



WHISTLEBLOWING
POLICY

Rev. no.	Rev. date	Notes
00	19.12.2023	First issue

LIST OF CONTENTS

INTRODUCTION 3

1. DEFINITIONS AND ABBREVIATIONS 3

2. TERMS OF VALIDITY AND DISSEMINATION..... 6

3. PURPOSE 6

4. CONTENT OF THE REPORT 7

5. RECIPIENTS OF THE *POLICY*..... 9

6. WAYS OF REPORTING UNLAWFUL CONDUCT AND RECIPIENTS OF REPORTS 9

 6.1. “INTERNAL” REPORTING CHANNELS (“Internal channels”) 9

 6.1.1. REPORT MANAGEMENT: PRELIMINARY VERIFICATION 11

 6.1.2. REPORT MANAGEMENT: PRELIMINARY EXAMINATION AND ASSESSMENT.. 12

 6.1.3. REPORT MANAGEMENT: OUTCOME OF THE INVESTIGATION 13

 6.1.4. CORRECTIVE ACTION MONITORING AND ANNUAL PERIODIC REPORTING 13

 6.1.5. PROCESSING AND MANAGEMENT OF PERSONAL DATA..... 14

 6.2. “EXTERNAL” REPORTING CHANNELS (“External channels”)..... 15

 6.3. PUBLIC DISCLOSURES (the “Public Disclosures”) 16

7. PROTECTION OF THE WHISTLEBLOWER AND OF THE REPORTED PERSON 17

 7.1. PROTECTION OF THE WHISTLEBLOWER 17

 7.2. PROTECTION OF THE REPORTED PERSON 21

8. DISCIPLINARY SYSTEM..... 22

9. DOCUMENTATION ARCHIVING 23

INTRODUCTION

The **Scigno Group**, consisting of the companies **Scigno S.p.A.**, **Master S.r.l.** and **Costruzioni Chiusure Ermetiche S.r.l.** (hereinafter also referred to as the “**Scigno Group**”) intends to promote a corporate culture characterised by virtuous conduct and a *Corporate Governance* system that prevents the commission of unlawful acts, while at the same time guaranteeing a working environment where employees can calmly report any unlawful conduct and promote a virtuous path of transparency and respect for adequate ethical *standards*.

With the aim of sponsoring and reinforcing such *standards*, the Scigno Group, recognising the importance of having a specific procedure governing the reporting of unlawful conduct by employees and third parties, has decided to adopt this *Whistleblowing Policy* (hereinafter also referred to as the “**Policy**”) - which is also an integral part of the Organisation, Management and Control Models pursuant to Italian Legislative Decree no. 231/2001¹ of the companies of the Scigno Group (hereinafter also referred to as “**231 Models**” or “**Organisational Models**”) - for the reporting of any conduct, including omissions, that constitutes or may constitute a violation or inducement to a violation of (i) national or European Union regulatory provisions, (ii) values and principles specified in the Code of Ethics of the companies of the Scigno Group, (iii) unlawful conduct relevant under Italian Legislative Decree No. 231/2001 or violation of Models 231; and (iv) Internal procedures adopted by Scigno Group companies.

To this end, the companies of the Scigno Group have defined specific communication channels for the management of Reports in order to comply with Italian Legislative Decree no. 24/2023. This legislation introduced into our legal system the content of EU Directive 2019/1937, which harmonised the rules on *whistleblowing* within the European Union, prescribing minimum protection *standards* that each Member State is required to transpose.

Therefore, the Recipients of this *Policy* are invited to promptly report any such conduct by means of the methods described below, refraining from undertaking autonomous initiatives of analysis and/or investigation.

1. DEFINITIONS AND ABBREVIATIONS

National Anti-Corruption Authority (ANAC): pursuant to Italian Legislative Decree 24/2023, it is the authority in charge of the management of External Reporting Channels.

¹ Pursuant to Art. 6, par. 2 *bis*, of Italian Legislative Decree 231/2001 (as amended by Art. 24, par. 5 of the Italian Legislative Decree 24/2023, for which the management, organisation and control models “provide, pursuant to the Italian Legislative Decree implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, for Internal Reporting Channels, the prohibition of retaliation and the Disciplinary System, adopted pursuant to paragraph 2(e)”).

Reporting Channels: communication channels identified by the Scigno Group as internal or external means to convey Reports.

Code of Ethics: a document setting out the values and reference principles governing activities and relations with all parties with which Scigno Group companies enter into relations in pursuit of their corporate purpose.

Reporting Committee: this is the collegial body, with a non-fixed composition, responsible for the process of analysing and managing Reports. It is composed of Mr. Pierpaolo Ruffolo, Director of Human Resources of the Scigno Group, and lawyer Lara Sanna, external consultant.

If the subject of the Report concerns unlawful conduct within the meaning of Italian Legislative Decree 231/2001, or violations of Models 231, the Chairman of the Supervisory Board (for *Scigno S.p.A.*) or the member of the single-member Supervisory Board (for *Master S.r.l.* and/or *Costruzioni Chiusure Ermetiche S.r.l.*) is involved in the Reporting Committee. If the subject of the Report does not fall within the competence of the Reporting Committee, the Reporting Committee is entitled to engage outsourced consultants to analyse and handle the reported facts, subject to due confidentiality and data protection procedures.

Unlawful conduct: any act or omission that constitutes or could constitute a violation or inducement to a violation in respect of the conduct among those referred to in par. 4 of the *Policy*.

Work context: this refers to present or past professional/work-related activities, carried out within the framework of relations with Scigno Group companies, through which a person acquires Information on Violations and in the context of which he/she could suffer retaliation in the event of a Report, Public disclosure or complaint to the Authority.

National Collective Labour Agreement (CCNL): National Collective Labour Agreement applicable to Scigno Group companies.

Recipients: this means the subjects of the Scigno Group, as well as third parties, natural or legal persons (such as, but not limited to, suppliers, self-employed and freelance workers, consultants or customers, collaborators or business partners).

Public disclosure: this means any activity making Information about Violations publicly available through print or electronic means or otherwise through means of dissemination capable of reaching a large number of people.

Facilitator: this means the natural person working in the same Work context as the Whistleblower and who has provided/is providing assistance to the latter in the Reporting process, whose assistance must be kept confidential.

EU Regulation No. 679/2016 (GDPR): legislation on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data.

Alternative Manager: Alternative Managers, according to this *Policy*, are one or more members of the Reporting Committee who are entrusted with the activities foreseen by this *Policy* for the management of the Reports, when the Whistleblower indicates and proves with objective and concrete evidence a conflict of interest of one or more members of the Reporting Committee or when the Reported person is a member of the Reporting Committee.

Report Manager/Manager: the person in charge of receiving and managing internal Reports for the purposes of this *Policy*, appointed in accordance with Article 4(2) of Italian Legislative Decree 24/2023.

Privacy policy: this means the *privacy* notice given pursuant to Article 13 and 14 of the GDPR to the persons concerned, i.e. to the Reported person and the Whistleblower.

Information on Violations: written/oral information, including reasonable suspicions, concerning Violations committed or likely to be committed, as well as circumstantial evidence of conduct aimed at concealing them².

Model 231 or Organisational Model: means the organic set of principles, rules, provisions, methods and operating procedures, aimed at preventing the offences referred to in Italian Legislative Decree 231/2001.

SB: Supervisory Bodies pursuant to Italian Legislative Decree 231/2001 of the Scigno Group companies.

Reporting Platform (so-called *Tool*): a computer system that guarantees, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, of the Reported person, of the person in any case mentioned in the Report, as well as the content of the Report and of the relevant documentation.

Internal procedures: this means the set of procedures, policies, operating instructions and all other documents that form part of the company's regulatory system.

Retaliation: direct or indirect retaliatory or discriminatory acts, carried out by the companies of the Scigno Group against the Whistleblower for reasons linked, directly or indirectly, to the Report.

² This also includes irregularities or anomalies that the Whistleblower believes could lead to a violation.

Whistleblower: a person belonging to the categories indicated in par. 5 of the *Policy* who makes the Report, or his/her Facilitator(s).

Reported person: a person to whom the Whistleblower attributes the Illicit Conduct that is the subject of the Report.

Report(s): communication(s) by the Whistleblower concerning information on Unlawful conduct.

Internal report: written or oral communication of Information on Violations, submitted through the Internal Reporting Channel according to par. 6.1 of the *Policy*.

External report: written or oral communication of Information on Violations, submitted through the External Reporting Channel according to par. 6.2 of the *Policy*.

Disciplinary system: set of sanctioning measures put in place against those who violate the provisions of this *Policy*.

Violation: this means all the conduct, acts or omissions identified in par. 4 below.

Terms defined in the singular form shall also be understood in the plural when the context so requires and vice versa.

2. TERMS OF VALIDITY AND DISSEMINATION

This *Policy* takes effect from the date of its issue indicated on the cover page.

Any subsequent update supersedes and replaces, from the date of its issue, all previously issued versions.

This *Policy* shall be disseminated as widely as possible.

To this end, it is published on the *website* of the companies of the Scigno Group, on the company *intranet* and made available in various formats on further company management systems, as well as at the company premises.

3. PURPOSE

The purpose of the Procedure is to regulate the Channels for Reporting Violations of offences or irregularities and to eliminate the factors that may hinder or discourage Reports, as well as to regulate the measures for the protection of Whistleblowers and the Disciplinary System.

4. CONTENT OF THE REPORT

This *Policy* describes the process and communication channels to be used for sending, receiving, analysing and processing Reports of Unlawful conduct, including omissions, which constitute or may constitute:

- a violation, or inducement to a violation, of laws and regulations relating to the scope of application of the European Union or national acts set out in the Annex to Italian Legislative Decree No. 24/2023 or, even if not included in that Annex, relating to the following areas:
 - a) public procurement;
 - b) financial services, products and markets and the prevention of money laundering and terrorist financing;
 - c) safety and conformity of products;
 - d) safety of transports;
 - e) radiation protection and nuclear safety;
 - f) food and feed safety and animal health and welfare;
 - g) consumer protection;
 - h) protection of privacy and protection of personal data, and security of networks and information systems;
 - i) public health;
 - j) environmental protection;
 - k) violation of laws on competition and government aids;
 - l) violation of tax regulations on Scigno Group companies;
 - m) financial interests of the European Union;
 - n) administrative, accounting, civil or criminal offences not covered by the above; or
- a violation or inducement of a violation of internal regulations, such as:
 - a) values and principles specified in the Scigno Group companies' Codes of Ethics;

- b) values, principles and controls identified in Model 231 of the Scigno Group companies;
- c) operating methods regulated in the Internal procedures of the Scigno Group companies.

The Report, **sufficiently evidenced and based on precise and concordant factual elements**, must be made by providing the following information, together with any supporting documentation:

- a detailed description of the events that occurred and how they came to be known;
- date and place where the event occurred;
- name and role of the persons involved or elements that might enable them to be identified;
- names of any other persons who may report on the facts that are the subject of the Report or elements that may enable them to be identified;
- reference to any documents that may confirm the accuracy of the reported facts.

The Whistleblower should take care not to report information that is irrelevant or unnecessary to the Report.

The sending of Reports made for the mere purpose of retaliation or intimidation or, in any case, unfounded and made with malice or gross negligence shall be sanctioned.

In particular, the sending of any communication that proves to be unfounded on the basis of objective elements and that is, again on the basis of objective elements, made for the sole purpose of causing unjust damage to the Reported person shall be sanctioned.

The companies of the Scigno Group guarantee the utmost confidentiality on the persons and facts reported, using, to this end, criteria and communication methods suitable to protect the identity and honourableness of the persons mentioned in the Reports, so that the Whistleblower is not subject to any form of retaliation, avoiding in any case the communication of the data acquired to third parties not involved in the process of management of the Report, as regulated in this *Policy*.

Whistleblowers in good faith will be guaranteed against any form of Retaliation, discrimination or penalisation.

The companies of the Scigno Group, in compliance with applicable legislation, guarantee the possibility of making Reports in anonymous form, provided that they are adequately evidenced and their content is sufficiently detailed to make them verifiable.

In the case of anonymous Reports, the Reporting Manager reserves the right to consider them on the basis of the seriousness of the facts reported and in relation to the level of detail and accuracy of their content.

5. RECIPIENTS OF THE *POLICY*

The *Policy* applies to the following subjects:

- a) employees of Scigno Group companies (employees, volunteers, paid and unpaid trainees, *former* employees³, job applicants⁴), as well as self-employed persons;
- b) shareholders and members of the administrative, management, supervisory or representative bodies of the Scigno Group companies, including non-executive members, volunteers and unpaid trainees;
- c) any person working under the supervision and direction of contractors, subcontractors and suppliers, customers, *partners*, consultants and, more generally, *stakeholders* of the Scigno Group companies.

6. WAYS OF REPORTING UNLAWFUL CONDUCT AND RECIPIENTS OF REPORTS

In order to bring the companies of the Scigno Group into line with current regulatory provisions, the following Reporting Channels have been identified, through which the Recipients of the *Policy* may give evidence of the commission or potential commission of Unlawful conduct.

6.1. “INTERNAL” REPORTING CHANNELS (“Internal channels”)

If a Whistleblower has a reasonable suspicion that Unlawful conduct has occurred or may occur, he or she may report it to the companies of the Scigno Group through the following Internal channels (also, the “**Internal report**”):

- (i) using the dedicated *whistleblowing* IT platform (the “**Platform**”), which can be found at the following *link* <https://scignogroupbf.web.app/>;

³ If they report or disclose information on violations acquired in the context of the terminated employment relationship.

⁴ If their employment relationship has not yet commenced and information concerning the violation has been acquired during the selection process or in pre-contract negotiations.

- (ii) through a face-to-face meeting with the Reporting Committee, set within a reasonable time limit. Reports issued through face-to-face meetings, subject to the consent of the Whistleblower, may be documented by drawing up a memo, supported, where appropriate, by a recording on a computer device suitable for listening, by the Reporting Committee. The memo is then submitted to the Whistleblower for the relevant verification and signature.

All Reports are received by the Reporting Committee, which is the body appointed to receive Internal Reports and, except as indicated below, the only authorised to access Internal Channels and view the content of the Internal Report itself, subject to written authorisation by the Scrigno Group company, pursuant to Articles 29 and 32, par. 4 of Regulation (EU) 2016/679 and Article 2-*quaterdecies* of Italian Legislative Decree 196 of 2003.

The management of the Report must be entrusted exclusively to persons who are not in a situation of conflict of interest.

Each Report Manager must be provided with personal authentication credentials to access the IT Platform.

The Report Manager shall take care to put in place appropriate methods to prevent the loss and destruction of Internal Reports, as well as undue access to them.

Although anonymous Reports are allowed, Scrigno Group recommends that they should be nominative, in order to allow the Managers a more efficient investigation activity, applying in any case the safeguards provided against possible Retaliation.

If the Internal Report concerns unlawful conduct relevant under Italian Legislative Decree no. 231/2001, or violations of the Organisational Model, the Reporting Committee involves the Supervisory Board in its activities, in order to more effectively assess the issues within its competence. If the Internal Report refers to one or more members of the Supervisory Board, it shall be forwarded to the Managing Director or to another suitably identified person.

Anyone who receives a Report that has been passed outside the prescribed channels must forward it to the Managers, in original and with any attachments, within 7 (seven) days of receipt.

The transmission should take place in accordance with the criteria of utmost confidentiality and in such a way as to protect the Whistleblower and the identity of the Reported persons, without prejudice to the effectiveness of the subsequent investigation activities.

No copy of the Report received and forwarded to the Managers shall be made.

6.1.1. REPORT MANAGEMENT: PRELIMINARY VERIFICATION

Reports are subject to preliminary verifications by the **Reporting Committee**.

The Manager verifies the presence of data and information useful for an initial assessment of the Report itself.

Within **7 (seven) days** of receipt of the Report, the Manager shall send the Whistleblower an acknowledgement of receipt of the Report, using the methods of communication adopted by the Whistleblower.

The Manager takes all necessary measures to treat Reports confidentially, also in order to protect the identity of the Whistleblower, the Reported Person and the other persons mentioned in the Report.

In the course of the verifications, the Manager may resort to the support of the competent corporate functions from time to time and, where deemed appropriate, of external consultants specialised in the field of the Report received and whose involvement is functional to the investigation of the Report, ensuring the confidentiality and anonymisation of any personal data contained in the Report.

All persons involved in the inspections must maintain strict confidentiality regarding information received in the course of the verifications.

Upon completion of the preliminary verification, the Reporting Committee may:

- a) **dismiss** the Report as manifestly unfounded or relating to conduct or facts not relevant to this *Policy*;
- b) **request additions/clarifications** if the Report appears well-founded but not sufficiently detailed. In the absence of the requested additions, the Manager shall proceed with dismissing.
- c) **open the investigation phase**.

The Manager shall inform the Whistleblower of the outcome of the inspections carried out within a reasonable time limit, in any case not exceeding **3 (three) months**⁵.

⁵ For the **Internal Report**, the Report Manager's acknowledgement must be received within 3 months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within 3 months from the expiry of the 7-day period from the submission of the report.

6.1.2. REPORT MANAGEMENT: PRELIMINARY EXAMINATION AND ASSESSMENT

With reference to each Report, where, following the preliminary analysis, useful and sufficient elements emerge or are otherwise inferable to make an assessment of the merits of the Report itself, the Manager shall:

- obtain further information and/or documentation from the Whistleblower in support of the reported facts;
- proceed to the hearing of the Reported Person and other persons possibly involved in the facts that are the subject of the Report;
- in the event that the reported conduct persists, consider suggesting to the Managing Director, or to another suitably identified person, the adoption of suitable preliminary measures to contain any risks (e.g. suspension of the Reported person);
- resort to the support of other Functions within the Scigno Group companies or third parties (e.g. consultants) when, due to the nature and complexity of the verifications, their involvement is necessary;
- terminate the investigation at any time if, in the course thereof, it is established that the Report is unfounded;
- check possible legal implications for the Scigno Group companies;
- assess whether there is an obligation to inform the competent Authorities of the nature of the offence reported.

In addition, the Manager must:

- ensure that the investigation is accurate, fair, impartial and protects the confidentiality of the identity of the Whistleblower and of the persons involved, including the Reported person;
- guarantee that appropriate measures are taken for the collection, processing and storage of personal information, ensuring that the needs of the investigation are balanced with those of *privacy* protection. On this point, the Manager has the responsibility to consider informing the Reported person about the investigation. The reported person is, however, always informed by the Manager if disciplinary proceedings are initiated;
- ensure that the investigation work is carried out within the time limits set out in par. 7.1.

6.1.3. REPORT MANAGEMENT: OUTCOME OF THE INVESTIGATION

Upon the outcome of the investigation, the Report Manager shall, in any case, issue a review addressed to the Board of Directors (the “**Review**”), which shall:

- summarise the *course of* the investigation;
- set out the conclusions reached and provide any supporting documentation;
- provide recommendations and suggest actions to be taken to remedy the Violations found and ensure that they do not occur in the future.

If, at the end of the investigation, it emerges:

- a) the absence of sufficiently evidenced facts, or the unfoundedness of the Internal Report, the Report Manager will file the Report, informing the Whistleblower (“**dismissal without remark**”), the so-called “*Report without sufficient and relevant indications*” or “*Report unfounded*”;
- b) the final substantiation of the Internal Report, the so-called “*Report founded*”; the Report Manager will:
 - (i) inform the hierarchical manager of the perpetrator of the Violation, as well as the Managing Director or another appropriately identified person, recommending the adoption of corrective measures;
 - (ii) propose disciplinary measures by written communication, in accordance with the Disciplinary System referred to in par. 8.

If, at the end of the investigation, proceedings are initiated against a specific reported person, an *ad hoc* Information Notice must be provided to the latter.

If the Violation is particularly serious or concerns one or more members of the Board of Directors, the Report Manager shall inform the other members of the management body and/or the Board of Statutory Auditors, if appointed, also informing the shareholders.

It is understood that, in all cases, upon completion of the verification of the substantiation of the Report received, **the Whistleblower will be provided with feedback within** a reasonable time limit, in any case not exceeding **three (3) months**.

6.1.4. CORRECTIVE ACTION MONITORING AND ANNUAL PERIODIC REPORTING

The hierarchical manager and the Managing Director, or other appropriately identified person, supervise the implementation of compliance with the identified corrective actions.

The Reporting Committee and the Alternative Managers, at least once a year, draw up a review on the Reports filed and the results of the activities carried out in relation to the Reports under investigation (the “**Annual Review**”). The Annual Review is forwarded to the Board of Directors and/or the Board of Statutory Auditors and, if applicable, to the Supervisory Board of the Scigno Group companies.

6.1.5. PROCESSING AND MANAGEMENT OF PERSONAL DATA

The personal data - including special categories of data and judicial data - communicated in the context of **Internal reports** will be processed in compliance with the provisions of the **GDPR** as better described in **Whistleblower Information Notice** (Annex 1) and **Reported Person Information Notice** (Annex 2), made available on the websites of the Scigno Group companies and also on the online platform.

Internal reports may not be used beyond what is necessary to adequately follow them up.

The identity of the **Whistleblower** and any other information, from which that identity may directly or indirectly be inferred, may not be disclosed without the express consent of the **Whistleblower**:

- a) to persons other than the **Report Manager** and other persons specifically authorised by the Controller. The **Report Manager** must request such consent before proceeding to communicate to any person other than the persons authorised to handle reports.

The **Report Manager** must request consent using the following wording and inform the recipient of the data:

I consent I do not consent

to the disclosure of my identity and any other information from which such identity may be directly or indirectly inferred, to persons other than those competent to receive or act upon Reports;

- b) in **disciplinary proceedings** where the charge is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is indispensable for the accused's defence. The **Report Manager** shall:
 - o in the case of a **Report** received by paper mail or by face-to-face meeting, request such consent prior to the disciplinary proceedings;
 - o in the case of a **Report** received via an IT platform where consent is already requested at the time of transmission of the **Report**, ask for confirmation of any consent already received or denied before the disciplinary proceedings.

The **Report Manager** must request consent using the following wording:

I consent I do not consent

to the disclosure of my identity in disciplinary proceedings where the charge is based, in whole or in part, on the Report and knowledge of my identity is indispensable for the accused's defence.

In the case of an oral **Report** by face-to-face meeting, in addition to the consents referred to in (a) and (b) above, the **Report Manager** must also acquire the following consent:

c) to the documentation of the **Report**.

The **Report Manager** must request consent using the following wording and inform the recipient of the data:

- I consent I do not consent the Authorised Persons to document the Report either by recording it on a device suitable for storage and listening or by a memo

If the **Report Manager** has received consent to document the Report under (c) above, he/she shall document the **Report** either by recording it on a device suitable for storage and listening to it or by means of a memo. The **Whistleblower** may verify, correct and confirm the memo of the meeting by signing it.

The protection of the identity of the **Whistleblower** and of the **Involved Persons** is guaranteed until the conclusion of the procedures initiated on account of the **Internal Report**.

Personal data that are manifestly not useful for the processing of a specific **Internal Report**, where possible, are not collected or, if accidentally collected, are deleted immediately.

The **Involved Person** may not exercise the rights set out in Articles 15-22 of the GDPR if the exercise of those rights would result in actual and concrete prejudice to the confidentiality of the identity of the **Whistleblower**.

6.2. “EXTERNAL” REPORTING CHANNELS (“External channels”)

The Whistleblower of an **Unlawful conduct** may make a Report through External Channels (the “**External Report**”) if, at the time of its submission, one of the following conditions is met:

- a) the Scrigno Group has not adopted the compulsory Internal Channel or, even if it is active, it does not comply with Article 4 of Italian Legislative Decree 24/2023;
- b) the Whistleblower has already made an Internal Report, through the modalities set out in this *Policy*, without it having been followed up;

- c) the Whistleblower has reasonable grounds to believe that, if he/she makes an Internal report, this would not be effectively followed up, or might give rise to the risk of Retaliation;
- d) the Whistleblower has reasonable grounds to believe that the Violation may constitute an imminent or obvious danger to the public;
- e) is himself/herself the Report Manager.

In the above-mentioned cases, the Whistleblower makes the External Report using the methods prepared and implemented by ANAC, either in written form, through the IT platforms or the other means implemented by the same Authority, or in oral form, through the telephone line and/or the recorded voice messaging system implemented.

In detail, ANAC has activated an IT channel for the receipt and management of External Reports - accessible in a special section of its *website* <https://whistleblowing.anticorruzione.it/#/> - which guarantees, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, of the Reported person, of any other persons involved in the Report, as well as the content of the Report and of the supporting documentation.

The same confidentiality is guaranteed even when the External Report is made through channels other than those indicated on the ANAC *website* or reaches staff other than those in charge of processing External Reports, to whom it is in any case transmitted without delay.

The External Report, submitted to a subject other than ANAC, must be transmitted to the competent Authority within 7 (seven) days from the date of its receipt, with simultaneous notification of its transmission to the Whistleblower.

Upon receipt of the External Report, ANAC provides feedback to the Whistleblower within three months or, if there are justified and motivated reasons, within six months from the date of receipt of the External Report or, in the absence of such notice, from the expiry of seven days from its receipt.

6.3. PUBLIC DISCLOSURES (the “Public Disclosures”)

The Whistleblower of an Unlawful conduct who makes a public Disclosure - i.e. through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people - shall benefit from the protection provided by the *Policy* if, at the time of the disclosure, one of the following conditions is met:

- a) the Whistleblower has previously made an Internal and External Report or has made an External Report directly, under the conditions and in the manner laid

down in the *Policy*, but has not received a reply within the time limits laid down in the *Policy*;

- b) the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public, such as where there is an emergency situation or the risk of irreversible damage;
- c) the Whistleblower has reasonable grounds to believe that the External report may entail a risk of Retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there are reasonable grounds to believe that the recipient of the Report may be colluding with the perpetrator of the Violation or involved in the Violation.

7. PROTECTION OF THE WHISTLEBLOWER AND OF THE REPORTED PERSON

7.1. PROTECTION OF THE WHISTLEBLOWER

In order to protect the Whistleblower against possible retaliatory and/or discriminatory acts, protection measures are provided for, which apply when the following conditions are met:

- a) at the time of the Report or Public Disclosure, the Whistleblower or Complainant had reasonable grounds to believe that the Information on the Violations was true and fell within the objective scope of this *Policy*;
- b) the Report or Public Disclosure was made in accordance with the terms of this *Policy*.

The identity of the Whistleblower is protected and kept confidential at all times, his/her data being processed in accordance with the law and all useful measures being taken to prevent the dissemination of the Whistleblower's data and the content of the Report.

Retaliatory or discriminatory acts, whether direct or indirect, against the Whistleblower for reasons directly or indirectly linked to the Report are forbidden and are also sanctioned.

The Scrigno Group companies guarantee the prohibition and removal of the effects of any form of Retaliation against the Whistleblower, including, in particular:

- dismissal, suspension or equivalent measures;
- demotion or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working

hours;

- suspension of training or any restriction of access to it
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines; coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a fixed-term employment contract into a permanent employment contract where the employee had legitimate expectations of being offered permanent employment;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- blacklisting on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of the contract for goods or services;
- cancellation of a licence or permit;
- request to undergo psychiatric or medical examinations.

It is reiterated that the measures to protect Whistleblowers also apply, where appropriate:

- a) to Facilitators;
- b) third parties connected with the Whistleblower and who might risk Retaliation in the Work context, such as colleagues or persons related to the Whistleblower by a stable emotional or kinship link up to the fourth degree;
- c) legal entities that the Whistleblower owns, works for or is otherwise connected to in a Work Context.

The Whistleblower may not be held liable for defamation, breach of copyright or obligations of secrecy, with the exception of those of the legal or medical profession, as

well as for violation of data protection rules if, at the time of the Report, he or she had reasonable grounds to believe that the Information on Violations was true, within the scope of the law and in accordance with established procedures.

No liability can be attributed to the Whistleblower even in relation to the conduct adopted to access the information reported, unless it constitutes a criminal offence.

The exclusion of liability does not apply if a conviction for the offence of defamation or slander has been obtained, even at first instance, or if liability on the same grounds of wilful misconduct or gross negligence has been established in civil proceedings.

This is without prejudice to cases in which the Report proves to be false and was made with malice or gross negligence, or in the event that the conduct, acts or omissions are not related to the Report, to the complaint to the judicial or accounting authorities or to the Public Disclosure, or that they are not strictly necessary for the disclosure of the Violation.

In addition, the persons concerned have the right to legal protection in the event that criminal or civil liability is found against the Whistleblower in connection with the falsehood of what has been declared or reported.

Confidentiality and disclosure of the identity of the Whistleblower (if disclosed) and of any other information from which the identity of the Whistleblower can be deduced directly or indirectly, is allowed to the extent that anonymity and confidentiality are enforceable under the law.

In particular, it is the task of the Reporting Committee to ensure the secrecy of the identity of the Whistleblower (if communicated) from the moment the Report is taken in charge until the end of the investigation into its merits, even if it turns out to be erroneous or unfounded. Reports may not be used beyond what is necessary to adequately follow them up.

The identity of the Whistleblower (if disclosed) and of any other information from which the identity of the Whistleblower can be deduced directly or indirectly, cannot be disclosed, without the express consent of the Whistleblower, to persons other than those competent to receive or follow up Reports and expressly authorised to process such data.

Anyway, personal data that are manifestly not useful for the processing of a specific Report are not collected or, if accidentally collected, are deleted immediately.

In case of transmission of the Report to other structures/organisations/third parties for the performance of investigations, it is the Reporting Committee's obligation to separate the identity of the Whistleblower (if known) from the content of the Report, so that the reported facts can be processed anonymously, and that the association of the Report with the identity of the Whistleblower (if known) only takes place when strictly necessary.

For Reports transmitted through the Platform referred to in the preceding paragraphs, the confidentiality of the Whistleblower is guaranteed in the following ways:

- the Platform consists of a **web application**, separate and independent from the IT systems of the Scigno Group companies, in that it is hosted on an independent *server* that allows Reports to be made from any device, in a highly confidential and facilitated manner, guaranteeing the protection of the identifying data of the Whistleblowers, including through the use of encryption tools;
- the Platform guarantees high standards of **security**, **non-traceability** and **integrity** of information, as well as **confidentiality** of the identity of the Reported Person and the Whistleblower, leaving the option for the Whistleblower to enter the Report also anonymously. This protection is also guaranteed in the case of verbal communications;
- adoption of the “*no-log*” policy, which does not collect in any way, directly or indirectly, information on the connection mode (e.g. *server*, *IP address*, *mac address...*), thus guaranteeing complete anonymity in access. This means, in particular, that computer systems are not able to identify the access point (*IP address*) to the portal, even if access is from a *computer* connected to the network of the Scigno Group companies;
- attribution of an identification code to the Report in order to protect the identity of the Whistleblower;
- provision of access via the Internet on the Scigno Group companies' *website* (available to anyone, including employees) in the absence of registration, the Whistleblower being able to remain anonymous. The latter, if he or she so wishes, may otherwise indicate his or her name and give express consent for his or her personal details to be disclosed.

The Reported person may not request to know the name of the Whistleblower, except in the cases expressly provided for by law.

Within the framework of the disciplinary proceedings activated by the companies of the Scigno Group, the identity of the Whistleblower (if known) cannot be disclosed if the allegation of the disciplinary charge is based on investigations that are distinct and additional to the Report, even if consequent to the same.

If instead the charge is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is indispensable for the accused person's defence, the Report will be usable for the purposes of disciplinary actions only if the Whistleblower consents to

the disclosure of his/her identity. In such cases, the Whistleblower is notified in writing of the reasons for the disclosure of the confidential data.

In addition, those who believe they have suffered Retaliation as a consequence of the Report or Public Disclosure shall inform the Report Manager, who, after assessing the existence of retaliatory or discriminatory elements, shall report the alleged discrimination to the Managing Director or to another appropriately identified person.

7.2. PROTECTION OF THE REPORTED PERSON

In order to avoid detrimental consequences within the Work context, even if only of a reputational nature, the protection reserved to the Whistleblower, as set out in the preceding paragraph, shall also be granted to the Reported person.

After investigating the merits of the Report, the Report Manager, if disciplinary proceedings are initiated against the Reported person:

- (i) informs the latter;
- (ii) keeps him/her informed of developments in the proceedings, consistently with the conduct of the necessary verification and evidence-gathering activities, so as to enable him/her to exercise the rights of defence.

The Reported person's personal data may be forwarded to the competent administrative or judicial authorities and, more generally, to public bodies, in compliance with the formalities laid down by law, also in order to comply with requests received from them.

The companies of the Scigno Group require everyone to cooperate in maintaining a climate of mutual respect, and prohibit and sanction attitudes that may offend the dignity, honour and reputation of each individual. The guarantees of confidentiality set out in this *Policy* also protect the Reported person or other persons involved.

The Reported Person has the right to be informed of the existence of the Report and of the outcome of the verifications carried out. Such information may, however, be delayed, limited to the time necessary, in order to avoid the risk of jeopardising the assessment requirements, including those that may be requested by the Judicial Authority, if involved.

The Reported Person shall not be sanctioned in the absence of objective evidence of the reported Violation, or without having investigated the facts that are the subject of the Report and contested the relevant charges, as provided for by the applicable regulations.

For the further protection of the Reported person, the actions and powers allowed to him/her by law remain unaffected.

It is specified that the identity of the persons involved and mentioned in the Report is also protected, until the conclusion of the proceedings initiated as a result of the Report, in compliance with the same guarantees provided for in favour of the Whistleblower.

8. DISCIPLINARY SYSTEM

Provision is made for disciplinary proceedings to be instituted against the person responsible in the event of a violation of this *Policy* and when Scrigno Group companies ascertain that:

- a Violation has been committed;
- Retaliation has occurred;
- the Report was obstructed, even in an attempted form;
- the obligation of confidentiality set out in Article 12 of Legislative Decree 24/2023 has been breached;
- the Whistleblower has made a Report, Public Disclosure or complaint to the Judicial Authority with wilful misconduct or gross negligence;
- verification and analysis of the Internal Reports received was not carried out.

The applicable sanctions are those set out in the Organisational Models, as borrowed from the CCNL applicable to Scrigno Group companies.

The companies of the Scrigno Group, through the bodies and functions in charge, shall impose sanctions proportionate to violations of this *Policy* with impartiality, uniformity and fairness.

Failure to comply with and/or violation of the rules of conduct set out in this *Policy* by employees/directors of the Scrigno Group companies constitutes a breach of the obligations arising from the employment relationship, giving rise to the application of disciplinary sanctions; such sanctions will be applied in compliance with the provisions of the law and collective bargaining and will be proportionate to the seriousness and nature of the facts.

Violations of this *Policy* by members of the corporate bodies of the Scrigno Group companies must be reported to the Report Manager / Board of Directors, who will take appropriate action in accordance with the law.

Any behaviour on the part of third parties, in violation of the provisions of this *Policy* may also result in the termination of the contractual relationship, without prejudice to any claim for compensation on the part of the Scrigno Group companies if damage is caused by such behaviour.

9. DOCUMENTATION ARCHIVING

The documentation used in carrying out the activities (even in the case of non-significant Reports) must be kept in a special archive, in order to ensure the reconstruction of the different stages of the process.

The Internal and External Reports and the related documentation are kept for as **long as necessary for the processing of the Report** and, in any case, no longer than **5 (five) years** from the date of the communication of the final outcome of the report procedure - in compliance with the confidentiality obligations set out in Article 12 and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of the Italian Legislative Decree No. 51 of 18 May 2018. Personal data that are manifestly not useful for the processing of a specific Report are not archived or, if accidentally collected, are deleted immediately.

If a recorded telephone line or other recorded voice messaging system was used for the Report, the Report, subject to the consent of the Whistleblower, is documented by the personnel in charge by means of a recording on a device suitable for storage and listening, or by a verbatim transcript.

If an unrecorded telephone line or other unrecorded voice messaging system is used for the Report, the Report is documented in writing by means of a detailed record of the conversation by the personnel in charge.

When, at the request of the Whistleblower, the Report is made orally in the course of a meeting with the personnel in charge, it is documented, with the consent of the Whistleblower, by the personnel in charge by means of a recording on a device suitable for storage and listening or by means of a memo.