Rev.	Date	Change description
00	02/08/2024	First Issue

HANDLING OF REPORTS OF MISCONDUCT OR IRREGULARITIES

TABLE OF CONTENTS

1. PREAMBLE - PURPOSE OF THE PROCEDURE 2
2. REGULATORY REFERENCES 2
3. DEFINITIONS 3
4. RECIPIENTS 4
Why report? 5
When is it time to report? 5
5. SCOPE OF APPLICATION 5
What are the main conducts reported? 6
6. REPORT 6
7. NECESSARY ELEMENTS OF THE REPORT 6
8. RECIPIENTS AND INTERNAL CHANNELS OF WHISTLEBLOWING REPORTS 7
Written reports 7
Oral reports 7
9. RECIPIENTS AND INTERNAL CHANNELS OF WHISTLEBLOWING REPORTS 8
10. USE OF THE PLATFORM 8
11. INTERNAL REPORT MANAGEMENT 8
12. PERSONAL DATA PROCESSING AND RECORD KEEPING 8
13. RIGHTS OF THE DATA SUBJECT 9
14. PROTECTIVE MEASURES 9
To whom the protective measures apply: 9
15. POSSIBILITY OF ANONYMITY 10
16. RESPONSIBILITIES OF THE WHISTLEBLOWER 10
17. PROTECTION OF THE REPORTED PERSON 10
18. RESTRICTION OF LIABILITY 10
19. INFORMATION AND TRAINING 11
20. MODES OF OPERATION 11
Phase 1: Report Submission and Registration 11
Phase 2: Evaluation of the Admissibility of the Report 11
Phase 3: Assessment of the Merits of the Report 11
Phase 4: Sharing of Findings 12
Phase 5 Keeping the Data Contained in the Report. 12

1. PREAMBLE - PURPOSE OF THE PROCEDURE

The purpose of this procedure is to regulate a system of whistleblowing within the scope of the Organisation's activities. In particular, the procedure implements the provisions of Legislative Decree No. 24 of March 10, 2023 (the "Whistleblowing Decree") - implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 - which regulates the protection of persons who report violations of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private employment context. The purpose of the directive is to regulate the protection of whistleblowers within the Union, through minimum standards of protection, aimed at standardising national laws. Whistleblowing is an institution that was first introduced in Italy in 2012 concerning the public sector only and was later partially extended to the private sector by Law 179/2017. The Legislative Decree 24/2023, by repealing the previous provisions on whistleblowing, intends to strengthen the principles of transparency and accountability in the area of whistleblowing. It also intends to prevent the commission of offences, by bringing together in a single regulatory text and an organic manner the entire discipline of whistleblowing channels and the protections afforded to whistleblowers in both the public and private sectors.
The procedure governs all stages of the process: from the making of the report to its receipt by the addressees, its analysis, processing and decision on the report, guaranteeing the confidentiality of the reporter (and of the reported person) and his or her safety from possible retaliatory and/or discriminatory actions resulting from the report.

2. REGULATORY REFERENCES

Legislative Decree 24/2023	Legislative Decree No. 24 of March 10, 2023
Law 179/ 17	Law No. 179 of November 30, 2017
Law 127/ 22	Law No. 127 of August 4, 2022
Directive (EU) 2019/1937	Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019
Legislative Decree 231/2001	Legislative Decree No. 231 of June 8, 2001
Law 190/2012	Law No. 190 of November 6, 2012 - Provisions for the prevention and repression of corruption and illegality in the Public Administration
Legislative Decree 165/2001	General rules on the organisation of employment in public administrations
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals concerning the processing of personal data and on the free movement of such data
Privacy Code	Legislative Decree No. 196 of June 30, 2003, as amended by Legislative Decree No. 101 of August 10, 2018
ANAC Guidelines	Guidelines on the protection of persons who report breaches of Union law and protection of persons who report breaches of national law. Approved by Resolution No. 311 of July 12, 2023

3. DEFINITIONS

- **Violations**: conduct, acts or omissions that harm the public interest or the integrity of the public administration or private entity.
- **Information on breaches**: information, including well-founded suspicions, concerning breaches committed or which, based on concrete elements, could be committed in the organisation with which the reporting person or the person complaining with the judicial or accounting authorities has a legal relationship within the meaning of Article 3(1) or (2) of Legislative Decree No. 24/2023, as well as elements concerning conduct aimed at concealing such breaches.
- **Reporting or flagging**: the written or oral communication of information on violations.
- **Anonymous reporting**: Reports that do not contain details that allow or could allow, even indirectly, the identification of the reporting party.
- **Internal reporting**: the communication, written or oral, of information on violations, submitted through the internal reporting channel.
- **External reporting**: the communication, written or oral, of information on violations, submitted through the external reporting channel.
- **Public disclosure or public dissemination**: making information about violations publicly available through print or electronic media or otherwise through means of dissemination capable of reaching a large number of people.
- **Whistleblower**: the natural person making the report or public disclosure of information about violations acquired in the context of his/her work.
- **Facilitator**: a natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential.
- **Recipient of the report**: the natural person or body designated to receive the report and to know the identity of the reporting person. An absolute obligation of confidentiality tout court.
- **Work context**: the work or professional activities, present or past, carried out in the context of the relationships referred to in Article 3(3) or (4) of Legislative Decree No. 24/2023, through which, regardless of the nature of such activities, a person acquires information about violations and in the context of which he/she could risk suffering retaliation in the event of a public disclosure or report to the judicial or accounting authorities.
- **Person involved or reported**: the natural or legal person mentioned in the internal or external report or the public disclosure as the person to whom the violation is attributed or as a person otherwise implicated in the reported or publicly disclosed violation.
- **Retaliation**: any conduct, act or omission, even if only attempted or threatened, occurring as a result of the report, judicial or accounting authority report or public disclosure and which causes or may cause the reporting person or the person making the report, directly or indirectly, unjust damage.
- **Organisation, Management and Control Model (Model 231)**: the organisation and management model (or model under Legislative Decree no. 231/2001), under Italian law, indicates an organisational model adopted by a legal entity, or association without legal personality, aimed at preventing the criminal liability of entities. It normally consists of a General Section and a Special Section drawn up on a case-by-case basis following the mapping of activities at risk of offences.
- **Receiver**: Internal person who receives the report and processes it in compliance with the indications and precautions defined in this document.
- **Supervisory Board**: the person formally appointed to manage the whistleblowing channel.

4. RECIPIENTS

This procedure applies to all persons who report, denounce to the judicial or accounting authorities, or publicly disclose information on violations of which they have become aware in the context of their work, and in particular to:

- employees, self-employed workers, and holders of collaborative relationships with the organisation;
- freelancers and consultants;
- volunteers and trainees, paid and unpaid;
- any shareholders (natural persons) and persons with administrative, management, control, supervisory or representative functions, even if such functions are exercised on a de facto basis;
- contractors and suppliers.

Employees are defined as:

- Workers whose employment relationship is governed by Legislative Decree No. 81/2015. These are, for example, part-time, intermittent, fixed-term, temporary, apprenticeship and ancillary employment relationships;
- Workers performing occasional services (whose employment relationship is governed by Article 54-bis of Decree-Law No. 50/2017, converted with amendments and additions by Law No. 96/2017).

Self-employed workers:

- Self-employed workers referred to in Chapter I of Law No. 81/2017. These are workers with self-employment relationships governed by Title III of Book V of the Civil Code, including the work contracts referred to in Article 2222 of the same Civil Code;
- holders of a cooperation relationship under Article 409 of the Code of Civil Procedure. This refers to the relationships indicated in No. 3 of the aforementioned provision, i.e. agency, sales representation and other collaboration relationships resulting in the provision of continuous and coordinated work, mainly of a personal nature, even if not of a subordinate nature. For example, lawyers, engineers, and social workers who work for a private sector entity by organising it independently (para-subordinate relationship);
- holders of a collaboration relationship referred to in Article 2 of Legislative Decree No. 81/2015. This is - under par. 1 of the aforementioned provisions - of collaborations organised by the principal that takes the form of exclusively personal and continuous work, the manner of performance of which is organised by the principal. This also applies if the manner of performance is realised through digital platforms.

The protections also apply to the following persons:

- Freelancers and consultants working in the private sector who may be in a privileged position to report violations they witness.
- Volunteers and trainees, paid and unpaid, working for private sector entities who may still face retaliation for reporting violations. Retaliation against these individuals could take the form of, for instance, no longer using their services, giving them negative work references, or otherwise damaging their reputation or career prospects.
- Shareholders and natural persons holding shares in one of the private sector entities, where the latter takes on a corporate form. Those have become aware of reported violations in the exercise of their rights as shareholders in the organisation.
- Persons with functions of administration, management, control, supervision or representation, even where such functions are exercised on a de facto basis in private sector entities. These are persons connected in a broad sense to the organisation where the violation occurs and where they exercise certain functions, even in the absence of a regular investiture (de facto exercise of functions). These may be, for instance, members of boards of directors, even without executive positions, or members of supervisory bodies (SBs).

The protections provided for the whistleblower also apply if the report, the complaint to the judicial or accounting authorities or the public disclosure of information takes place in the following cases:

- when the legal relationship has not yet begun if information on violations was acquired during the selection process or at other pre-contractual stages;
- during the probationary period;
- after the termination of the legal relationship if the information on violations was acquired in the course of that relationship.

Why report?

Reporting is needed to investigate potential unlawful and unethical conduct, to identify risks at an early stage and to prevent damage to Thema S.r.l.'s reputation. In this way, reporting can help minimise risks, for the working environment and all employees. Each report contributes to the success of Thema S.r.l. and the promotion of an ethical, healthy and sustainable culture, offering an important contribution to the internal compliance control system.

If, as an employee or collaborator of Thema S.r.l., as a customer, supplier, business partner or because of any other relationship with Thema S.r.l., you become aware of actions or conduct that are, or could appear to be, not in line with the values of Thema S.r.l., not appropriate, fair, lawful or that could endanger Thema S.r.l., the working environment and all employees.

When is it time to report?

If you are not sure how to act, ask yourself a few questions such as:

- Could the conduct have been carried out in contravention of rules of ethics and conduct, procedures, protocols or provisions contained in the Model or Code of Ethics?
- Could the conduct have been in breach of laws and/or regulations applicable to Thema S.r.l.?
- Could the conduct constitute a criminal offence (e.g. bribery, environmental offences, occupational health and safety offences)?
- Could reporting prevent negative consequences for Thema S.r.l.?

5. SCOPE OF APPLICATION

Thema S.r.l. has adopted Model 231, therefore, the violations that may be reported under the Whistleblowing Decree must relate to conduct, acts or omissions that harm the public interest or the integrity of the public administration or entity of which the Whistleblower has become aware in the context of his or her work and which consist of:

- unlawful conduct relevant to the regulation 231;
- Dissemination of model 231.

The report may also relate to:

- information on conduct aimed at concealing the above violations;
- unlawful activities that have not yet taken place but which the whistleblower reasonably believes may take place in the presence of concrete, precise and concordant elements;
- well-founded suspicions, which must in any case be based on good faith and not on mere suspicions or the sole basis of unreliable indiscretions or rumours.

In particular, violations may concern:

- the predicate offences for the application of Legislative Decree No. 231/2001;
- violations of the organisation and management models provided for in the aforementioned Legislative Decree No. 231/2001

The following cannot be reported:

- disputes, claims or requests linked to an interest of a personal nature of the person making the report that relate exclusively to his or her work or public employment relationship, or inherent to his or her work or public employment relationship with hierarchically superior figures (e.g. reports concerning labour disputes, discrimination between colleagues, interpersonal conflicts between the person making the report and another worker);
- violations where they are already mandatorily regulated by EU or national acts (e.g. the market abuse reporting procedures set out in Regulation (EU) No. 596/2014 of the European Parliament and the Council to Commission Implementing Directive (EU) 2015/2392 adopted based on the aforementioned Regulation, which already contains detailed provisions on whistleblower protection);
- national security breaches, as well as contracts relating to defence or national security aspects, unless the relevant secondary law of the European Union covers these aspects.

What are the main conducts reported?

By way of example:

- Corruption and fraud
- Embezzlement and theft
- Money laundering
- Health, safety and environmental violations
- Discrimination, harassment, mobbing and other labour law issues
- Personal Data Protection (Privacy) and IT security breaches
- Violation of tax regulations
- Breaches of competition law (Antitrust)
- Disclosure of business secrets.

6. REPORT

This procedure, by current legislation, provides for and describes the following internal reporting channels:

- written communication;
- oral communication.

7. NECESSARY ELEMENTS OF THE REPORT

The report must be as detailed as possible to allow the assessment of the facts by the persons competent to receive and handle reports. In particular, you must clarify:

- the circumstances of time and place in which the event reported occurred;
- a full and detailed description of the fact or conduct, including omission, that is the subject of the report and how it came to its knowledge;
- personal details or other elements enabling identification of the person to whom the reported facts can be attributed;
- personal details, the role held or other elements that may allow the identification of the person(s) who has/have carried out the reported fact or behaviour;
- personal details, the role held or other elements that may allow the identification of other persons who may report on the reported fact or behaviour;
- an indication of any other information and/or deed and/or document, however, represented or on whatever medium stored, that may be useful for verifying the validity of the facts reported.

If the reporter wishes to be contacted to be informed of the progress and/or outcome of the procedure, he/she should indicate not only his/her details but also the method of contact (e-mail address or telephone number).

Furthermore, it should be indicated in the report whether:
- the facts that are the subject of the report were learnt personally or were reported to the reporter by a third party;
- the reported facts were also brought to the attention of other corporate functions;
- the reported facts have also been passed on to public bodies or judicial police officers.

It is also useful to attach documents that may provide evidence of the facts being reported, as well as an indication of other persons potentially aware of the facts. It should be noted that even anonymous reports, i.e. lacking any elements allowing their author to be identified, submitted following this procedure, adequately substantiated and accompanied by sufficient elements to allow an adequate investigation, are treated as 'ordinary' reports and will be taken into account.

8. RECIPIENTS AND INTERNAL CHANNELS OF WHISTLEBLOWING REPORTS

The Organisation provides channels for sending internal reports, suitable for guaranteeing the confidentiality of the identity of the Whistleblower, the Facilitator, the Whistleblower or in any case of the persons mentioned in the Report, the content of the report and the relevant documentation.
Specifically, the person in charge of receiving and following up reports is the Supervisory Board.
These individuals were specifically trained on the procedure and investigation to be carried out and informed of the obligations of secrecy, being able to rely exclusively on the support of a core group of persons, who were also suitably trained and informed.
Under the Whistleblowing Decree, the organisation has set up an internal reporting channel that allows for computerised reporting. Internal reports can be made:
- in writing, via computer platform https://whistleblowersoftware.com/secure/THEMA
- orally through the possibility of sending an audio recording, again managed through an IT platform https://whistleblowersoftware.com/secure/THEMA;

Access to the internal reporting channel may only take place by the Report Recipient. The name of the Recipient is made public.

Written reports
Reports in written form are submitted via the 'whistleblower software' IT platform accessible via the link available on the corporate website. The platform uses encryption tools that allow each report received to be identified using a unique code. The reporter must keep this code and use it, in the days following the report, to access the platform and check whether there has been a response or whether further elements have been requested to supplement the report.
Once logged in to the IT platform, the reporter enters preliminary information and a description of the fact. The authorised person treats all data, including the identification data of the reporter, with the necessary confidentiality. Entering personal data, such as name, surname, telephone number, e-mail and job position, is not compulsory and can also be done at a later stage, by resubmitting the report via the code assigned at the end of registration. The reporter may choose whether to report anonymously or by revealing his or her identity.

Oral reports
Oral reports are made through a voice recording on the software provided by the company. At the end of the listening, a report will be signed, which will be kept by the authorised person in a confidential manner and with the application of appropriate security measures.
Verbal or written communications that are not formalised in the manner and content specified in this procedure will not be taken into consideration.

9. RECIPIENTS AND INTERNAL CHANNELS OF WHISTLEBLOWING REPORTS

The Organisation provides channels for sending internal reports, suitable for guaranteeing the confidentiality of the identity of the Whistleblower, the Facilitator, the Whistleblower or in any case of the persons mentioned in the Report, the content of the report and the relevant documentation.
Specifically, Thema S.r.l. has made a platform available to Whistleblowers, managed by an independent party, which has the requirements to ensure that the Internal Reporting Channel meets the legal requirements.

10. USE OF THE PLATFORM

The Internal Reporting Channel adopted allows the reporting person to make reports in written form, following the procedure below. The reporting person, to create a report, accesses the portal via the link made available on the corporate website. Through the platform, the reporter will be guided through each step of the reporting process and will be asked, to better substantiate the report, and to fill in several fields respecting the requirements.
The reporting person may decide whether to send an anonymous report or to provide his or her details. Once this choice has been made, the reporter is asked to provide a detailed description of the facts to be reported (place, time of occurrence, any supporting evidence). Once the fields required as mandatory have been completed, the reporter will send the Report. By registering the report on the Portal, the reporting party will obtain a unique identification code that it can use to check the progress of the report and/or 'interact' with the receiving party. It is therefore important that the unique identification code is properly kept by the reporter, as it can no longer be retrieved and/or duplicated if it is lost.
The organisation also takes into account anonymous reports, where these are adequately substantiated, i.e. they are such as to bring to light facts and situations relating them to specific contexts (e.g.: documentary evidence, indication of names or particular qualifications, mention of specific offices, proceedings or particular events, etc.).

11. INTERNAL REPORT MANAGEMENT

Whistleblowers are obliged to comply with indications that the legislator has laid down to ensure both efficient and timely handling of the report and the protection of the reporting persons:

- issues the reporting person with an acknowledgement of receipt of the report within seven days of its receipt;
- maintains discussions with the reporting person;
- follow up properly on the reports received or provide feedback to the reporting person.

The whistleblower may send a report - either in an identified form or anonymously - through the reported channels (for more information on the procedure for sending reports, see the chapter on Operating Modalities).

12. PERSONAL DATA PROCESSING AND RECORD KEEPING

All processing of personal data is carried out in compliance with the confidentiality obligations set out in Article 12 of Legislative Decree No. 24/2023 and under the personal data protection regulations set out in Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), Legislative Decree No. 196 of June 30, 2003, and Legislative Decree No. 51 of May 18, 2018. Personal data protection is ensured not only for the Reporting Party (for non-anonymous reports) but also for the Facilitator and the Person involved or mentioned in the report.
Information on the processing of personal data is provided to possible interested parties through publication on the dedicated portal.

The entire documentation relating to the Report and any supporting annexes are kept for the time strictly necessary for their definition, and in any case for no longer than 5 years, starting from the date of communication of the outcome of the Report.
Personal data that are not useful for processing a specific alert are not collected or, if accidentally collected, are deleted promptly. Originals of reports received in paper form are stored in a secure environment.

13. RIGHTS OF THE DATA SUBJECT

The person involved or the person mentioned in the report, concerning his or her data processed in the context of the report, public disclosure or complaint, cannot exercise the rights that the EU Data Protection Regulation 679/2016 "GDPR" grants to data subjects (the right of access to personal data, the right to rectification, the right to obtain erasure or so-called right to be forgotten, the right to restriction of processing, the right to portability of personal data and the right to object to processing). This is because the exercise of such rights could result in actual and concrete prejudice to the protection of the confidentiality of the identity of the reporting person. In such cases, the reported person or the person mentioned in the report is also precluded from addressing the data controller and, in the absence of a reply from the latter, from complaining to the Data Protection Supervisor if they consider that the processing operations concerning them violate their rights.

14. PROTECTIVE MEASURES

Reports must be made in good faith and are without prejudice to the criminal liability of the Whistleblower should a Report constitute an offence of slander, defamation, or other offence and without prejudice to the cases of non-punishability referred to in the Whistleblowing Decree.
The Whistleblowing Decree provides for the following protection measures for the Whistleblower and Connected Persons:

- prohibition of retaliation on account of a Report;
- support measures, which consist of information, assistance, and advice free of charge from third-sector entities indicated in a list available on the ANAC website on the reporting modalities and regulatory provisions in favour of the Reporting Party and the Involved Person;
- protection against retaliation, which includes: the possibility of informing ANAC of retaliation one believes to have suffered as a result of a Report; the provision of nullity of acts taken in breach of the prohibition of retaliation, which can also be enforced in court;
- limitations of liability in the event of disclosure (or dissemination) of violations covered by the obligation of secrecy or relating to the protection of copyright or the protection of personal data, or information on violations offending the reputation of the person involved or reported, if at the time of disclosure (or dissemination) there were reasonable grounds to believe that it was necessary to disclose the violation;
- limitations of liability, unless the act constitutes a criminal offence, for the acquisition of or access to information on breaches;
- sanctions.

To whom the protective measures apply:

- to the reporting person;
- the Facilitator (a natural person who assists the reporter in the reporting process, operating within the same work context and whose assistance must remain confidential);
- persons in the same work environment as the reporting person, the whistleblower or the person making a public disclosure and who are related to them by a stable emotional or family relationship up to the fourth degree;

- co-workers of the reporting person or of the person making a public disclosure, who work in the same work environment as the reporting person and who have a regular and current relationship with that person;
- entities owned by the reporting person or for which those persons work as well as entities operating in the same work environment as those persons.

The protections are not guaranteed and a disciplinary sanction is imposed on the reporting or whistleblowing person when the criminal liability of the reporting person for the offences of defamation or slander or, in any case, for the same offences committed with the complaint to the judicial or accounting authority or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance.

15. POSSIBILITY OF ANONYMITY

"Anonymous" reports, made without identification of the whistleblower, are taken into account provided that they too are adequately substantiated and made with a wealth of details, i.e. where they can bring to light facts and situations relating them to specific contexts.
In any case, the anonymous whistleblower or complainant, subsequently identified, who has reported that he or she has suffered retaliation may benefit from the protection that the decree guarantees against retaliatory measures.

16. RESPONSIBILITIES OF THE WHISTLEBLOWER

This procedure is without prejudice to the criminal and disciplinary liability of the whistleblower in the event of a libellous or defamatory report under the Criminal Code and Article 2043 of the Civil Code. Article 16(3) of the decree provides that protection is no longer guaranteed when the reporting person is found, even in a court of first instance, to be criminally liable for the offences of defamation or slander or, in any case, for the same offences committed with the report to the judicial or accounting authorities, or to be civilly liable for the same offences in cases of wilful misconduct or gross negligence. A disciplinary sanction is imposed on the reporting or denouncing person. Any form of abuse of this procedure, such as manifestly opportunistic reports made with the sole aim of harming the whistleblower or other persons and any other hypothesis of improper use or intentional exploitation of the institution, shall also give rise to liability in disciplinary and other competent fora.

17. PROTECTION OF THE REPORTED PERSON

To avoid detrimental consequences, even if only of a reputational nature, within the work context, the protection reserved to the Whistleblower should also be granted to the reported person, with particular regard to the phase of forwarding the report to third parties.

18. RESTRICTION OF LIABILITY

The person who detects or disseminates information on the following violations is not punishable:

- Violations covered by the obligation of secrecy;
- Violations relating to copyright protection or the protection of personal data;
- Violations offending the reputation of the person involved or denounced.

When the aforementioned hypotheses occur, any liability, including civil or administrative liability, is also excluded.

19. INFORMATION AND TRAINING

Information on this Procedure is made accessible and available to all in the workplace and by publication on the company website.
Information on the Procedure is also made available when hiring and leaving an employee.
Training on whistleblowing and, in general, on the provisions of this Procedure, is also included in the personnel training plans provided by the Organisation on corporate compliance.

20. MODES OF OPERATION

Phase 1: Report Submission and Registration
Reports can be made through any of the channels indicated in the above procedure. Upon receipt of a Report, regardless of the channel used, the Addressee will assign a sequential identification number that will enable it to be uniquely identified.
It will therefore provide a so-called Reporting Register containing at least the following fields (which it will update in line with the outcome of the activities referred to in the subsequent steps of the process outlined in this Procedure):

- Identification protocol;
- Date of receipt;
- Report Reception Channel;
- Outcome of the assessment phase on the admissibility of the Report;
- Outcome of the stage of assessing the merits of the Report;
- Sharing of findings;
- Conclusion.

Phase 2: Evaluation of the Admissibility of the Report
Once the Report is received, the addressee has 7 days to assess its admissibility. With this first analysis, the addressee of the Report assesses the existence of the following requirements, which are essential for the Report:

- The whistleblower is among the Recipients of Whistleblowing, as identified by the rule;
- there is an interest in the integrity of the organisation;
- the reported conduct constitutes an offence as specified in the procedure.

If only the first requirement is not met, the recipient of the Report will take the Report into account, but the protection of the confidentiality of the Whistleblower will not be guaranteed. If only the second requirement is not met, the addressee of the Report proceeds to delete the Report received from the system. If only the third requirement is not met, the addressee proceeds to delete the Report received from the system.

- In the case of a prohibited Report, the addressee considers the possibility of reporting to the Judicial Authority.

Phase 3: Assessment of the Merits of the Report
Once the admissibility of the Report has been declared and noted in the Register, the addressee initiates a verification and analysis activity to assess its validity. The management and verification of the justification of the circumstances represented in the report are entrusted to the addressee. He does so in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the personal hearing of the reporter and of any other persons who may report on the facts reported, with the adoption of the necessary precautions. The addressee's activity is not one of actual fact-finding but takes the form of making an initial impartial assessment of the existence of what has been reported.
To carry out its investigative activity, the addressee may request further information from the Whistleblower, may acquire deeds and documents from other offices of the administration, and may avail itself of the

support of other functions of the Organisation, always taking care that the protection of the confidentiality of the Whistleblower and the reported person is not compromised.
For the definition of the enquiry, the time limit is 30 days, starting from the date of its commencement, it being understood that, where necessary, the Organisation will authorise the Recipient to extend the aforementioned time limits, providing adequate justification.
If the Report proves to be unfounded, the addressee proceeds with its filing, giving the Reporting Party adequate reasons. If the Report proves to be well-founded, the Addressee of the Report shall send a report of investigative findings to the relevant internal bodies or external authorities concerning the profiles of unlawfulness found. He shall make sure that such documentation does not contain any reference to the identity of the Reporting Party and the Reported Person, or any other implicit reference that could lead, without any doubt, to the Reporting Party. The same duty of confidentiality applies to the internal managers whose task it is to verify the truthfulness of the Report as it does to the Reporting Recipient.
Well-founded Reports relate to the Organisation's Code of Ethics and Model 231. In the event of a founded Report about the Code of Ethics or the Organisation's 231 Model, the Recipient
of the Report proceeds to forward the report of investigative findings to the Supervisory Board, ensuring that such documentation does not contain any reference to the identity of the Whistleblower and the Whistleblower, or any other implicit reference that could lead to the Whistleblower. In this case, the same duty of confidentiality applies to the Supervisory Board as to the recipient of the report. The Recipient of the Report, regardless of whether or not the Report relates to the Code of Ethics and/or Model 231, shall periodically inform the Supervisory Board of the Reports received.

Phase 4: Sharing of Findings
Of all the activities carried out by the internal bodies in charge and of the findings, the Report Recipient is kept constantly informed. A final report will be drawn up by the internal body that analysed the Report on its merits, on the results of the verification carried out, on any deficiencies found and highlighting, where possible, actions for improvement. The body in charge ensures that such documentation does not contain any reference to the identity of the reporting person and of the reported person, or any other implicit reference that could lead, without any doubt, to the reporting person. The final report will be forwarded and/or shared with the organisation, which will proceed to inform the corporate functions involved, should it be necessary to take disciplinary action. For the management of the relevant disciplinary procedure and any sanctions that may be imposed, please refer to the organisation's disciplinary system, the Supplementary Measures and the organisation's Model 231.

Phase 5 Keeping the data contained in the Report.
The Report Recipient must appropriately file the Report and the related documentation in electronic and/or paper format, depending on the medium. It must be kept, to ensure the management and traceability of the reports and the activities carried out to duly follow them up, for five years from the receipt of the Report, unless judicial or disciplinary action is taken against the whistleblower or the person making the false or defamatory statements. In that case, the relevant documents must be kept until the conclusion of the proceedings and the expiry of the time limit for appeal. After the above deadlines, the Report and its documentation will be deleted or anonymised.