istitutomarangoni

WHISTLEBLOWING REGULATION

Table of Contents

Art. 1 – Legal Framework

The present regulation (hereinafter, '**Regulation**') covers the procedures for receiving and handling reports of wrongdoing in the corporate sphere regarding whistleblowing (that is the institution established to protect the individual who reports breaches of which he/she becomes aware in the work context). It is an integral part of the activities envisaged in the Organization, Management and Control Model (in Italy, the so-called *Modello di Organizzazione e Gestione* – hereinafter, '**MOG**' – adopted in compliance with the Italian Legislative Decree no. 231 of June 8, 2001, as amended), of Istituto Marangoni (hereinafter, '**Company**').

The Company undertakes to comply with the applicable legislation prescribed by the European Union and national legislators regarding (i) the protection of persons who report breaches of Union and national law and (ii) the protection of individuals with regard to the processing of personal data and the free movement of such data.

The Company also undertakes to comply with all other provisions adopted by the competent authorities aimed at providing guidance and principles for the proper performance of the established obligations (hereinafter, collectively, '**Applicable Legislation**').

Art. 2 – The whistleblower

The whistleblower (hereinafter, '**Whistleblower**') is the person who makes a report (hereinafter, '**Report**') on the breaches acquired in the work context, thereby exposing himself/herself to the risk of retaliation, understood as any act, measure, conduct or omission, even if only attempted or threatened, that causes or is likely to cause, directly or indirectly, unjustified harm to the person.

These Reports represent an effective widespread control solution that provides an internal protection mechanism within the Company, indirectly creating a self-sustaining compliance system.

For such Reports to be encouraged, it is necessary for the Whistleblower to be 'protected' from retaliation, for example, by being able to benefit from the protection of confidentiality about his or her identity.

Art. 3 – Purpose

The Regulation sets the way Reports are received and handled, with the overall objective of protecting

the Whistleblower by limiting, as much as possible, the presence of factors that may discourage the use of the institution of whistleblowing.
Specifically, it is deemed proper to provide the Whistleblower with all operational indications about the subject, content, recipients, and mode of transmission of Reports, taking care to indicate the protections that the Applicable Legislation makes available to him/her.

Further objectives of the Regulation can be summarized as to define and formalize:

- The reporting procedure by establishing terms, roles, and responsibilities.
- The rules that need to be observed in order to ensure the confidentiality of the identity of the Whistleblower, the person involved, and the person mentioned in the Report, as well as the content of the Report and related documentation.
- The duties of the managing party of the internal reporting channels (hereinafter, '**Handler**').

Art. 4 – Individuals who can make Reports

Reports may be made by:

- Employees, including trainees and those in part-time, intermittent, fixed-term, temporary, contract, casual or occasional employment relationships with the Company.
- Collaborators of the Company in various capacities, such as: independent contractors, partners (e.g., attorneys), freelancers and consultants who work for the Company.
- Volunteers and interns (paid and unpaid) who perform their activities for the Company.
- Shareholders (individuals) of the Company.
- Members of management and supervisory bodies.

If a Report is submitted, the protection of the confidentiality of the identity of the Whistleblower and of the person reported or otherwise mentioned in the Report, as well as of the content of the Report and its documentation, is guaranteed to all the aforementioned persons from the moment of receipt and in any subsequent contact. However, the protection of the confidentiality of identity is not to be understood as anonymity: indeed, in order to benefit from the protection offered by the Applicable

Legislation, the Whistleblower must identify himself/herself.

Art. 5 – Subject of the Report

The Whistleblower may Report any unlawful conduct that has come to his/her attention because of his/her relationship with the Company, regardless of whether the reported breach occurred during, before or after the establishment of the legal relationship: in fact, the Report may be submitted during the selection process, during the probationary period or after the termination of the employment relationship. The Report must be based on factual information related to the Company.

Subject of the Report may be all behaviors, acts or omissions consisting of:

1. Breaches of European Union law using all available reporting channels (internal and external channels, public disclosure, reporting to judicial authorities):
    a. Offenses falling within the scope of EU acts related to the following areas: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data; security of network and information systems.
    b. Acts or omissions that harm the financial interests of the EU, such as fraud, corruption, and any other illegal activities related to Union expenditures.
    c. Acts or omissions relating to the EU internal market, including any mechanism designed to obtain a tax advantage that nullifies the object or purpose of the applicable corporate tax law.
    d. Acts or conducts that frustrate the object or purpose of the EU provisions set forth above.
2. Breaches of national law, reportable through internal channels only:
    a. Prerequisite offenses for the application of national law (Italian Legislative Decree no. 231 of June 8, 2001), included but not limited to: receiving undue disbursements, committing fraud against the State, a public entity, or the European Union, or obtaining public disbursements, computer fraud against the State or a public entity, and fraud in public

procurement, embezzlement, extortion, undue inducement to give or promise benefits, bribery and abuse of office, etc.

b. Breach of the MOG adopted by the Company.

It should be noted that the Report may also concern information (including well-founded suspicions) relating to conduct aimed at concealing the aforementioned breaches, information relating to unlawful activities that have not yet been carried out but which the Whistleblower reasonably believes may occur on the basis of concrete elements (including irregularities and anomalies), or on the basis of the presence of concrete, precise and concordant elements. On the other hand, Reports based on mere suspicions or rumors are not worthy of protection.

In any case, the following can't be the subject of a Report:

- Facts related to a personal interest of the Whistleblower or pertaining exclusively to his or her individual employment relationships (including in relation to hierarchically superior figures).
- Facts related to breaches already compulsorily regulated in certain special sectors, to which a specific reporting discipline continues to apply (such as financial services, products and markets, prevention of money laundering, prevention of terrorism financing, transport safety, environmental protection, etc.).
- Facts concerning national security and defense.

Art. 6 – Content of the Report

The Whistleblower must provide all relevant elements so that the Handler can proceed with the investigations aimed at verifying the validity of the facts brought to his/her attention.

For this purpose, the Report must contain the following elements:

a) Identity and contact details of the Whistleblower.

b) A clear and complete description of the facts that are the subject of the Report.

c) The circumstances of time and place in which the facts were committed.

d) Personal details or other elements enabling identification of the person(s) who has/have committed the facts reported.

In addition, where known, the following information may also be provided:

- The details of other informed persons who can report on the facts that are the subject of the Report.
- Documents that can confirm the validity of such facts.
- Any other data that may serve to provide useful feedback on the existence of the facts reported.

Art. 7 – Anonymous Reports

Anonymous Reports are those that are lacking in elements allowing their author to be identified; by virtue of the Applicable Legislation, they do not fall within the scope of the Regulation and are therefore treated in the same way as ordinary Reports.

The Handler must also record anonymous Reports, which are retained with all the relevant documentation attached, in order to guarantee to the Whistleblower, who identifies himself/herself at a later stage and who has informed the Italian National Anti-Corruption Authority (hereinafter, '**ANAC**') that he/she has suffered retaliatory measures as a result of the Report, the protections offered by the Applicable Legislation.

Such Reports, which are in principle inadmissible, may in any case be the subject of subsequent verifications only if they relate to particularly serious facts and whose content is adequately detailed and circumstantiated.

In such cases, the protection typically afforded by the institution of whistleblowing will be guaranteed only in the event of Reports made by clearly identifiable and/or correctly identified persons.

Art. 8 – Safeguards provided

The Applicable Legislation provides the following protection measures:

1. **Protecting the confidentiality of the Whistleblower's identity**

   The identity of the Whistleblower, as well as any other information from which it may be inferred (directly or indirectly), may not be disclosed to persons other than the Handler without the

Whistleblower's express consent; this principle, in the context of any proceedings instituted as a consequence of the Report, is declined as follows:

a. In criminal proceedings, the identity of the Whistleblower must be kept confidential until the accused is informed of it, and in any case, no later than the end of the preliminary investigation.
b. In proceedings before the Court of Auditors, the obligation of secrecy is provided for until the end of the investigation phase. Subsequently, the identity of the reporter may be revealed by the judicial authority for subsequent use in the proceedings themselves.
c. Within the scope of disciplinary proceedings, the identity of the Whistleblower may not be disclosed, where the contestation of the relevant charge is based on separated investigations and additional to the Report (even if consequent to it). If the charge is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is essential for the defense of the accused, the Whistleblower's Report will be usable for the purposes of disciplinary proceedings only if the Whistleblower expressly consents to the disclosure of his/her identity.

1.1. Protection of the confidentiality of the identity of other parties

It is also protected the confidentiality of the identity:

a. Of the person concerned.
b. Of the facilitator, i.e., the person who assists the Whistleblower in the reporting process and who operates within the same work context (confidentiality must be guaranteed both regarding identity and with reference to the activity in which the assistance takes place).
c. Of persons different from the person concerned but mentioned in the Report (e.g., witnesses).

2. Protection from retaliation

Retaliation may consist of: suspension, lay-off, dismissal or equivalent measures; demotion or withholding of promotion; transfer of duties, change of location of place of work, reduction in wages, change in working hours; withholding of training; a negative performance assessment or

employment reference; imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; coercion, intimidation, harassment or ostracism; discrimination, disadvantageous or unfair treatment; failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment; failure to renew, or early termination of, a temporary employment contract; harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry; early termination or cancellation of a contract for goods or services; cancellation of a license or permit; request for submission to psychiatric or medical examinations.

The above list of retaliatory measures is not exhaustive: in fact, 'retaliation' should be considered all those instances that directly or indirectly cause or are likely to cause unfair harm to the person.

Individuals who are protected from possible retaliation, even if only attempted or threatened, include:

a. Whistleblower.
b. Facilitators.
c. Persons in the same work environment with stable emotional or kinship ties within the fourth degree with the Whistleblower.
d. Colleagues working in the same work context who have a regular and current relationship with the Whistleblower.
e. Entities owned or operating in the same work context as the Whistleblower or in which the latter works.

To be protected from retaliation, the following conditions must be met:

- The Whistleblower reported based on the reasonable belief that the information about the breaches was true and within the range of the reportable ones, as clarified in paragraph '**Art. 5 – Subject of the Report**'.

- The Report was made in compliance with the discipline provided within the Regulation.
- There is a cause-and-effect relationship between the Report made and the retaliation suffered; the burden of proof on the causal relationship shifts depending on the person who complains of retaliation and/or harm: if the Whistleblower proves that the Report was made and that retaliation was suffered as a result, the burden shifts to the person who perpetrated the alleged retaliation; conversely, the burden of proof shifts to all other persons, other than the Whistleblower, who enjoy the protections against retaliation listed above.

3. **Limitations of liability with respect to disclosure and dissemination of some categories of information**

   In addition to the protections listed above, the legislator has provided, as a further form of safeguard, for the limitation of the Whistleblower's liability in respect of the disclosure and dissemination of certain categories of information covered by official, professional, scientific and industrial secrecy, or which, if disclosed, would constitute an infringement relating to the protection of copyright, personal data, or which would offend the reputation of the person concerned.

   For this protection to be effective, two conditions must be met:

   - At the time of the collection or dissemination of the information, the Whistleblower has reasonable grounds to believe that it is necessary to disclose the breach; and
   - The Report was made in accordance with the rules and Applicable Legislation.

Art. 9 – Internal reporting channels

The Company has implemented the internal channels listed below, through which Reports of breaches under '**Art. 5 – Subject of the Report**' can be submitted.

The Whistleblower is free to choose from:

- **Written mode**: The Company has opted for the use of an IT platform to receive and manage Reports (hereinafter, '**Platform**'), which, by means of a questionnaire, guides the Whistleblower

in the filling in of all information that must be provided, with the possibility to attach any document and to remove metadata from them, in order to guarantee (through the use of encryption tools) the confidentiality of the identity of the Whistleblower, the person concerned and the persons in any case mentioned in the Report, as well as the content of the same and of the related documentation, thus resulting in compliance with the provisions of the Applicable Legislation.

- **Oral mode**: also, through the Platform, it is possible to send a Report by recording an audio (with a smartphone or pc) through the voice messaging system integrated within it. The Whistleblower can choose to distort the voice and remove metadata from the audio file, consistent with the principle of confidentiality protection.
- **Oral mode in person**: by means of a face-to-face meeting with the Handler (at the request of the Whistleblower), who ensures that the meeting can be held within a reasonable time.

In any case, once the Report has been sent (in any mode), the Whistleblower will receive a password automatically generated by the Platform, which he/she will need to access later in order to follow the case, see any updates and, if necessary, communicate with the Handler.

Art. 10 – Handler of internal reporting channels

Management of internal reporting channels is entrusted to Mrs. Marcella Caradonna – supervisory body of the Company under Italian Legislative Decree no. 231 of June 8, 2001 (hereinafter, '**Supervisory Body**').

The Company ensures that its appointed Handler meets all the requirements of the Applicable Legislation; in particular, the Company has:

- Assessed that this is a profile endowed with autonomy.
- Expressly appointed the Handler as individual authorized to process personal data, giving specific instructions regarding the processing that can be carried out.
- Delivered specific training on whistleblowing and personal data protection.

Art. 11 – Report management

Upon receipt of the Report through the relevant internal channels, the Handler must:

1. **Release acknowledgement to the Whistleblower within seven (7) calendar days from the date of receipt of the Report**; such acknowledgement does not imply any evaluation of the contents that are the subject of the same but is solely for the purpose of informing the Whistleblower that it has been properly received. Such notice shall be forwarded to the address indicated by the Whistleblower at the time of submission of the Report.
2. **Maintain communication with the Whistleblower** to request any necessary additional information in order to properly handle the Report.
3. **Diligently follow up on the Report**, i.e., assess processability, admissibility and merits; specifically:
    a. In terms of processability, the Handler verifies the existence of the subjective and objective prerequisites provided for in the Applicable Legislation, in order to ascertain that the Whistleblower falls within the scope of the subjects entitled to make the Report (see '**Art. 4 – Individuals who can make Reports'**) and that the related subject falls within the scope of the Applicable Legislation (see '**Art. 5 – of the Report**'). If the Report does not fall within the scope of application, it may be treated as ordinary. For eligibility purposes, however, it will be necessary for the Report to contain all the required elements, as outlined in '**Art. 6 - Content of the Report**'.

    A Report is deemed inadmissible when:

    - Factual elements attributable to the reportable breaches are missing or manifestly unfounded.
    - The statement of facts is generic and does not allow understanding of what happened and/or the identification of the person to whom the breach is attributed.
    - Only documentation is produced without an actual Report being made.

    If the Report is found to be improper or inadmissible, the Handler proceeds with the filing, recording the reasons supporting the choice made.

    b. After confirming the admissibility of the Report, the Handler will proceed to verify its merits by carrying out all appropriate activities, including personal interviews with the

Whistleblower and any other persons who can provide information on the reported facts, in accordance with the principles of impartiality and confidentiality. The goal is to analyze and evaluate reported facts to determine whether corrective actions are necessary to improve the internal control system for the business areas and processes involved.

During this phase, the Handler may seek support and cooperation from the appropriate corporate structures. If necessary, it may also involve internal or external individuals (such as experts or consultants), who have been specifically appointed as data processing authorizations/processors. It is important to always maintain the confidentiality of the Whistleblower's identity, the reported person, and the content of the Report and relevant documentation.

4. **Provide acknowledgement to the Whistleblower within three (3) months from the date of the acknowledgement of receipt** or, if such an acknowledgement has not been issued due to lack of knowledge of the identity and/or contact details of the Whistleblower or if there are other obstructive causes, within three (3) months from the expiration of the 7-day period provided for issuing the acknowledgement of receipt of the Report. The assessment activity does not necessarily have to close within three (3) months: in fact, the completion of the checks may take longer; therefore, after this period has elapsed, the Handler may notify the Whistleblower:
   - The dismissal.
   - The initiation of an internal investigation and its findings.
   - The steps taken to address the reported facts.
   - Information regarding the activities to be undertaken and the progress of the investigation (in the latter case, once the activity is completed, it must also communicate the results to the Whistleblower).

If at the outcome of the verification the Report proves to be well-founded, the Handler will forward it to those responsible for assessing any responsibility profiles, pursuant to the disciplinary system adopted within the MOG.

Art. 12 – Report sent to party other than the Handler

If the Report is submitted to an entity other than the Handler and the Whistleblower explicitly states that it wishes to benefit from the protection offered by the Applicable Legislation (or this intention can be inferred from the Report), the non-competent entity receiving the Report must forward it to the Handler within seven (7) days of its receipt, without sending copies to any other entity, and at the same time inform the Whistleblower. The operation must be carried out while maintaining the confidentiality of the identities of the person concerned and of any other person mentioned in the Report, as well as of the contents of the latter and its supporting documents.

Art. 13 – External reporting channels

Provision is made for the possibility of submitting a Report through external channels, limited to breaches of the provisions of the law of the EU, as set out in paragraph '**Art. 5 – Subject of the Report**'; the competent authority for activating and managing these channels is the ANAC, which guarantees, also through the use of encryption tools, the confidentiality of the identity of the Whistleblower, of the person concerned and of the person mentioned in the Report, as well as of the content of the latter and of the related documentation, including through the use of encryption tools.

Access to external channels is only allowed when one of the following conditions is met:

1. Internal channels are not active or do not comply with the Applicable Legislation.
2. The internal Report produced has not been followed up.
3. The Whistleblower believes that an internal Report will not be effectively followed up or may result in a risk of retaliation.
4. The Whistleblower has reasonable grounds to believe that the breach may pose an imminent or obvious danger to the public interest.

ANAC acquires external Report through the channels specifically set up:

- IT platform.

- Oral telephone Reports.
- Oral communications in person (face-to-face meetings set within a reasonable time).

The platform implemented by ANAC allows, in a computerized way, the compilation, sending and receiving of the Report form, the management of the investigation and the possible forwarding to other competent authorities; this tool uses encryption mechanisms that guarantee the technological security of the reporting process while keeping all the data contained therein confidential. In fact, the data of the Whistleblower are obscured and segregated in a special section of the platform, so that they are inaccessible even to the investigating office of ANAC. The platform allows the identification of each Report received by assigning a unique progressive code to it. On ANAC's institutional website, clicking on the link to the dedicated page provides access to the service dedicated to whistleblowing (here is the link[1]). The Whistleblower can freely access the appropriate section of the ANAC platform without prior authentication; in this area he/she views the Report form to be completed and submitted. This includes a part called 'identity' that he/she will have to fill in to sign the Report. As anticipated, the data entered in this section is subject to obscuration and therefore not accessible to those who will handle the investigation.

With regard to oral Reports, ANAC has set up a telephone service with an operator that enables their acquisition; specifically, the operator:

- Receives the Report by telephone.
- Enters it on the platform along with the audio file related to the recording of the telephone call.
- Upon completion of the entry of the Report, it acquires from the platform the unique 16-character alphanumeric identification code (key code) that it transfers contextually (during the phone call) and orally to the Whistleblower.

The last tool made available by ANAC, on the other hand, concerns the acquisition of the Report by direct meeting through an operator who enters the data in the IT platform, similarly to what is

[1] https://www.anticorruzione.it/-/whistleblowing

provided for oral Reports.

For more information regarding the external channel, please refer to the ANAC GUIDELINES available at the following link[2].

Art. 14 – Public disclosure

Another way to report breaches of EU law, as outlined in paragraph '**Art. 5 – of the Report**', is through public disclosure: in such a case, information on breaches shall be placed in the public domain through print or electronic media or, otherwise, through means of dissemination capable of reaching a large number of people.

The conditions for making a public disclosure are as follows:

- The Whistleblower has previously made an internal Report to which the Company has not provided a response within the prescribed time limit, and which has been followed by an external Report to ANAC (or the Whistleblower has directly made a Report to ANAC) which, in turn, has not provided feedback to the Whistleblower within reasonable time limits.
- The Whistleblower believes that the breach poses an imminent or obvious danger to the public interest.
- The Whistleblower believes that the external Report may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the particular case (e.g., evidence may be concealed or destroyed, or there is a well-founded fear that the Handler may plot with the reported person or be involved in the breach).

Art. 15 – Complaint to the judicial authority

Individuals protected by the Applicable Legislation, as defined in paragraph '**Art.** Error! Reference source not found. **-** Error! Reference source not found.', section 2 '**Error! Reference source not found.**', may file a complaint with the competent judicial authorities, regarding a breach of EU law (as defined in paragraph '**Art. 5 – of the Report**') of which they have become aware in the course of their work.

[2] https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing

The offices of the judicial authorities, to which the complaint is made, must also adhere to the aforementioned rules on confidentiality protection.

Art. 16 – Data protection compliance

The Company is committed to complying with and implementing the obligations set forth in the Applicable Legislation: therefore, it has taken steps to supplement its privacy document system as follows (with respect to the processing carried out in the context of the management of Reports):

- A specific privacy notice (as required by Articles 13 and 14 of the General Data Protection Regulation (EU) 2016/679, so-called '**GDPR**') for all data subjects has been prepared and published on the Platform.
- The record of processing activities has been updated, pursuant to Article 30 GDPR.
- The Data Protection Impact Assessment (so-called '**DPIA**') has been carried out.
- The Handler has been expressly appointed as the person authorized to process personal data.
- A specific training on data protection and whistleblowing to the Handler has been carried out.
- The Platform provider has been appointed as data processor under Article 28 GDPR.

Where the Handler relies on the collaboration of additional parties (internal and/or external) to carry out the activities inherent to the management of Reports, and where it is not possible to maintain complete confidentiality regarding the information contained therein, the Company must proceed to appoint such parties as authorized persons (pursuant to Art. 29 GDPR) or data processors (pursuant to Art. 28 GDPR), depending on whether the relevant parties are internal or external.
In order to ensure the proper performance of the assigned role, each of the authorized persons is adequately trained with regard to the GDPR and the obligations applicable to the whistleblowing area; in addition, they have been required to sign a confidentiality obligation aimed at safeguarding the secrecy of the information they may become aware of in the performance of their duties.

Art. 17 - Penalties

Failure to comply with the provisions of the Regulation may result in disciplinary sanctions, as outlined

within the MOG, to which reference is made.

Pursuant to Legislative Decree no. 24 of March 10, 2023, ANAC may apply an administrative fine of 10,000 to 50,000 euros to:

- ✓ The natural person who: (i) has committed retaliation, (ii) obstructs, or attempts to obstruct, the Report, or (iii) has violated the obligation of confidentiality of the identity of the Whistleblower; on this subject it should be noted that the penalties applicable by the territorially competent data protection supervisory authority for the profiles of competence remain unaffected.
- ✓ The Handler, in case of failure to carry out the verification and analysis activities of the Reports received.
- ✓ The Company's governing body, if (i) internal reporting channels are not established, (ii) a procedure for making and handling Reports has not been adopted or has been adopted but does not comply with the provisions of the Applicable Legislation.
- ✓ The person who, as a result of the inspections, is found to be guilty of the facts that are the subject of the Report or otherwise of established breaches.

ANAC may apply an administrative fine of 500 to 2,500 euros to the Whistleblower who makes with malice or gross negligence Reports that turn out to be unfounded. On this issue, it is noted that the criminal and disciplinary liability of the same is left unaffected in the event of libelous or defamatory reporting under the Italian Penal Code and Civil Code.

Lastly, if the outcome of the verifications carried out as a result of the Report reveals foundational elements regarding the commission of an unlawful act by an employee, the Company may file a complaint with the judicial authorities. Similarly, if the results of the verifications carried out have revealed unlawful behavior by a third party (e.g., a supplier), the Company may proceed with suspension/deletion from the Company rolls, without prejudice to any further powers provided for by law and by contract.

Art. 18 - Reporting

In the presence of Reports, the Supervisory Body prepares an annual report to be submitted to the Board of Directors and the Board of Statutory Auditors on the Reports received and the progress of verification activities. Similarly, the Company updates the Supervisory Body on all Reports having even marginal impact on the Code of Ethics and the MOG.

Art. 19 – Company's activities

The Company ensures that specific communications and information are sent to all internal staff on the institution of whistleblowing, on the Regulation and on any other relevant and useful information in order to inform and raise awareness on the purposes of this institution, on the protections offered and on the procedures for submitting and managing Reports.