

WHISTLEBLOWING PROCEDURE

System for reporting work-related breaches – Collection, verification and treatment of reports -

**Approved by the Board of Directors of Italtel SpA
in the meeting of 23 September 2026**

Edition 3

Italtel SpA
office Via Caldera, 21 20153 Milan
Secondary office Via Laurentina , 449/451 00142 – Rome
Share capital Euro5,732,073.28 fully paid up.
Tax code / VAT number 15882821000

Index

1.	Objective	3
2.	Introduction	3
3.	Scope of application	3
4.	References	4
5.	People who can submit a report	4
6.	Subject of the reports	5
7.	Internal channels available for reporting	6
8.	Contents of the report	7
9.	Anonymous reports	8
10.	Recipients of the reports	8
11.	Process of receiving and processing the report	8
11.1	Entering the report	9
11.2	Preliminary analysis	9
11.3	Examination of documentation	9
11.4	Conducting investigations	9
11.5	Definition of measures	9
11.6	Closing the report	10
12.	Essential elements of the reporting process	12
12.1	Disciplinary measures and sanctions	12
12.2	<i>Feedback</i> to the whistleblower	12
12.3	Obligation of confidentiality	13
12.4	Conflict of interest	13
13.	Protections for the whistleblower	13
14.	Protections for the person involved	15
15.	Processing of personal data	15
16.	Data retention period	15
17.	Reporting	16
18.	Training and information	16
19.	Attachment	17

1. Objective

This procedure aims to describe the **system for reporting violations of which one has become aware in the context of one's work context** (hereinafter, also “**Whistleblowing system**” or “**Whistleblowing**”) used within the Italtel Group (hereinafter, also “**Group**”).

The purpose of the Whistleblowing system is to counter possible unlawful conduct that may take place in the workplace and to promote and disseminate a culture of ethics and legality, as well as to protect people reporting such breaches.

Hereinafter, the terms “**Company**” or “**Italtel**” will mean Italtel S.p.A, the parent company of the Italtel Group, and the term “**Model 231**” will mean the Organization, Management and Control Model of Italtel S.p.A pursuant to Legislative Decree 231/2001.

This procedure is submitted to the Supervisory Body for its opinion (Model 231) and subsequently submitted to the Board of Directors for approval. It is communicated to staff via internal organizational communication on the company intranet.

2. Introduction

The Whistleblowing system allows for the collection of reports on unlawful conduct of which one becomes aware in a work-related context.

The methods of processing reports acquired through the system described in this procedure comply with the provisions of Legislative Decree no. 24 of 10 March 2023 *“Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and provisions concerning the protection of persons who report breaches of national law”* (hereinafter also the “**Decree**”) as they protect the authors of the reports (hereinafter also “**reporting persons**” or “**whistleblowers**”) from possible retaliation or discrimination resulting from the same reports and guarantee the confidentiality of the identity of the authors themselves until the conclusion of the proceedings initiated as a result of the report.

The Decree provides, among other provisions, that the ANAC (National Anti-Corruption Authority) will apply sanctions against those who violate the measures protecting whistleblowers and those who, with intent or gross negligence, make reports that prove to be unfounded. It also requires the Company to apply the sanctions indicated in Model 231 for the same responsibilities.

The Decree also requires ANAC to offer support measures consisting of free information, assistance, and advice on reporting procedures and protection from retaliation under national and European Union regulations. Finally, it establishes that ANAC will maintain a list of third sector organizations that provide support to whistleblowers (<https://www.anticorruzione.it/-/whistleblowing#p0>).

3. Scope of application

This procedure applies to the activities of the Italtel work context

“Work-related context” means any current or past work or professional activity through which, regardless of the nature of such activity, a person acquires information about violations and in which they may be at risk of retaliation if they report or disclose it publicly or report it to judicial or accounting authorities.

The system described here also applies when the employment relationship has not yet begun and information on violations was acquired during the selection process or in other pre-contractual phases.

4. References

- Legislative Decree no. 24 of 10 March 2023 *“Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law and laying down provisions regarding the protection of persons reporting breaches of national legislation”*
- Legislative Decree 8 June 2001, n. 231 *“ Regulation of the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law 29 September 2000, n. 300 ”*
- Italtel Code of Ethics
- Italtel S.p.A. Organization, Management and Control Model pursuant to Legislative Decree 231/2001 and subsequent amendments.
- European Regulation 2016/679 - GDPR (*General Data Protection Regulation*) of 27 April 2016
- Legislative Decree 30 June 2003, n. 196 *“Personal Data Protection Code”* as subsequently integrated and amended
- ANAC Guidelines - *“Guidelines on the protection of persons reporting violations of Union law and protection of persons reporting violations of national regulatory provisions - Procedures for the submission and management of external reports”* Approved with Resolution No. 311 of 12 July 2023 and subsequent amendments.
- Provision of the Italian Data Protection Authority, no. 304 of 6 July 2023 regarding the ANAC Guidelines
- Provision no. 581 of the Italian Data Protection Authority of 9 October 2025, containing its opinion on the draft *“Guidelines on Whistleblowing on Internal Reporting Channels”* and the resolution amending and supplementing the ANAC Guidelines on Whistleblowing.
- Confindustria Operational Guide on the new Whistleblowing regulations, updated May 2026.

5. People who can submit a report

People eligible to access the reporting system are employees, directors, shareholders, auditors, persons with administrative, management, control, supervisory, or representation roles, and, in general, anyone who operates, in Italy or abroad, on behalf of or for the benefit of the Italtel Group or who maintain business relationships with it through any type of contract or assignment (collaborators, consultants,

suppliers, agents, intermediaries, interns, etc.) who wish to report a breach they become aware of in the work-related context.

The protection of the above-mentioned individuals also applies in cases where information about violations was acquired before the legal relationship began (pre-contractual phases) or during a probationary period, or after the termination of the legal relationship if the information about violations was acquired during the relationship itself. Furthermore, protection measures apply not only to the reporting person but also to individuals within the same work environment who are linked to the reporting person by a stable personal relationship or a family tie up to the fourth degree; protection measures apply to the reporter's colleagues with whom they have a regular, ongoing working relationship and, finally, to entities owned by the reporting person and entities operating within the same work environment as the aforementioned individuals.

Within the whistleblowing system, governed by Legislative Decree No. 24 of March 10, 2023, the **internal reporting channel** is the primary tool for promoting the timely disclosure of unlawful conduct or irregularities detected in the workplace. Establishing an effective, accessible internal reporting channel that complies with the confidentiality guarantees required by law is an essential element of the corporate compliance system, as it allows for the timely detection of violations, facilitating their management and resolution before they cause detrimental consequences for the company, workers, or other stakeholders. In this regard, Italtel S.p.A provides both written and oral reporting methods (see Section 7 of this procedure). Should these reporting methods prove ineffective, the whistleblowing regulations provide additional tools. Reporting persons may, in fact, file an **external report** to ANAC if they have already filed an internal report through the Whistleblowing system described in this procedure and have received no response, or if they have reasonable grounds to believe that the report is not being effectively addressed or may result in a real risk of retaliation. Furthermore, after filing an internal and external report, or after filing an external report directly without receiving a response within the required timeframe, reporting persons may make a so-called "**public disclosure**," that is, make information about violations publicly available through the press, electronic media, or any other means of dissemination capable of reaching a large number of people.

Public disclosure may be made, benefiting from the protection provided by the Decree, even in cases where the violation may constitute an imminent or manifest danger to the public interest, or where the reporting person has reasonable grounds to believe that the report may entail the risk of retaliation or that evidence of the violation may be hidden or destroyed, or, finally, that the person receiving the report may be colluding with the perpetrator of the violation or involved in the violation itself.

6. Subject of the reports

The events that may be the subject of a report generally concern information, **including reasonable suspicions, regarding violations committed in the context of work activities that could harm the integrity of the Company or the Group.**

Such events must be attributable to:

- administrative, accounting, civil or criminal offenses;
- violations of the Organization, Management and Control Model pursuant to Legislative Decree 231/2001;
- violations of the Code of Ethics (discrimination, harassment, conflict of interest, ...);
- violations of internal provisions or procedures subject to disciplinary action;
- in general, facts that may constitute crimes or cause damage (financial or image) to the Company or the Group.

They must not be reported and, in any case, if submitted, after a preliminary check on their admissibility, they will be ignored by the system:

- disputes, claims or requests related to a personal interest that pertain exclusively to one's individual employment relationships;
- facts based on “rumour” or “hearsay”.

Furthermore, the following cannot be reported pursuant to art. 1, paragraph 2, letters b) and c) of Legislative Decree 24/2023:

- ✓ violations for which specific mandatory reporting channels already exist under national or European Union legislation, as referred to in the decree;
- ✓ violations affecting national security, as well as procurement relating to defence or national security.

The decree also specifies that the special provisions established by national and European Union legislation in particularly sensitive matters, such as the protection of classified information, legal and medical professional secrecy, the confidentiality of judicial decisions, as well as provisions on criminal procedure, remain applicable.

7. Internal channels available for reporting

People wishing to submit internal reports in writing have the following channels available:

➤ **web portal**

- accessible via the dedicated section on the Company intranet or via the Company website (<https://www.italtel.com/it/about/whistleblowing/>)

➤ **e-mail address**

- comitato_etico@italtel.com (the recipients of which are the members of the Ethics Committee)
- The dedicated email address represents an alternative and residual channel, made available to whistleblowers to facilitate access to the reporting system. Access is permitted only to members of the Ethics Committee expressly authorized to manage reports, in compliance with appropriate technical and organizational measures aimed at ensuring the confidentiality, integrity, and security of the personal data processed.

Those who wish to report verbally can call the following **number**, which is answered by the Head of the Internal Audit function.

- +39 02 4388 2421

Italtel does not provide the option of recording verbal reports. The content of the telephone call will be documented in a written record, and that record will be shared with the whistleblower.

The reporting person can verify, correct and confirm the content of the transcript by signing it.

The web portal is the primary and preferred reporting channel adopted by the Company. This channel guarantees, also by encryption tools, the confidentiality of the identity of the reporting person, the person involved, and any persons mentioned in the report, as well as the content of the report and related documentation.

The report may also be made through **a direct conversation** between the whistleblower and the recipient of the report, identified as the Head of Internal Audit. In this case, the report may be transcribed in full in a written report; in such circumstances, the reporting person may verify, correct, and confirm the content of the report by signing it.

Following receipt of the report via oral channel (telephone or face-to-face interview), the Head of the Internal Audit function shares the relevant content with the Ethics Committee for collegial evaluation, in order to ensure uniform treatment with respect to reports received via the platform and via e-mail (comitato_etico@italtel.com)

In fact, reports sent via the platform are received and processed collegially by the Ethics Committee pursuant to Article 10 below, as are those sent to the email address comitato_etico@italtel.com.

8. Contents of the report

In general, **the report must contain information that allows the bodies responsible for analyzing and processing the report to conduct appropriate checks to verify its validity.** The report, it is reiterated, must concern a work-related matter and be aimed at protecting the integrity of the Company or Group.

The minimum information required for a complete description of the report is reported below:

- Name and position of the whistleblower
- Type of report chosen from the following (proposed by the web portal):
 - violation of laws
 - violation of Model 231
 - violation of the Italtel Code of Ethics

- violation of internal provisions or procedures
- other
- Clear and complete description of the facts being reported, including the places and dates on which they occurred
- Name and position of the person who committed the acts (the “person involved”)
- Any names of other people who can report on the facts
- Further information useful for verifying the facts

Additionally, the web portal allows you to attach documents, photos, or audio and video recordings.

Attached (paragraph 19) is the reporting form to be used in the event that you decide to use communication channels other than the web portal (as indicated in the previous paragraph 7).

9. Anonymous reports

Anonymous reports are those in which the identity of the whistleblower is neither disclosed nor otherwise identifiable. These reports are taken into consideration when the information provided is detailed enough to reveal facts and situations that can be investigated. **Please note that if the report is made anonymously, the Company is unable to activate the appropriate legal protections to prevent retaliation against the whistleblower. However, legal protections also apply to anonymous reports if the reporting person is subsequently identified and has suffered retaliation.**

10. Recipients of the reports

Reports are received, analyzed, verified, and processed by the Ethics Committee (hereinafter also “EC”), consisting of the General Counsel and Chief Compliance Officer and the heads of the Human Resources and Internal Audit functions. If a report is received by a person not authorized to process reports and, therefore, not a member of the aforementioned Ethics Committee, that person must immediately forward it to one of the EC members. That person must avoid, to the extent possible, becoming aware of the report’s content and, if she/he does become aware of it, she/he must ensure the confidentiality of the identity of all individuals named in the report and its content.

11. Process of receiving and processing the report

The following describes the report management process carried out through the **dedicated web portal**.

11.1 Entering the report

The reporting person submits the report on the web portal following the instructions provided. As described in paragraph 9 above, the whistleblower can choose to remain anonymous or disclose her/his personal data.

Once the report is submitted, the portal sends a notification to the members of the Ethics Committee, sets the report to " *Open* " status and issues the whistleblower a **unique code** through which she/he will be able to access the portal at any time to view the status of her/his report.

11.2 Preliminary analysis

The initial assessment of the report is carried out by the General Counsel and Chief Compliance Officer (hereinafter also "CO") in order to evaluate the admissibility of the report itself on the basis of what is set out in the previous paragraph 6. If the CO deems the report inadmissible, he/she places it in "*Rejected* " status and archives it on the portal, reporting the reasons for this decision on the same.

If the CO deems the report admissible, it is upgraded to " *Accepted* " status and, together with the other members of the Ethics Committee, proceeds to analyze the information contained in the report. **The upgrade must occur within seven days of receiving the report and can be verified by the reporting person using their unique code.**

11.3 Examination of documentation

Once the documentation relating to the report has been received, the Ethics Committee begins the analysis phase, evaluating whether to contact the whistleblower (if not anonymous) if further information or information useful for subsequent investigations is needed. At this stage, the CO moves the report to the " *In Progress* " status.

In the event that the report concerns a violation of Model 231, the CO promptly informs the Supervisory Body.

11.4 Conducting investigations

After reviewing the documentation, the Ethics Committee decides whether to proceed with further investigations, possibly involving other functions (e.g., ICT) or external consultants only to the extent necessary to properly conduct the checks and in compliance with the principles of necessity, minimization, proportionality, and confidentiality of personal data processing. The aim is to verify the veracity of the report based on objective evidence. In the case of reports of unlawful conduct discovered in the course of the work of a foreign subsidiary of the Group, the Ethics Committee will evaluate how to involve the foreign company's Supervisory Body (if established) or the relevant local functions.

11.5 Definition of measures

Once the investigation is complete, the Ethics Committee identifies the necessary measures, also taking into account the potential risks to the Company. Once the validity of the reported matter has been

ascertained, it determines the appropriate communication methods for the individual involved. Depending on the seriousness of the report, the Committee may also decide to report the matter to the judicial or accounting authorities.

In the event that the report concerns a violation of Model 231, the Ethics Committee shares the decisions and measures to be taken with the Supervisory Body.

The analysis and investigations conducted must also include the possibility of identifying, among the measures, any actions suitable for strengthening the internal control system where the latter has highlighted gaps or weaknesses.

11.6 Closing the report

Once the necessary measures have been identified, the CO will place the report in " *Closed* " status. **The report must be closed within three months of receiving the report;** feedback must be provided to the whistleblower within the same timeframe. The Ethics Committee, through the CO, will monitor the identified actions until they are fully addressed. Please note that the above-mentioned timeframe may also consist of a communication announcing, for example, the initiation of an internal investigation or referral to a competent authority for further investigation. In such cases, without prejudice to any subsequent updates provided to the whistleblower regarding the progress of the investigation, the final outcome must in any event be communicated to the whistleblower.

The following figure 1 schematically shows the process described so far, highlighting the activities and states to which each report is subjected as well as the related responsibilities.

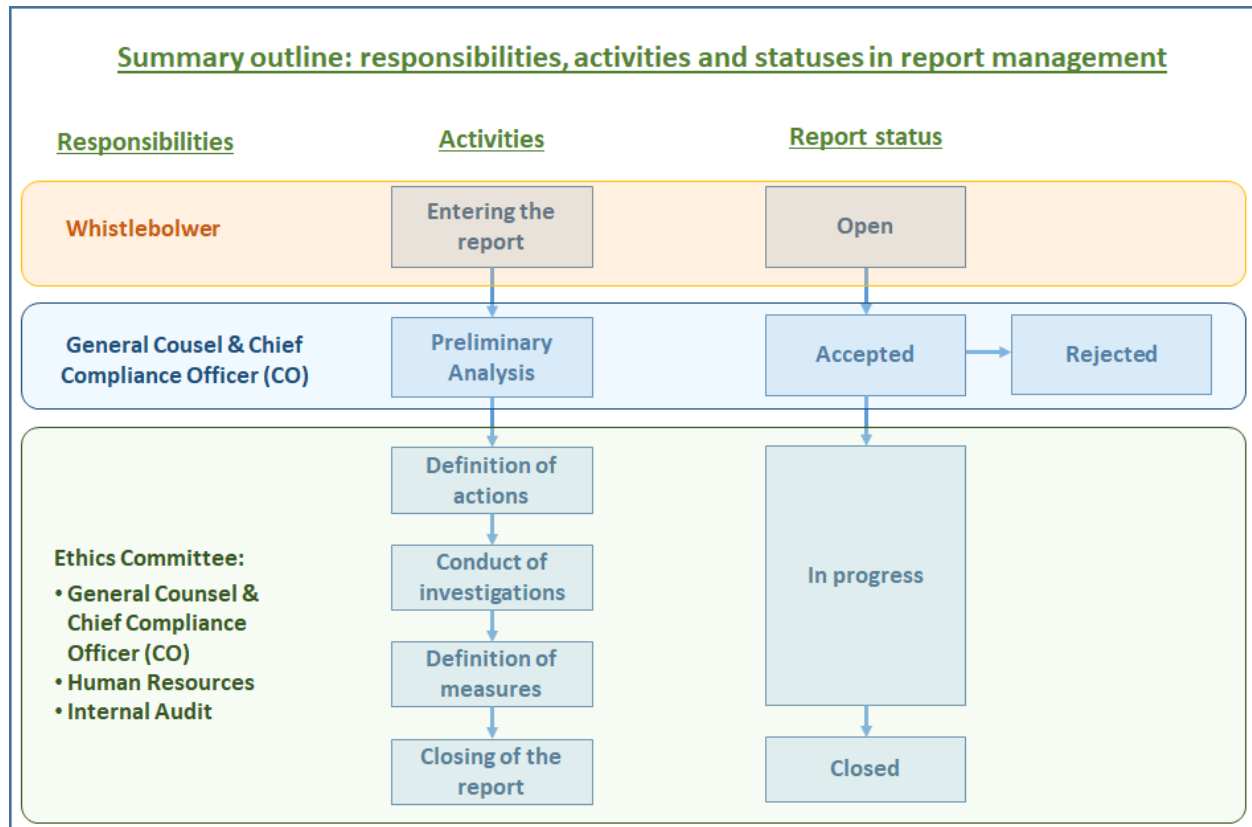


Figure 1

12. Essential elements of the reporting process

Below, we outline the essential elements that the reporting process must include to ensure the necessary protection and confidentiality measures are in place for all individuals involved.

12.1 Disciplinary measures and sanctions

The disciplinary measures to be applied in relation to the facts found are based on the **Workers' Statute and applicable national collective bargaining agreements**. If the act was committed by a person external to the Company or Group (pursuant to paragraph 5), any sanctions to be applied must be based on the letters of appointment or contracts governing the relationships with such individuals. These contracts must include appropriate clauses that regulate the aforementioned sanctions (termination of the contract, penalties, etc.) in the event of potential violations.

If the report is found, due to the whistleblower's intent or gross negligence, to be unfounded and manifestly defamatory of the person involved, the whistleblower will be subject to disciplinary action or sanctions pursuant to the applicable agreements. Specifically, if the whistleblower made the report with intent or gross negligence, he or she will be subject to a financial sanction by the ANAC, unless he or she has been convicted, even in the first instance, of defamation or slander.

Furthermore, when the reporting person's criminal liability for defamation or slander is ascertained, even by a first-instance ruling, in the event of intent or gross negligence, the legal protections provided by the Decree are not guaranteed.

12.2 Feedback to the whistleblower

Throughout the entire duration of the report's management, the various stages of its processing are recorded on the portal, through which **the whistleblower can obtain continuous feedback on the progress of his or her specific report using the unique code provided by the portal itself when the report was opened**.

If the reporting person chooses to use the alternative written communication channel other than the web portal (see the email address referred to in paragraph 7), the reporting person must use the form attached to this procedure to submit the report, entering the requested information. Once the form is delivered via the aforementioned email channel, the CO will enter the relevant information on the web portal to track the progress of the report according to the steps described above. In this case, the unique code will be communicated to the whistleblower if they have provided personal information that allows them to be contacted; without this information, it will not be possible to inform the whistleblower, who will therefore have chosen to remain anonymous.

If the report is submitted orally, either in person or by telephone, with the Internal Audit Manager, the information collected will be entered into the web portal by the CO, subject to the whistleblower's acceptance of the text of the report (see section 7). In this case, too, the unique code will be communicated to the whistleblower so they can receive ongoing feedback on the progress of their report.

12.3 Obligation of confidentiality

The departments responsible for evaluating reports are the only ones with access to the portal and **are required to maintain the strictest confidentiality of its contents**. Disciplinary measures or sanctions, pursuant to applicable contracts, are applicable to individuals who violate confidentiality obligations or fail to verify a report. Specifically, those responsible for such violations will be subject to a financial penalty from the ANAC.

12.4 Conflict of interest

If a whistleblower believes that one of the members of the Ethics Committee is involved in any way in the report, or believes it necessary or even appropriate that one of these members be excluded from handling the report, they can highlight this circumstance within the portal, which will automatically modify the information flow required for processing the report, preventing the sending of information and notifications to the indicated member. In any case, the whistleblower may alternatively file an **external report** directly with the ANAC, as described in paragraph 5 above.

13. Protections for the whistleblower

The web portal dedicated to Whistleblowing is designed to **guarantee the confidentiality and protection of the whistleblower's identity** (unless they have explicitly consented to its disclosure) and the report data throughout all stages of its processing.

Any form of direct or indirect retaliation or discrimination against the whistleblower for reasons directly or indirectly related to the report is prohibited and will not be tolerated; disciplinary action will be taken against those responsible for such retaliation or discrimination.

Retaliation is considered to be any behavior, act, or omission, even attempted or threatened, committed as a result of a report, which causes or may cause the whistleblower, directly or indirectly, unjustified harm. Specifically, retaliation to which the whistleblower may be subject includes: dismissal, demotion, unjustified transfer, mobbing, harassment, and any other type of behaviour that results in intolerable working conditions.

If the whistleblower believes they have been the victim of retaliation related to their report, they may, pursuant to the Decree, report this circumstance to the ANAC, which will inform the National Labor Inspectorate for the relevant measures. If the whistleblower believes they have suffered retaliation, the burden of proof falls on the person who committed the action; therefore, it is up to the person who took the action to demonstrate that it was not retaliatory. Therefore, in proceedings before the ANAC, retaliatory intent is presumed until proven otherwise.

Retaliatory or discriminatory dismissal, changes in duties, and any other retaliatory or discriminatory measures adopted against the whistleblower as a result of the report **are void pursuant to the Decree**.

Finally, for further protection of the whistleblower, Article 2- *undecies* , paragraph 1, letter f) of the Privacy Code, as amended by the Decree, provides that the rights of data subjects (pursuant to Articles 15 to 22 of the GDPR) cannot be exercised by submitting a request to the Data Controller or by filing a complaint with the Italian Data Protection Authority (Article 77 of the GDPR) if the exercise of such rights could result

in actual and concrete harm " *to the confidentiality of the identity of the person reporting violations of which they have become aware by virtue of their employment relationship or the duties performed [...]* ".

Therefore, the Company, while guaranteeing the right of defense of the person involved, will take into account the rule introduced to protect the confidentiality of the whistleblower.

Furthermore, the protection of the whistleblower's identity must take into account the various proceedings that may be initiated following the filing of a report. In criminal proceedings, the whistleblower's identity is protected by confidentiality until the preliminary investigation is concluded and the case is brought to trial. In accounting proceedings, similarly to criminal proceedings, the whistleblower's name cannot be revealed until the investigation is concluded. Finally, in disciplinary proceedings initiated following a report, if the complaint is based, in whole or in part, on the report and knowledge of the whistleblower's identity is essential for the defendant's defense, the report may be used by persons other than those authorized to receive or follow up on reports only with the whistleblower's express consent to disclosure of their identity.

The protective measures provided for by Legislative Decree no. 24/2023 are not limited to the whistleblower alone, but also extend to other individuals who, due to their role or specific relationship with the whistleblower, could be exposed to the risk of retaliation as a result of reporting. Specifically, these protections apply to:

- the facilitator, i.e. the natural person who assists the whistleblower in the reporting process, operating in the same work context and whose support activity must be protected by adequate guarantees of confidentiality;
- persons belonging to the same work environment as the whistleblower, the complainant, or the person who made a public disclosure, and who are linked to the latter by a stable personal relationship or a family tie within the fourth degree;
- work colleagues of the whistleblower, the complainant, or the person who has made a public disclosure, provided that they operate in the same work environment and maintain a regular and continuous relationship with them; the entities owned, exclusively or majority-owned, by the whistleblower, the complainant, or the person who made a public disclosure (for example, if the whistleblower is the majority shareholder or owner of a company, that company will also be protected from any retaliation that could indirectly affect it as a result of the report);
- the entities where the whistleblower, the complainant or the person who made a public disclosure carries out their work (the protection applies where the whistleblower carries out their work for a party other than the "formal" employer: consider, for example, a worker with a temporary contract, a consultant, a seconded employee).

In order to ensure the effective application of protection measures and to ensure compliance with the confidentiality obligations set forth in current legislation, it is appropriate that, as part of the investigation of the report, the whistleblower be asked to expressly indicate the possible existence of such entities, providing adequate evidence to demonstrate the existence of the requirements for recognition of the relevant protections.

14. Protections for the person involved

The **person involved** is the person to whom the whistleblower attributes the commission of the unlawful act or violation reported. **The identity of the person involved must be protected, as must the identity of the whistleblower; however, it is guaranteed by the systems used**, without prejudice, in the event of ascertaining responsibility, to the laws that regulate investigations or measures initiated by the judicial or accounting authority regarding the facts which are the subject of the report.

15. Processing of personal data

Except as indicated in paragraphs 13 and 14 above, all personal data contained in the reports are processed in accordance with the applicable data protection legislation, as set forth in paragraph 4, in full respect of the fundamental rights and freedoms of the data subjects, with particular regard to the confidentiality of their identity and the security of the processing.

The personal data (name, surname, position held, etc.) processed for the management of reports under this procedure relate to the whistleblower, where the report is named, the person involved, and any other persons named in the report. Any additional information collected during the investigation that is necessary and adequate to ascertain and verify the validity or otherwise of the report is also processed. In any case, the identity of the whistleblower and any other information from which such identity may be directly or indirectly deduced may not be disclosed to persons other than those authorized to receive and process reports, without the express consent of the whistleblower.

Personal data that are clearly not useful for processing a specific complaint are not collected or, if collected accidentally, are deleted immediately.

For more detailed information regarding the processing of personal data, please refer to the relevant privacy policy published on the company intranet and website.

16. Data retention period

The data will be retained for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure (reaching the "Closed" status, as shown in Figure 1 above).

17. Reporting

To monitor the functioning of the entire whistleblowing system, the web portal allows for the issuance of periodic reports containing statistics on the reports received and processed. The information contained in the reports is presented in aggregate form and, in any case, anonymized.

The reports are addressed to the Supervisory Body, in accordance with the provisions of the Organization, Management and Control Model pursuant to Legislative Decree 231/01.

18. Training and information

The staff responsible for managing reports (Ethics Committee) has the necessary skills to ensure that reports are handled appropriately and in compliance with applicable provisions.

To this end, they receive periodic training regarding this procedure, the regulatory aspects, and the obligations of the staff entrusted with managing the reporting channel and in the area of Data Protection . The training also covers the general principles of conduct that staff must adhere to in the reporting process, such as confidentiality and privacy, ethics, integrity, transparency, and a willingness to listen and collaborate. Training is particularly required in the event of regulatory updates regarding relevant and applicable provisions relating to the management of reporting channels.

The Company also provides adequate training to all staff on whistleblowing matters so that they are aware of the purposes and methods of managing reports.

The Company provides the whistleblower with clear information regarding the channel, procedures and prerequisites for making reports by publishing this procedure both on the company intranet and on its institutional website where the IT platform for the notification and management of reports is implemented.

19. Attachment

Work-related breach reporting form (Ref.: Italtel Whistleblowing Procedure)	
<i>Name of the whistleblower</i>	
<i>Position of the whistleblower</i>	
<i>Type of reported breach</i>	Breach of laws ☐
	Breach of Model 231 ☐
	Breach of the Italtel Code of Ethics ☐
	Breach of internal provisions or procedures ☐
	Other ☐ • specify ----- -----
<i>Description of report (including places and dates)</i>	----- ----- ----- ----- ----- ----- ----- ----- -----
<i>Name and position of the person who set the reported facts</i>	----- -----
<i>Possible names of other persons who can report on the facts</i>	----- -----
<i>Further information that can be used to check facts</i>	----- ----- ----- -----