WHISTLEBLOWING
-
Procedure for the Management of Reports

Services involved:	All Recipients of the Model
Approved by:	Chief Executive Officer (with subsequent ratification by the Board of Directors)

Revisione

n.	Data decorrenza	Oggetto	Effettuata da:
0	24.02.2020	First version of the document	-
1	15.04.2020	Second version of the document	-
2	17.11.2025	Third version of the document	-

INDEX

1. Definitions

In this document, the following terms have the meanings indicated below:

"Activities at risk of offence": the process, transaction, act, or the set of operations and acts that may expose the Company to sanctions under the Decree as a result of the commission of an Offence.

"CCNL": the National Collective Labour Agreement applicable to employees.

"Code of Ethics": the document officially adopted and approved by the Company's top management as an expression of corporate policy, containing general principles of conduct — i.e., recommendations, obligations and/or prohibitions — that Recipients must comply with, and whose breach is subject to sanctions.

"Work context": current or past work or professional activities carried out within the relationships referred to in Article 3, paragraphs 3 or 4 of Legislative Decree 24/2023, through which, regardless of the nature of such activities, a person acquires information on violations and may risk retaliation in the event of reporting or filing a complaint with judicial or accounting authorities.

"Legislative Decree 231/2001" or **"Decree"**: Legislative Decree no. 231 of 8 June 2001, "Regulation of the administrative liability of legal persons, companies and associations including those without legal personality, pursuant to Article 11 of Law 300/2000", published in the Official Gazette no. 140 of 19 June 2001, and subsequent amendments and integrations.

"Recipients": Corporate Bodies (Board of Directors, Statutory Auditor), Employees, Suppliers and all persons acting in the interest or to the advantage of the Company, with or without representation and regardless of the nature and type of relationship with the Company. Recipients must comply with the Model, the Code of Ethics and the preventive Protocols.

"Employees": all natural persons who have an employment relationship with the Company.

"Facilitator": a person who assists a Reporting Person in the reporting process, operating within the same work context and whose assistance must remain confidential.

"Information on violations": information, including reasonable suspicions, concerning violations committed or which, based on concrete elements, may be committed in the organisation with which the Reporting Person or the person submitting a complaint to judicial or accounting authorities has a legal relationship under Article 3, paragraphs 1 or 2 of Legislative Decree 24/2023 (public sector or private sector), as well as elements related to conduct aimed at concealing such violations.

"Guidelines": the Guidelines for the creation of organisation, management and control models under Legislative Decree 231/2001, published by industry associations, which were taken into account in preparing and adopting the Model.

"Organisation, Management and Control Model pursuant to Legislative Decree 231/2001" or **"Model"**: the organisation, management and control model deemed suitable by the Corporate Bodies to prevent Offences and therefore adopted by the Company pursuant to Articles 6 and 7 of the Decree, to prevent the commission of Offences by top management or subordinate personnel, as described in this document and its annexes.

"Corporate Bodies": the Board of Directors and/or the Statutory Auditor of the Company, depending on context.

"Supervisory Body" (OdV): the body established under Article 6 of the Decree, responsible for supervising the functioning and compliance of the organisation, management and control model, as well as its updating.

"Personnel": all natural persons who have a working relationship with the Company, including employees, temporary workers, collaborators, interns, volunteers and self-employed professionals assigned tasks by the Company.

"Top Management": persons referred to in Article 5, paragraph 1, letter a) of the Decree, namely those with functions of representation, administration or management of the Company; specifically, the Chair, Directors, any general managers or attorneys of the Company, and operating partners performing managerial activities.

"Personnel subject to the direction of others": persons referred to in Article 5, paragraph 1, letter b) of the Decree, i.e. all Personnel operating under the direction or supervision of Top Management.

"Reporting Person": the natural person who submits a report or discloses information on violations acquired within their work context.

"Person concerned": the natural or legal person mentioned in the internal report as responsible for or involved in the reported violation.

"Public Administration" (P.A.): refers to:

- The State (or State Administration);
- Public Entities: defined by law or entities subject to public controls, State or administrative interference in appointing or revoking administrators, and administrative management. They may be characterised by State participation in operating costs, directive powers, public funding or public initiative in their formation.
  Examples (non-exhaustive): Ferrovie dello Stato, Autostrade S.p.A., AEM Milano.

"Public Official": one who performs a public legislative, judicial or administrative function (Art. 357 Italian Criminal Code).

"Person in Charge of a Public Service": one who, in any capacity, performs a public service, defined as an activity governed similarly to a public function but without the authoritative powers typical of the latter (Art. 358 Italian Criminal Code). This applies even without formal appointment ("de facto" officials).

"Protocol": the organisational, physical and/or logical measure provided within the Model to prevent the risk of Offences being committed.

"Offences": all offences referred to by Legislative Decree 231/2001, including future amendments.

"Retaliation": any conduct, act or omission, even only attempted or threatened, carried out as a consequence of a report or complaint, causing or potentially causing unjust harm to the Reporting Person or complainant.

"Report": the written or oral communication of information on Violations pursuant to Legislative Decree 24/2023.

"Internal Report": the written or oral communication of information on Violations submitted through the Company's internal reporting channel pursuant to Legislative Decree 24/2023.

"Follow-up": the action taken by the person responsible for managing the reporting channel to assess the validity of the reported facts, the outcome of investigations and any resulting measures.

"Disciplinary System": the set of sanctions applicable when a reported Violation is found to be substantiated.

"Company": TEF Bridge s.r.l.

"Violations": conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity and which consist of:

- unlawful conduct under Legislative Decree 231/2001;
- violations of the Model, Code of Ethics or preventive Protocols that may generate sanction risk for the Company.

2. Introduction

The Company has aligned its corporate policy with the principles of legality and fairness contained in the Code of Ethics, clearly expressing its repudiation of improper or unlawful conduct or policies. This policy is implemented through the Organisation, Management and Control Model adopted pursuant to Articles 6 and 7 of Legislative Decree 231/2001 for the purpose of preventing the risk of offences.

All Recipients of the Model are required to report any Violations that harm the public interest or the integrity of the public administration or the private entity, within the scope of Violations covered by this Procedure, and of which they become aware through their Work Context.

Such Reports must be as detailed as possible, submitted in good faith, and based on a reasonable belief grounded in precise and consistent factual elements.

This Procedure represents the Company's internal implementation of the regulatory provisions on the protection of persons who report Violations pursuant to Legislative Decree 24/2023. This regulation serves as the primary reference for all activities described herein.

3. Purpose

The purpose of this Procedure is to regulate the process for handling Reports of Violations pursuant to Legislative Decree 24/2023, through methods designed to ensure the confidentiality of the identity of the Reporting Person.
Through this Procedure, the Company defines:

- its internal model for receiving and managing Reports;
- the internal reporting channel;
- the technical and organisational measures designed to ensure an adequate level of security in relation to the specific risks arising from the processing of personal data handled during the management of Reports,

in full compliance with Regulation (EU) 2016/679 and Article 18 of Legislative Decree 51/2018.

4. Reports covered by this Procedure

This Procedure covers Reports relating to the Violations identified in Article 2 of Legislative Decree 24/2023, including:

- unlawful conduct relevant pursuant to Legislative Decree 231/2001;
- violations of the Organisation and Management Model adopted by the Company under the same Decree, **excluding those falling under points 2), 3), 4) and 5)** of the law.

Reports may concern:

- information, including reasonable suspicions, regarding Violations already committed;
- information, including reasonable suspicions, regarding Violations which, based on concrete elements, may be committed;
- elements relating to conduct aimed at concealing such Violations.

Examples of conduct falling under item (1) include, without limitation:

- unlawful acts relevant under Legislative Decree 231/2001;
- violations of the Model, the Code of Ethics, or preventive Protocols that may give rise to sanction risk for the Company;
- suspected violations of the Model, Code of Ethics, or preventive Protocols involving sanction risk;
- business or corporate transactions suspected of involving sanction risk for the Company.

5. Scope of Application

This document applies to the Recipients identified in Chapter “1. Definitions”.
The process for managing Reports described herein **does not apply** to:

- communications of a commercial nature;
- information of a merely defamatory or misleading nature not related to Violations under Legislative Decree 24/2023.

This Procedure **does not apply** to disputes, claims or requests related to the personal interest of:

- the Reporting Person, or
- the person who filed a complaint with judicial or accounting authorities,

where such interest concerns exclusively:

- **their individual employment relationship**, or
- their relationship with hierarchical superiors.

As a general rule, the Company encourages employees to resolve internal workplace disputes — where possible — through dialogue, including informal dialogue, with colleagues and/or their direct supervisor.

5.1 Corporate Perimeter

This Procedure applies to all Recipients identified in Chapter 1.

6. Process for Handling Reports

6.1 Reporting Channels

6.1.1 Internal Reporting

Pursuant to law, the Company has activated an internal reporting channel under Legislative Decree 24/2023, which guarantees the **confidentiality** of:

- the identity of the Reporting Person,
- the identity of the Person concerned,
- the identity of any person mentioned in the Report,
- the content of the Report and its related documentation.

The management of this channel is entrusted to the **Supervisory Body (SB / OdV)**.
The member of the Supervisory Body has been duly authorised by the Company to process personal data contained in internal Reports.
If a Report concerns the Supervisory Body member, reference must be made to Chapter 11 "Special Cases".
Reports may be submitted through the following methods:

• Written form – Digital submission (PEC)
Via certified email (PEC) to the following address:
whistleblowing.tefbridge@legalmail.it

• Written form – Postal submission
By ordinary mail, addressed to:
TEF Bridge s.r.l.
Via Giovanni Durando 39
20158, Milan – Italy
Submitted as follows:

1. The documentation relating to the Report is placed in a **sealed envelope**.
2. A second sealed envelope contains the Reporting Person's identifying information.
3. Both envelopes are placed inside a **third sealed envelope** labelled: **"confidential – for the attention of the SB (OdV)"**

• Oral form – Meeting with the Supervisory Body
A direct meeting may be requested with the Supervisory Body within a reasonable timeframe.
With the **consent of the Reporting Person**, the Report may be documented by the authorised staff:

- through an audio recording device suitable for storage and playback, or
- through detailed minutes.

In the case of written minutes, the Reporting Person may:

- verify
- correct
- approve

the content through their signature.

(For additional details, see paragraph **6.2**.)

6.2 Submission of the Internal Report

Anyone wishing to submit a written internal Report may do so by attaching the specific form provided in **Annex 1**.
The Form provides the Reporting Person with a **guided structure**, consisting of:

- questions,
- requests for supporting information,
- prompts designed to ensure a **clear, precise and detailed** description of the facts being reported.

Reports must be based on **precise and consistent factual elements**. The Reporting Person is encouraged to attach **all documentation** supporting the facts, and must refrain from carrying out any **independent investigations**.

6.3 Receipt and Analysis of the Internal Report

Internal Reports are handled by the **Supervisory Body (SB / OdV)**, which processes them confidentially and applies appropriate verification methods to safeguard:

- the identity of the Reporting Person, and
- the identity of any Persons concerned.

Preliminary Verification

All internal Reports received are subjected to a **preliminary verification** by the Supervisory Body in order to determine whether:

- the Report includes the information required to assess its initial credibility;
- there is sufficient detail to allow appropriate follow-up actions.

The SB undertakes to provide the Reporting Person with an **acknowledgement of receipt within 7 days** of receiving the internal Report.
The SB diligently follows up on the Reports and may request further information from the Reporting Person where necessary.
Without prejudice to confidentiality obligations, the SB may — during preliminary verification — rely on:

- other internal Company departments, or
- external specialised consultants,

if their expertise is required given the nature of the Report.

Reports that may be closed after preliminary verification

The SB may close a Report during the preliminary verification phase if it is:

- **not sufficiently detailed**;
- **lacking sufficient information** to allow further investigation;
- **manifestly unfounded**.

Verification and Investigation Phase

During the verification and investigation phase, the SB:

- ensures **impartiality, fairness and accuracy** in the analysis;

- ensures confidentiality of all information collected;
- protects the identity of the Reporting Person (where provided);
- undertakes **not to use information beyond what is strictly necessary** for handling the Report.

The SB **cannot disclose** the identity of the Reporting Person — or any information from which their identity could be directly or indirectly inferred — without their **express written consent**, except to persons:

- authorised to receive or follow up Reports,
- expressly authorised to process such data under GDPR Articles 29 and 32(4) and under Article 2-quaterdecies of the Italian Data Protection Code.

Reports that do NOT pass the preliminary verification

Reports closed at this stage are:

- archived by the SB in a **dedicated encrypted logical repository**, accessible only to the SB member;
- recorded in the **periodic reporting**.

The SB must also record:

- the Report,
- the actions taken in response,

inside the **Register of Reports and Investigations**, always protecting:

- the identity of the Reporting Person,
- the identity of all Persons concerned.

The Register is kept exclusively by the SB and is only accessible to authorised individuals.

Reports that DO pass the preliminary verification

If the SB determines that the internal Report:

- is properly detailed,
- includes adequate supporting evidence, and
- concerns conduct that may be actionable (even only from a disciplinary perspective),

the SB shall:

1. Immediately inform the functions/bodies responsible for applying the disciplinary and sanctions system

These functions must autonomously evaluate:

- whether disciplinary action is appropriate,
- the type and severity of action to be taken,
- compliance with legal requirements, including
  - specificity of charges,
  - timeliness,
  - consistency.

They may carry out further investigations, requesting support from the SB.

The SB remains the **only point of contact** for the Reporting Person and continues to guarantee anonymity.

2. Possible outcomes of further investigations
If the competent functions:
a) Consider the conduct NOT sanctionable
They must immediately inform the SB, which will:
- archive the Report according to procedures, and
- inform the Reporting Person of the outcome.

b) Decide to proceed with disciplinary action
They must ensure that the Person concerned receives:
- **privacy information** pursuant to Article 14 GDPR,
- within **one month** from the start of processing.

3. Inform the Management or Control Body
The SB must notify the relevant corporate body for evaluations within its remit.

4. Final Report
At the end of the investigation, the SB prepares a **final report**, addressed to:
- the function responsible for disciplinary action, and/or
- the function responsible for corrective measures to prevent future occurrences.

This is in line with Article 7(4) of Legislative Decree 231/2001.

Follow-up deadlines
The SB must process Reports within a **reasonable period** and provide a follow-up response to the Reporting Person:
- **within 3 months** from the acknowledgment of receipt, or
- if no receipt was given, **within 3 months** from the expiry of the 7-day deadline following submission.

7. Sanctions and Disciplinary System
7.1 Activation of the Sanctions and Disciplinary System
When, based on the investigations carried out, the Violations forming the subject of the internal Report are found to be **substantiated**, the corporate body or function responsible for activating the sanctions system determines **which type of sanction** should be applied to the individuals who committed the violation.
Depending on the role and legal classification of the Person concerned, the Disciplinary System is activated by:
- **Chief Executive Officer (CEO)** – if the reported person is an employee or manager of the Company;
- **Board of Directors** – if the reported person is the Statutory Auditor;
- **Statutory Auditor** – if the reported person is a Director;
- **Board of Directors** – if the reported person is the member of the Supervisory Body;
- **Chief Executive Officer (CEO)** – if the reported person is an external third party.

Sanctions are determined considering:

- the seriousness of the violation,
- compliance with applicable laws (e.g., labour law when applied to Company employees).

Reporting Person also responsible for the Violation

If the Reporting Person is **jointly responsible**, they may receive **more favourable treatment**, to the extent compatible with:
- the violation committed,
- applicable legislation.

Confidentiality of the Reporting Person's Identity

The identity of the Reporting Person — and any information from which their identity may be directly or indirectly inferred — **may not be disclosed** without their **express written consent**.
This consent must be:
- free
- specific
- unambiguous
- informed

and must be archived by the Supervisory Body.

Confidentiality in disciplinary proceedings

If:
- the disciplinary charge is based on **elements other than** the Report
  → The identity of the Reporting Person **must NOT be disclosed**, even without consent.

If:
- the disciplinary charge is based **fully or partly on the Report**, and
- disclosure of the Reporting Person's identity is **indispensable** for the defence of the Person concerned
  → The SB must inform the Reporting Person **in writing**, explaining:
- why disclosure is necessary
- what information might reveal their identity

If the Reporting Person **denies consent**, the SB must **close the Report with no further action**.

False or malicious Reports

This Procedure does not affect the criminal or disciplinary liability of the Reporting Person in cases of:
- **malicious or defamatory Reports** (criminal code),
- **grossly negligent Reports**,
- abuse of the reporting system.

Improper behaviours include:
- opportunistic Reports aimed solely at harming others,
- intentionally abusive or manipulative use of the reporting channel.

Where the Reporting Person is convicted (even in first instance) for:
- **defamation**,
- **calumny**,
- or civil liability due to intent or gross negligence,

→ **all protections under this Procedure cease**,
→ a **disciplinary sanction** is applied.

8. Protections for the Reporting Person and Application of Safeguards

No form of **Retaliation** against the Reporting Person is allowed.
According to the law, protections also apply to:

- **Facilitators**;
- persons in the same Work context who have a stable emotional or family bond with the Reporting Person (up to the fourth degree);
- colleagues working in the same Work context who have a habitual working relationship with the Reporting Person;
- **entities owned** by the Reporting Person or by the person who filed the judicial or accounting complaint;
- entities operating in the same Work context.

Conditions for protection

Protection applies when, at the moment of reporting:
The Reporting Person:

1. **reasonably believed** the information was true and concerned violations of national/EU law harming the integrity of the private entity;
2. submitted the Report **in compliance with Legislative Decree 24/2023**.

➤ **Motivations behind the Report are irrelevant** for protection purposes.

Protection in case of anonymous reports

Protections also apply when:

- the report was anonymous,
- the Reporting Person was later identified,
- and has suffered retaliation.

They also apply to reports submitted to:

- **EU institutions**,
- **EU bodies**,
- **EU agencies**,
- in accordance with Article 6 of Legislative Decree 24/2023.

Protection against discriminatory measures

Any discriminatory measures against Reporting Persons may be reported to **ANAC**. ANAC may then notify the **National Labour Inspectorate**.
Acts taken in violation of the prohibition of Retaliation are **null and void**.
A Reporting Person dismissed due to a Report has the **right to reinstatement**.

Burden of proof

In judicial, administrative or extrajudicial proceedings regarding retaliatory acts:

- it is **presumed** that the detrimental act was motivated by the Report or complaint;
- the burden of proving otherwise lies with the **employer or responsible party**.

If the Reporting Person files for damages and can demonstrate:

- they submitted a Report or complaint, and

- suffered damage,

→ It is presumed (unless proven otherwise) that the damage resulted from the Report/complaint.

8.1 Limitations of Liability

The Reporting Person **is not punishable** for disclosing or disseminating information covered by confidentiality obligations (except for state secrecy under Article 1(3) of the Decree), or information concerning:

- copyright,
- personal data protection,
- the reputation of the Person concerned, when:
- the Reporting Person had reasonable grounds to believe disclosure was necessary to expose a violation, and
- acted in accordance with Legislative Decree 24/2023.

In such cases:

- **civil or administrative liability is also excluded**.

The Company and the Reporting Person are not liable — even civilly or administratively — for acquiring or accessing information on Violations, provided the conduct is not a separate offence.
However, liability is **not excluded** for:

- conduct unrelated to the Report,
- conduct not strictly necessary to reveal the violation.

9. Retention and Archiving

The Supervisory Body (SB) is informed of any sanctions imposed following internal or external Reports.
The Company's competent functions **retain and archive** the documentation related to the disciplinary and sanctions process.
The SB archives all documentation relating to:

- the Report submitted through the IT channel, and
- the subsequent investigation,

within a **dedicated encrypted logical space**, accessible only to the SB member and designed to ensure the confidentiality of the Reporting Person.
Any paper documentation — as well as the **Register of Reports and Investigations** kept by the SB — must be stored by the SB and made accessible exclusively to individuals authorised by the Company.
Internal Reports are retained:

- **for the time strictly necessary** for processing, and
- **in any case no longer than five years** from the date of notification of the final outcome of the procedure,

in compliance with:

- Article 12 of Legislative Decree 24/2023 (confidentiality obligations),
- Article 5(1)(e) GDPR (data minimisation and storage limitation),
- Article 3(1)(e) of Legislative Decree 51/2018.

The SB may maintain a **Register of Reports** in which:

- personal data of the Reporting Person,
- data of Persons concerned,
- data of any other persons involved

are **anonymised**, in order to guarantee evidence of proper management of Reports — a required element of effective implementation of the Model under Article 6 of Legislative Decree 231/2001.

10. Reporting

The Supervisory Body prepares **an annual report** on the proper functioning of the Company's internal reporting system, including:
- aggregated information on the activities carried out,
- statistics and outcomes of Reports received,
- the follow-up provided.

When preparing this report, the SB must comply with:
- rules on the protection of the identity of the Reporting Person;
- applicable legislation on personal data protection.

11. Special Cases

If an internal Report **concerns the member of the Supervisory Body**, the Report must be submitted to the **Board of Directors (BoD)** by delivering all supporting documentation to the Chair of the Board.
The Board of Directors:
1. assesses whether the Report contains the necessary information to make a preliminary evaluation;
2. determines whether to initiate further investigations;
3. carries out the investigation, making use of:
    - Company internal expertise,
    - external specialised consultants (if needed), always ensuring compliance with confidentiality requirements set out by law and in this document.

The investigation follows the same procedure described within this document.
The final decision of the Board of Directors is formalised in a **written resolution.**

WHISTLEBLOWING REPORTING FORM

We recommend attaching any documentation deemed useful to support the Report; if the Report is made verbally, such documentation may be delivered directly.

DATA OF THE REPORTING PERSON

Name and Surname *(non-mandatory data)*

____

Structure and qualifications *(non-mandatory data)* ____

Preferred contact channels (e.g., private email address, telephone number, etc.)

Does the Reporting Person have a personal interest related to the Report? Yes ☐ No ☐

Specify the nature of the private interest connected to the Report

Is the reporting person jointly responsible for the violations he or she reports? Yes ☐ No ☐

OFFENCE REPORTED

Period/Date in which the incident occurred ____

Area of company operations to which the incident may relate ______________________________________

Parties involved:

Interni	Esterni

Description of the fact being reported

Other subjects who can report on the facts that are the subject of the Report.

Inside TEF Bridge s.r.l.	
Outside TEF Bridge s.r.l.	

Other parties to whom the Report of the Incident was forwarded? Yes ☐ No ☐

Specify which parties and when

Date Signature *(non-mandatory data)*

ANNEX 2 - PRIVACY NOTICE – REPORTING PERSON

Pursuant to Article 13 of Regulation (EU) 2016/679 relating to the processing of personal data in connection with reporting violations under Legislative Decree 24/2023

Pursuant to Article 13 of Regulation (EU) 2016/679 ("GDPR") and the applicable legislation on personal data protection, we inform you that the personal data provided in your capacity as Reporting Person ("Data Subject") through this "Reporting Form", or otherwise provided in connection with an internal report under Legislative Decree 24/2023, will be processed in compliance with applicable law and according to principles of fairness, lawfulness and transparency, by staff authorised by TEF Bridge s.r.l., pursuant to Article 29 GDPR and Article 2-quaterdecies of the Italian Data Protection Code (Legislative Decree 196/2003).

Data Controller

The Data Controller is **TEF Bridge s.r.l.**,
Via Giovanni Durando 39, 20158 Milan, Italy.

Purpose of Processing and Legal Basis

Personal data are processed for managing internal reports of alleged violations—i.e., conduct, acts or omissions harming the public interest or the integrity of the public administration or private entity, as defined by Article 2(1)(a) of Legislative Decree 24/2023—of which the Reporting Person becomes aware by virtue of their work relationship with the Controller.
Data processed include:

- personal data contained in the internal Report,
- documents attached to the Report,
- and any data necessary for investigative activities to verify the Report.

Where required, data may also be processed to initiate corrective actions, disciplinary actions or legal proceedings.
The legal basis is compliance with a **legal obligation** (Article 6(1)(c) GDPR), including Legislative Decree 165/2001, Legislative Decree 231/2001, Law 179/2017 and Legislative Decree 24/2023.
Processing may include:

- special categories of data (Article 9 GDPR),
- data relating to criminal convictions or offences (Article 10 GDPR),
- if included in the Report.

Recipients of Personal Data

Personal data will be processed by:

- the member of the Supervisory Body (authorised by the Controller) to manage and respond to Reports in compliance with the Decree and the Model;
- external service providers appointed as **Data Processors** under Article 28 GDPR (if the Company outsources the management of the reporting channel).

Data:

- will **not be disseminated**;
- may be transmitted to the **Judicial Authority**;
- will **not be transferred outside the EEA**.

If the Report is submitted externally to **ANAC**, ANAC will provide its own privacy notice.

Retention Criteria

Internal Reports and related documentation are retained:

- for the time necessary to manage the Report, and

- in any case **no longer than five years** from the communication of the final outcome,

in compliance with:

- confidentiality obligations (Art. 12 of Legislative Decree 24/2023),
- Article 5(1)(e) GDPR,
- Article 3(1)(e) Legislative Decree 51/2018.

After five years, data may be retained **only in anonymised form** for purposes of defence and proof of proper handling of Reports.

Processing Methods

Processing is performed only by **authorised personnel**, using methods ensuring:

- confidentiality of the Reporting Person's identity,
- security of documents and information,
- protection from unauthorised access, destruction or loss.

The Reporting Person's identity:

- is known **only to authorised individuals**,
- may not be disclosed **without express consent**, except where required by law (e.g. criminal proceedings).

Provision of Data

Providing personal data is **optional**.
However, failure to provide data may hinder the investigation:
anonymous reports are considered **only if sufficiently detailed**.

Rights of the Data Subject

The Data Subject may exercise the rights under Articles 15–22 GDPR, **within the limits** of Article 2-undecies(3) of the Italian Privacy Code.
Rights **may not be exercised** if doing so would compromise:

- the confidentiality of the identity of the Reporting Person, or
- ongoing investigations.

In such cases, rights may be exercised **via the Italian Data Protection Authority (Garante)**.
If the Data Subject believes their data are processed unlawfully, they may lodge a complaint with the Garante (Art. 77 GDPR) or bring proceedings before the competent courts (Art. 79 GDPR).