e.g. specific legal or technical expertise on the reported facts or underlying processes).

On the basis of the results of these further investigations, if the reported facts are confirmed, the actions set out in section 4.7.2 may be taken.
Otherwise, further action should be taken for legal protection or reporting to the competent authorities for any necessary investigations.

3.7.6. Report of facts that are plausible but cannot be verified

In these cases too, the actions referred to in 4.7.2 above may be taken.

3.7.7. Referral

The Case Manager may decide to refer the communication back to the authority, body or third party body considered competent to deal with it (e.g. FIU).

Whatever the decision, it must be communicated to the Reporting Officer without delay, unless the Reporting Officer has waived it or the communication is anonymous , and to all other interested parties.

3.7.8. Communication

The Whistleblower Manager works with the relevant corporate functions (e.g. management, compliance functions, human resources, public relations, etc.) to define who is competent to communicate with the various relevant stakeholders, and to effectively plan the manner and content of such communications.
The Case Manager plans communication with governmental authorities on the specific issues under investigation, if applicable.
Before communicating with them, corporate legal counsel (internal or external) should be consulted and any guidelines in place to ensure that the organisation's interests and rights are fully protected.

4. CONSERVATION

The Company will keep a record of all Reports received.
The Reporting Register is not public, therefore the records and data it contains will be kept confidential.

Records will not be kept longer than necessary and, in any case, for as long as necessary to comply with any applicable legal requirements at any given time.

Reports of irregularities or other cases that do not qualify as Violations included in this Procedure must be deleted, unless an obligation to further retain them arises from other Procedures in force at the Company, in which case they will be processed within the limits provided for by the same.

Once the investigation of the Report has been concluded and the appropriate actions have been taken, as the case may be, the data of the Report that has been followed up will be duly blocked in order to comply with the legal obligations that may be applicable in each case.

In no case may the data (report, related documentation) be kept for a period longer than **5 years from the date of the documentation of the final outcome of** the reporting procedure .

If it is decided not to follow up the Report submitted, the information may be kept anonymously.

The aforementioned term of 5 years is without prejudice to the different term provided, on the other hand, for the preservation of data, deeds and documents relating to the proceedings (e.g. disciplinary proceedings) initiated and to the initiatives (e.g. corrective measures, compensation, etc.) taken by the Company in total or partial dependence on the Report.

5. LEGAL PROTECTION

The Whistleblower and the other Protected Persons are guaranteed by the Company the Protections indicated in ***Appendix B***.

6. TRAINING

Training on whistleblowing, and its periodical updating, by the internal recipients of this Procedure (employees, collaborators) is mandatory for the Company, as it is an essential element to ensure a conscious and accurate handling of Reports.

Training of Whistleblowers

Specific training, to be periodically updated, should be addressed, first and foremost, to the persons in charge of or involved in the Whistleblowing management process, with the aim of providing them with the fundamental skills needed in the implementation and effective management of the whistleblowing processes, as well as with the knowledge of the topics covered by the reports (see ANAC Guidelines, point 5).

These persons should receive detailed training in the various facets related to the management of whistleblowing with a view to promoting their autonomous and ethical, as well as professional, operation. Therefore, staff should be trained on at least the following topics:

- the regulatory profiles of whistleblowing (both the European legislation and the provisions contained in Legislative Decree no. 24/2023), with particular attention also to the issue of personal data protection, in order to ensure maximum security and confidentiality of information
- the procedures and operating methods, with specific focus on the requirements to be fulfilled by Whistleblowers, including the management of conflicts of interest;
- the general principles of conduct (confidentiality and privacy, ethics and integrity, active listening, communication skills and cooperation).

As an alternative to the aforementioned training, the aforementioned specific skills and knowledge may be appropriately demonstrated by the Whistleblowers by means of CVs, certificates or similar documentation.

Training for all the entity's employees and non-employees

The training should involve all the employees and collaborators of the Company, so as to provide a clear and exhaustive picture of the new rules (clarifying, for instance, who the Whistleblower is, what can be reported and through which channels, what protections the law guarantees to the Whistleblower and which reports, on the other hand, do not fall within those protected, as well as specifying the involvement - also guaranteed by the protections - of the various persons working in the same work context as the Whistleblower).

7. DISTRIBUTION

The Whistleblowers shall make available to the addressees of this Procedure, clear information on the Whistleblowing Channels, on the prerequisites for making internal and external Whistleblowings and public Disclosures, using the following methods:

- Publication in a separate and easily identifiable section of the Company's website (the URL address of which shall be communicated by the Company to the main addressees, if reasonably possible),
- Making available:
  - ✓ by hand and/or
  - ✓ via e-mail or intranet or other document distribution application software.

8. DISCIPLINARY MEASURES AND SANCTIONS

This Procedure is a mandatory rule for all members of the Company. Its violation may give rise - in addition to the other civil and criminal liabilities provided for by the laws in force - to **disciplinary sanctions** by the Company, in accordance with the provisions of the labour laws and of the National Collective Labour Agreement and/or the Company Collective Labour Agreement, if any (to be therefore understood as expressly referred to herein).

When it is determined that the reported conduct constitutes a labour offence, the Company may take appropriate measures in accordance with the applicable disciplinary regime and, in particular, with the provisions of the Collective Agreement and labour legislation applicable to the Company.

Notwithstanding the adoption of disciplinary measures, if the facts may be suspected of constituting a criminal offence, the relevant information shall be immediately forwarded to the Public Prosecutor's

Office. If the facts concern the financial interests of the European Union, the matter is referred to the European Public Prosecutor's Office.

The following **sanctions** are also provided for:

Whoever:

- **obstructs or attempts to obstruct** one of the Whistleblowers or the other Protected Persons, in connection with any Reporting, or
- **adopts a retaliatory act**,
- **violates confidentiality provisions**,
- **fails to verify and analyse** the Reports received

commits an **administrative offence** and, unless the offence is punished with a more severe penalty by another provision of law, is punished by the ANAC - National Anti-Corruption Authority, with a **fine** ranging from EUR 10,000.00 to EUR 50,000.00.

The Company's governing body shall be jointly and severally liable for the penalty, without prejudice to the recourse action to be brought against all the persons responsible for the violation, in accordance with Article 6 of Law 689/1981.

9. OTHER

For all matters not expressly provided for by this Procedure, the Whistleblowing Decree and the ANAC Guidelines, and the further regulations referred to therein, shall apply.

10. AMENDMENTS

This Procedure may be amended or updated, at any time, in accordance with operational, legislative or regulatory requirements, and on the basis of lessons learnt during its actual application. Such amendments shall be promptly communicated to all persons involved and shall become binding from the moment of their communication or, if necessary, from the effective date established by the Company.

If the changes are substantial, they must be approved by the competent bodies of the Company.

APPENDIX A - SECTORAL VIOLATIONS

Sectoral Violations include:

a) **offences** (acts or omissions, even if only attempted or concealed) **that fall within the scope of the following sectoral acts of** the Union[2] , regardless of their classification under national law:

SECTOR
Privacy and data protection Examples • Omitted or inaccurate privacy notices to employees, applicants, visitors, customers, potential customers, suppliers, agents • Omitted or inaccurate privacy policy on the company website (so-called privacy policy) and/or cookie policy • Omitted or inaccurate privacy policy on whistleblowing • Absence or inaccurate privacy policy on video surveillance or automated monitoring and decision-making systems • Failure to obtain the prior specific consent of the data subject in cases provided for by law (in particular: ✓ use of the employee's image for advertising purposes ✓ use of the image of guests at company events for advertising purposes ✓ processing of personal data for direct marketing, profiling or market research purposes) • Failure to obtain a trade union agreement or administrative authorisation for video-surveillance or automated monitoring and decision-making systems • Failure or deficiency of register of processing operations • Failure or deficiency of appointment of external data controllers • Failure or deficiency of co-ownership agreements for processing in cases required by law • Failure to distribute written appointments and instructions to employees on the processing of personal data • Failure to comply with the privacy clauses of the corporate Whistleblowing Procedure • Failure to adopt organisational (e.g. physical, managerial) or technical (in particular, IT) protection measures suitable to avoid/reduce the risk of unauthorised access, loss or alteration, even accidental, of personal data processed by the company • Failure to draw up a DPIA (assessment of the impact of a given processing operation or set of processing operations on the rights of data subjects) in the mandatory cases provided for by law • Failure or delay in handling requests received by the company to exercise data subjects' rights
Protection of the environment

[2] See Annex to EU Directive 1937/2019

E.g. so-called 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 and disposal of hazardous waste.

E.g. violations of administrative requirements punished by administrative fines.

Product safety and conformity

E.g. violation of obligations aimed at ensuring that any product manufactured or marketed by the Company [...], under normal or reasonably foreseeable conditions of use, including duration and, where appropriate, commissioning, installation and maintenance, does not present any risk or only minimal risks, compatible with the use of the product and considered acceptable in compliance with a high level of protection of the health and safety of persons [...].

E.g. Infringement of the producer's obligation to provide the consumer with all information relevant to the assessment and prevention of risks arising from normal or reasonably foreseeable use of the product.

E.g. Infringement of the producer's obligation to take measures proportionate to the characteristics of the product supplied to enable the consumer to be informed of the risks.

NB: A product is defective when it does not offer the safety that may legitimately be expected taking into account all the circumstances, including:
(a) the manner in which the product was put into circulation, its presentation, its obvious characteristics, and the instructions and warnings provided;
(b) the use for which the product may reasonably be intended and the behaviour which may reasonably be expected in connection therewith; the time during which the product was put into circulation.
A product is defective if it does not offer the safety normally offered by the others in the same series.

N.B. The scope of risk relevant here goes beyond the mere presence of flaws and defects in the product (e.g. damage, failure to function, appearance not corresponding to the agreed description, etc.) that do not, however, result in a real **safety risk** for the purchaser/user even though they affect the suitability for use or the promised qualities.

Consumer protection

E.g. prohibition of unfair/aggressive commercial practices in the promotion of services/products.

Anti-money laundering and terrorist financing

The offence of money laundering exists when, apart from cases of complicity in the offence, a person replaces or transfers money, goods or other utilities originating from a crime, or carries out other transactions in connection with them, in such a way as to obstruct the identification of their criminal origin.

The offence of financing terrorism occurs when anyone (i) collects, disburses or makes available goods or money intended to be used, in whole or in part, for acts of terrorism, or (ii) deposits or keeps goods or money intended for such purposes (even if not subsequently used).

b) **acts or omissions affecting the financial interests of the Union** referred to in Article 325 TFEU specified in the relevant EU secondary legislation;

According to Article 2 of the relevant directive, 'financial interests' includes all revenue and expenditure covered by the Union budget, including VAT revenue.

Examples of infringements: fraud involving Community resources; cross-border VAT fraud; breaches of customs law.

c) **acts or omissions relating to the internal market**, as referred to in Article 26(2) TFEU, including:

a. infringements of EU competition rules (e.g. abuse of a dominant position, agreements between undertakings restricting competition in the internal market, merger rules) *(N.B.: these regulations do not apply to the Company to which this Procedure is addressed and are therefore relevant only in the event that the Company in its capacity as supplier and/or partner of third parties detects any violations in this matter exclusively referable to the activity of the latter),*

b. violation of the Union rules on **State aid**

(e.g. falsification of data and information in order to obtain state aid that is not due, use of state aid for purposes other than those for which it was granted, false reporting)

c. internal market violations related to acts in breach of **corporate tax** rules

(e.g. any accounting/tax irregularity aimed at distorting the correct assessment of IRES, IRAP, such as under-declaration of turnover, over-declaration of costs, invoicing of nonexistent transactions, deduction of non-deductible costs, creation and use of slush funds), or

d. **practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the** applicable corporate tax **law;**

d) **acts or omissions that frustrate the object or purpose of the provisions of Union acts** in the areas mentioned under (a), (b) and (c).

E.g. abusive practices as defined by the case law of the EU Court of Justice. Consider, for example, an undertaking operating in a dominant market position: the law prevents such an undertaking from gaining, through its own merits and abilities, a dominant position on a market, or from ensuring that less efficient competitors remain on the market. However, such an undertaking could jeopardise, by its own conduct, effective and fair competition in the internal market by resorting to so-called abusive practices (adoption of so-called predatory pricing, target rebates, tying) in violation of the protection of free competition.

*NB. For a detailed description of these relevant sectors, please refer to the **Annex (Part I and Part II) of the Decree** available at www.normattiva.it.*

APPENDIX B - PROTECTIONS

1. PROTECTED SUBJECTS

The Protected Persons include,

- **the Whistleblower** (even anonymous, whose identity is discovered at any time),
- those who lodge a complaint with the judicial authorities in relation to a Violation,
- those who make a Public Disclosure, and
- the following categories of persons:
  - **Facilitators**,
  - **Persons in the same work context** as the Whistleblower, the person making a complaint to the judicial authority or the person making a Public Disclosure and who are **related to them by a stable emotional or kinship relationship up to the fourth degree** (cousins),
  - **Co-workers** of the Whistleblower, of the person who has reported the matter to the judicial authority or made a Public Disclosure, who work in the same work context as the Whistleblower and who have a regular and current relationship with the Whistleblower,
  - **Legal representatives of employees in the exercise of their functions in advising and supporting the Whistleblower**,
  - **Entities owned, or which are employers, or which work in the same Work Context, as the aforementioned persons, or with which the aforementioned persons have any other type of relationship in the work context, or in which they hold a significant interest.**
    For this purpose, an interest in the capital or voting rights attached to shares or participations is considered significant when, by virtue of its proportion, it enables the person holding it to exercise influence over the legal person in which the interest is held.

2. PROTECTIONS

In the event of a Report, the following three categories of legal protections are guaranteed to **all Protected Subjects**

- **PROTECTION MEASURES,**
- **SUPPORT MEASURES,**
- **RIGHT TO CONFIDENTIALITY**,

as set out below.

With regard, moreover, to **Whistleblowers only**, the Safeguards also apply if the Report or the complaint to the judicial authority or the Public Disclosure occurs in the following cases

a) **when the legal relationship** with the Company **has not yet started**, if the information on the Breaches has been acquired during the selection process or in other pre-contractual phases,

b) **during the probationary period**,

c) **after termination of the Legal Relationship**, if the Violation Information was acquired during the course of the Legal Relationship.

The **reasons** that led the person to report or publicly disclose **are irrelevant** for the purposes of the Safeguards.

3. PROTECTIVE MEASURES[3]

The following **Protection Measures** apply to Protected Persons, provided they are bona fide:

- Prohibition of Retaliation,
- Protection from Retaliation,
- Limitation of Liability,
- Waivers and Conditional Settlements.

NB: The Protection Measures also apply

(a) in cases of anonymous Reporting or Public Disclosure, if the Whistleblower was subsequently identified and retaliated against, and

(b) in cases of External Reports submitted to the competent institutions, bodies, offices and agencies of the *European* Union (*e.g. the European Anti-Fraud Office*), in accordance with the conditions for External Reports themselves.

3.1. Prohibition of Retaliation

Protected Persons may not be subjected to any Retaliation (**prohibition of retaliatory acts**). The Company undertakes to strictly enforce this prohibition.

Retaliation" is to be **understood extensively**, including, but not limited to;

a) **dismissal**, **suspension** or equivalent measures;

(b) downgrading or **non-promotion**;

(c) change of duties, **change of place of work**, **reduction of salary**, **change of working hours**;

(d) **suspension of training** or any restriction on access to it;

(e) **demerits or negative references**;

f) the adoption of **disciplinary measures** or any other sanction, including a fine;

(g) **coercion, intimidation**, **harassment** or **ostracism**;

(h) **discrimination** or otherwise **unfavourable treatment**;

(i) **failure to convert** a fixed-term employment contract into an employment contract of indefinite duration, **where the employee had legitimate expectations of** such conversion;

(j) the **non-renewal** or **early termination** of a fixed-term employment contract

(k) **damage**, including to a person's reputation, in particular on social media, or **economic or financial** loss, including loss of economic opportunities and loss of income

(l) inclusion on improper lists (e.g. **blacklists)** 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;

[3] The protection envisaged for the Whistleblower will be guaranteed only in the case of reports made by clearly identified persons. The disclosure of the identity by the Whistleblower may take place at any time after the Report, without prejudice to the protection granted above.

(m) the **early** termination (termination) or **cancellation of a contract for the supply of goods or services**; **the introduction of detrimental changes** to the service or supply contract;

n) the **cancellation of a licence or permit**;

(o) the request to undergo **psychiatric or medical examinations**.

3.2. <u>Protection from Retaliation</u>

3.2.1. Retaliation

In the event that a member of the Company, in contravention of the provisions of this Procedure, engages in direct or indirect retaliatory acts, the Company itself shall take the necessary measures to ensure that such acts cease as soon as possible and, where appropriate, shall take the necessary disciplinary or liability measures against those responsible.

3.2.2. Invalidity of acts

In case of non-application or non-compliance, even partial, of the prohibition of retaliatory acts by the Company, the Protected Subject may invoke, even cumulatively:

- **The nullity ex lege of the acts of Retaliation**, as well as of the administrative acts aimed at preventing or hindering the submission of Whistleblowings, resulting in the restoration of the situation prior to the same.
- The **reinstatement in the workplace** under the same conditions ex ante, pursuant to the legislation applicable to the worker, if the Protected Subject was dismissed because of the Report.

  Non-exhaustive examples of remedial actions

  - ✓ *Fair access to any promotion and training that may have been denied*
  - ✓ *Withdrawal of litigation against the Whistleblower*
  - ✓ *Deletion of any record/data/document that could constitute a file for a blacklist or subsequent retaliation*
  - ✓ *Reopening of a tender procedure*
  - ✓ *Reinstatement of a cancelled contract*
  - ✓ *Apology*
  - ✓ *Acknowledgement for upholding the values or interest of the Company through the Violation Report*
  - ✓ *Financial compensation for past, present and future losses*
  - ✓ *Financial compensation for pain and suffering, including medical expenses*
- **Compensation for damages**, if any.

3.2.3. Reporting to ANAC

Whistleblowers may report to the ANAC any Retaliation they believe they have suffered.

In order to acquire preliminary elements that are indispensable for ascertaining the retaliation, ANAC may avail itself of the cooperation of the Civil Service Inspectorate and INL, within the scope of their respective competences, without prejudice to ANAC's exclusive competence regarding the assessment of the elements acquired and the possible application of administrative sanctions.

3.2.4. Burden of proof

In the context of judicial or administrative proceedings or, in any case, of extrajudicial disputes concerning the ascertainment of the conduct, acts or omissions, constituting Prohibited Retaliation,

it is presumed that the same have been put in place as a result of the Reporting or Public Disclosure itself.

The burden of proving that they were motivated by duly justified reasons unrelated to the Report or Public Disclosure rests on the person who has committed them.

In the event **of a claim for damages brought before the judicial authority by the Whistleblower** (not, therefore, also by other Protected Persons), if the Whistleblower reasonably proves that it made a Report or Public Disclosure and suffered damage, **it shall be presumed, unless the accused proves otherwise, that the damage is a consequence of such Report or Public Disclosure**.

3.3. Limitations of Liability

The reporting entity or person shall not be criminally liable, and **any further civil or administrative liability**, in judicial proceedings, for the disclosure or dissemination of Infringement Information:

- covered by **secrecy** obligations (official, corporate, professional, scientific, commercial or industrial) (e.g. punished by Articles 326, 622, 623 of the Italian Criminal Code),
- relating to the protection of copyright,
- relating to **the protection of personal data** (privacy),
- offending the reputation of the Involved Person (**defamation**), or

provided, however, that there were **reasonable grounds to believe** that Public Reporting or Disclosure of the same Information **was necessary** to disclose the Infringement.

The above-mentioned criminal, civil and administrative exemption, however, does not apply

a) in the case of **criminal conduct engaged in by the Whistleblower in order to acquire or access the Information that** is the subject of the Report.
E.g., the offence of unauthorised access to a computer system exists in relation to the act of a person who intentionally hacked into a work colleague's e-mail system to obtain evidence in support of the Report, and
b) **for conduct, acts or omissions** not related to the Report, the report to the judicial authorities or the Public Disclosure or not strictly necessary to disclose the Breach.

The Company may also order the imposition of **disciplinary sanctions** against persons who decide to retaliate, in accordance with the following documents:

- National Collective Labour Agreement and the Company Collective Bargaining Agreement, if any (to be understood as expressly referred to herein), and/or
- Organisational Model 231.

3.4. Obligatory Form of Waiver and Settlement

The rights and protections provided in favour of the Whistleblower **may not be subject to waiver or settlement, in whole or in part,** which, therefore, shall be deemed invalid, unless they are made in the form and manner set forth in Article 2113, fourth paragraph, of the Civil Code.

4. SUPPORT MEASURES

The Whistleblower is also entitled to **support measures** consisting of **free information, assistance and advice** on the modalities of Whistleblowing and on the protection from retaliation

offered by national and European Union law provisions, on the rights of the Whistleblower, and on the terms and conditions of access to legal aid.

These support measures are provided by Third Sector Entities (ETS) that have entered into agreements with ANAC. The list of Third Sector Entities is published on the website: https://www.anticorruzione.it/-/whistleblowing.

Such free information, assistance and advice may be requested at any time by the Whistleblower from these Third Sector Entities, even before the actual communication of the Report.

NB: The activity of the ETSs consists in providing information, assistance and advice in the terms set out above, also during the Reporting process; however, the actual Reporting must be carried out personally by the Whistleblower and in any case the activities of the ETSs must be kept separate from the actual examination of the Report, which is the sole responsibility of the Case Manager.

5. CONFIDENTIALITY

5.1. Generalities

Reports may not be used beyond what is necessary for their proper follow-up.

The non-anonymous Whistleblower must be guaranteed, by the Company, the Whistleblower Manager and anyone else involved in the receipt and processing of a Whistleblowing, confidentiality regarding:

- **his or her identity and that of the Facilitators** (right to confidentiality), throughout the whole process of handling the Report, towards anyone who is not the Case Manager or otherwise authorised, and
- **the content of the Report**, including the **documentation** attached to it, to the extent that its disclosure, even indirectly, may allow the identification of the Whistleblower.

In all phases of activity, **it is forbidden to reveal the identity of the Whistleblower to the Reported Subject and to other subjects not expressly authorised, without the** express **consent of** the Whistleblower.

The Internal Reporting Channels adopted by the Company must, therefore, guarantee the aforementioned confidentiality, which also extends to the identity of any other interested person mentioned in the Report (e.g. Involved Person, witnesses, etc.) or whose name is identified in the course of the assessments and investigations following the Report.

In this regard, specific confidentiality undertakings will also be signed with the persons in charge of handling them.

5.2. Exclusion of confidentiality

The confidentiality obligation **does not apply** in the following cases:

(i) when the **disclosure of** the identity of the Alerts **is a necessary and proportionate obligation** imposed by Union or national law **in the context of investigations** by national authorities **or judicial proceedings**, including in order to safeguard the rights of defence of the person reported.
To this end, the **Involved Person should be warned without delay by the Case Managers of an unsubstantiated Report made in bad faith or with gross negligence against**

him/her in order to be able to consider whether to exercise any rights against the person making the Report[4] ; or

ii) the existence of an obligation to communicate the name of the Whistleblower to the **judicial authorities** (Court, Public Prosecutor's Office), **or the Police**, or

iii) any **voluntary waiver** in writing of confidentiality at any time by the Whistleblower, or

(iv) where **knowledge of** the identity of the **Whistleblower is indispensable** for **the accused's defence**, only where the Whistleblower has given his/her express **consent to** the disclosure of his/her identity.

Such disclosures are subject to the guarantees provided for by the applicable rules. In any case, the Whistleblower **must be informed in writing** by the Case Manager or by the competent Authority of the **reasons for** the disclosure of confidential data **before** his/her identity **is disclosed**, **unless this would prejudice the relevant investigation or** judicial **proceedings**[5]**.**

The Company, the Case Managers and anyone else involved in the receipt and processing of a Report must also protect **the identity of the Persons Involved and of the other persons mentioned in the Report** until the conclusion of the proceedings initiated as a result of the Report, in compliance with the same guarantees of confidentiality provided for in favour of the Whistleblower.

6. PREREQUISITES OF THE PROTECTIONS. REPORTING IN BAD FAITH OR WITH SERIOUS MISCONDUCT

The Protection Measures described above apply if the following **conditions** are met:

a) at the time of the Report or Complaint to the Judicial Authority or Public Disclosure, the Whistleblower had **reasonable grounds to believe that the Violation Information** reported or publicly Disclosed **was true,** even if no conclusive evidence is provided, and fell within the objective scope of Section 2.3; and

b) the Report or Public Disclosure was made on the basis of the provisions of this Procedure and applicable law.

The Protection of the Protected Subjects also exists in the case of **Reports or Disclosures that later prove to be unfounded**, if the Whistleblower, at the time of the Report or Public Disclosure, had **reasonable grounds to believe that the Report was necessary to disclose the Violation** and the Report or Public Disclosure or report to the Judicial Authority that the Information was within the scope of this Procedure.

Safeguards in favour of the Protected Subjects are not guaranteed, and a Disciplinary Sanction shall also be imposed on the Whistleblower, if **it is established, even by a first instance judgement:**

i) criminal liability of the Whistleblower **for offences of slander or defamation** in relation to the facts reported, or

[4] In order to allow the reported person to file a complaint-complaint for the offence of slander, defamation or any other offence that may be detectable in the specific case, and also in view of the fact that the reported person, in Italy, may entrust a lawyer with the task of carrying out "preventive defensive investigations" (pursuant to Articles 327 bis and 391 nonies of the Code of Criminal Procedure, institutes that can also serve the person unjustly accused of a crime to identify the identity of the person who made an anonymous report against him).

[5] When the competent authority informs the reporting person as above, it sends him a written explanation of the reasons for disclosing the confidential data in question.

ii) **the civil liability** of the Whistleblower, for the same reason (pursuant to Article 2043 of the Civil Code, which provides for the right to compensation for damages in favour of anyone who is the victim of an extra-contractual damage caused by a third party), in cases of **wilful misconduct or gross negligence**.

Reports made with the **awareness of** the **abuse/exploitation** of the Reporting procedure, e.g. manifestly unfounded, **opportunistic** and/or made for the **sole purpose of harming** the reported person or other persons mentioned in the Report (employees, members of corporate bodies, suppliers, partners, group companies, etc.) are to be considered in **bad faith/grievous misconduct** (and therefore a source of liability, in disciplinary and other competent fora).

In the event of a **Public Disclosure**, the Whistleblower benefits from Legal Protection if, in addition to the basic condition, one of the Public Disclosure Prerequisites set out in Chapter 3.3.2.2 is also met.

APPENDIX C - PROCESSING OF PERSONAL DATA

1.1 Any processing of personal data carried out for the purposes of the management of the Report must be carried out in accordance with the legislation on the protection of personal data (GDPR, Supervisory Measures, Legislative Decree 196/2003).[6]
Accordingly, anyone involved in the receipt and processing of non-anonymous Reports **is required to comply with all the policies, delegations, appointments, authorisations, procedures, protocols and written security instructions set out in the** Company's **privacy system**, without prejudice to the further rules set out in this procedure.

1.2 **Personal data that appear not reasonably pertinent and useful for the processing of a specific Report shall not be collected or, if received or collected accidentally, shall be promptly deleted** by the appropriate Case Manager with respect to the Violation.

Similarly**, any personal data reported and referring to conduct not included in the scope of the law and/or this Procedure shall be deleted**.
If the information **received contains personal data included in the special categories of data referred to in Article 9 of the GDPR, it will be deleted immediately**, without being recorded and processed.

1.3 **If it is established that the information provided or part of it is untrue, it must be deleted immediately** as soon as this circumstance emerges, **unless the untruthfulness may constitute a criminal offence**, in which case the information will be retained for as long as necessary during the legal proceedings.

1.4 The aforementioned processing shall be carried out by the Company (data controller) in compliance with the general principles set out in Articles 5[7] and 25[8] of the GDPR, as well as by taking appropriate measures to protect the rights and freedoms of the data subjects.

---

[6] And, by the Authorities competent for the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, of Directive (EU) 2016/680.
7 Art. 5 GDPR: Personal data shall be:
(a) processed lawfully, fairly and transparently towards the data subject ("lawfulness, fairness and transparency");
(b) collected for **specified, explicit and legitimate purposes**, and further processed in a way that is not incompatible with those purposes ('purpose limitation');
(c) **adequate, relevant and limited to** what is necessary in relation to the purposes for which they are processed ('data minimisation')
(d) **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that data which are inaccurate in relation to the purposes for which they are processed ('accuracy') are erased or rectified without delay
(e) **kept** in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which** they are processed ('limited storage'); and
(f) processed in such a way as to **ensure appropriate security of** personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage ('integrity and confidentiality')
8 Article 25 GDPR: Article 25 Data protection by design and data protection by default
1. Taking into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing, as well as risks of varying likelihood and severity to the rights and freedoms of natural persons constituted by the processing both when determining the means of the processing and at the time of the processing itself, the controller shall implement appropriate technical and organisational measures, such as pseudonymisation, to implement effectively the principles of data protection, such as minimisation, and to integrate in the processing the necessary safeguards in order to meet the requirements of this Regulation and to protect the rights of data subjects.
2. The controller shall **implement appropriate technical and organisational measures** to ensure that only personal data necessary for each specific purpose of processing are processed by default. This obligation shall apply to the amount of personal data collected, the scope of the processing, the storage period and the accessibility. In particular, these measures ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person.

1.5 The Company's Case Manager, in coordination with the IT Function, the Privacy Function and the HR Function:

- defines, by means of this procedure and its annexes, its own model for the receipt and management of Internal Reports, identifying technical and organisational measures suitable to guarantee a level of security appropriate to the specific risks arising from the processing operations performed,
- regulates the relationship with any external suppliers that process personal data on behalf of the Company pursuant to Article 28 of the GDPR (e.g. external Data Processors appointed by the Company, third party technical managers of the Portal/Software),
- provides, and/or identifies the different corporate Functions, if any, in charge of providing, to the Whistleblower, to the Involved Persons and to the other relevant categories of data subjects, appropriate ***information on the processing of personal data*** (pursuant to Articles 13 and 14 of the GDPR), in compliance with the texts approved by the competent Board of Directors of the Company.

1.6 Access to the personal data contained in the Portal/Software shall be limited, within the scope of their respective competences and functions, exclusively to:

a) the System Managers (Admin) who directly manage it, within the limits of the privileges attributed to the same;
b) the Case Managers designated on the basis of this Procedure, and, upon their authorisation, the external consultants delegated in the investigation, with whom prior confidentiality agreements will be signed;
c) any appointed Data Processors (which include the 231 Supervisory Board when it acts as Case Manager limited to Reports relating to 231 Breaches) and/or any external data processors designated by the Company (which include the 231 Supervisory Board when it acts as Case Manager in relation to Reports not relating to 231 Breaches).

Determining the rules on the information to data subjects pursuant to Articles 13-14 GDPR:

The ***Whistleblowing Privacy Notice*** must be made available to Data Subjects by the relevant Case Manager in the following main ways:

- by means of a specific **link/text viewable on the landing page of the Portal/Software**;
- by hand delivery, or as an attachment to a chat via videoconference, at the first useful opportunity, in case of **personal meeting** with the Reporting Subject who has not used the Portal/Software for the Reporting
- in the event that the first useful contact with the person concerned takes place by telephone (in particular, in the event that the Whistleblower requests a personal meeting by telephone): by verbal notice of the availability of the ***Privacy Policy*** on the landing page of the Portal/Software and/or in the separate "whistleblowing" section in the footer of the Company's website.

a. **response to the exercise of data subject's rights**: the Company acts as an independent data controller in accordance with its own procedures for managing the exercise of data subject's rights, to which reference is made herein;

b. **personal data breaches**: the Company acts as an autonomous data controller in accordance with its own data breach management procedures relating to personal data related to the Reports, to which reference is made herein;
c. **security measures**: the Company is required to comply with the security measures provided for i) by this Procedure, ii) by the technical-functional specifications of the Portal/Software, ii) by its own privacy system, iv) by the personal data protection legislation applicable to it;
the security measures applied to the Portal/Software are illustrated in the mandatory DPIA document prepared by the Company as well as in the additional documents referred to therein from time to time.