

## ETHICS AND COMPLIANCE

Secondo Mona designs and manufactures on-board systems and equipment for civil and military, fixed-wing and rotary-wing aircraft.

The achievement of the company's objectives is pursued, by all those involved, with loyalty, seriousness, honesty, competence and transparency, in absolute compliance with applicable laws and regulations.

The Company increasingly values, in addition to the economic result, aspects such as: quality, independence, reliability and reputation to be understood also in terms of ethical and social responsibility.

To this end, it has adopted the Organization, Management and Control Model pursuant to Legislative Decree 231/01 and the Code of Ethics.

The adequacy and effectiveness of the Code of Ethics and the Model depend, among other things, on the existence of an effective system for detecting unlawful conduct and violations that allows any transgressions to be brought to light.

Implementing this profile was first the Law 179/2017 laying down provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship (so-called whistleblowing), and most recently Legislative Decree 24/2023, with which Italy implemented Directive (EU) 2019/1937 of the European Parliament and of the Council concerning the protection of persons who report violations of Union law and/or violations of national regulatory provisions.

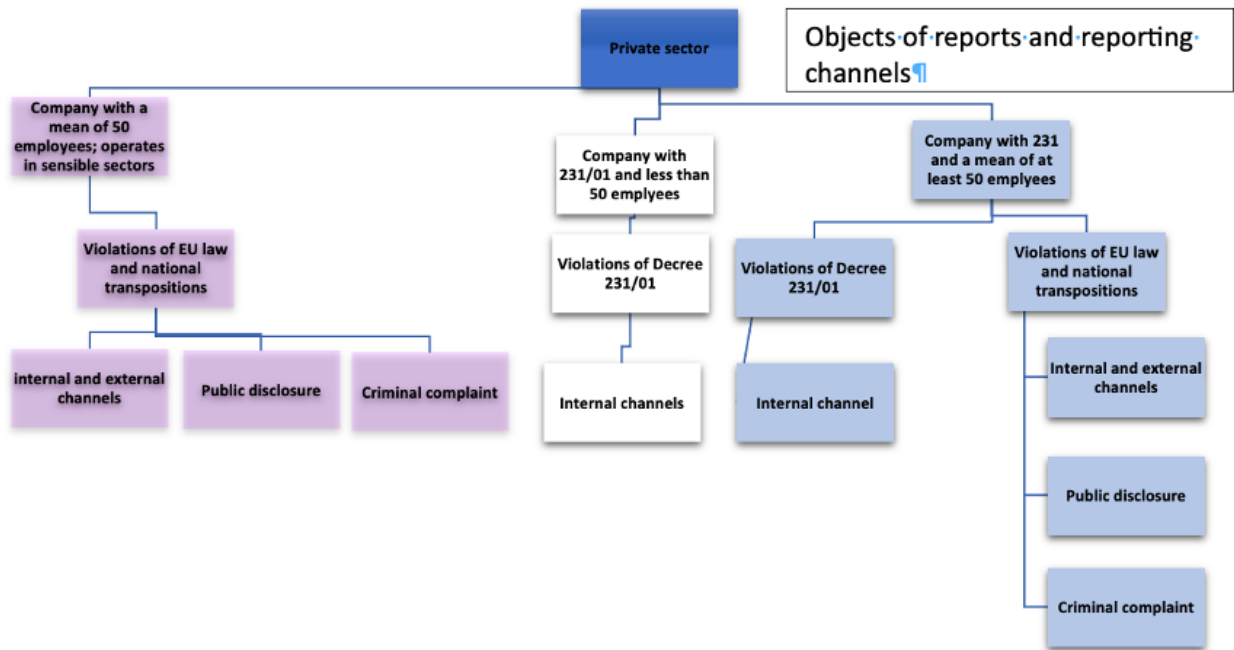
In more detail, Legislative Decree 24/2023 stipulates that the Model must contain requirements regarding, among others:

- ✓ to internal reporting channels;
- ✓ to external reporting channels;
- ✓ to the prohibitions of retaliation;
- ✓ to the provision of an appropriate disciplinary system to punish non-compliance with the measures indicated in the Model.

Secondo Mona has equipped itself with appropriate tools to collect reports, including anonymous ones, coming from inside or outside the company and relating to facts likely to integrate the commission of administrative, accounting, civil or criminal offenses, unlawful conduct relevant under Legislative Decree 231/2001, violations of the Organizational Model, acts or omissions that harm the financial interests of the European Union or concerning the internal market.

The scope of the subject of the report varies depending on the type of subject involved. With specific reference to the private sector, the regulations have been summarized by the Guidelines for External Reporting adopted by ANAC on July 12, 2023 and the Guidelines adopted by Confindustria on October 27, 2023, as follows:

## Private Sector



Given the private nature of the entity and the presence of at least 50 employees, **Secondo Mona is therefore required to implement an internal channel for reports relating not only to violations of Legislative Decree 231/2001 and this Organizational Model, but also to violations of EU law and national transposing legislation**. An external channel is also established at ANAC (National Anti-Corruption Authority) for reporting the latter, and in such cases the reporter may also resort to **public disclosure** or **whistleblowing**.

### Form and content of reporting

Reports may be made **in written form (including by computer) or in oral form**.

A **report** means any communication, even anonymous, having as its object the description of conduct (active or omissive), referable to members of the administrative and control bodies, personnel (managers, executives and employees) and third parties, with respect to which there is reasonable suspicion or awareness that they are illegal or carried out in violation of the Code of Ethics, the Model, the company's internal regulations or the compliance procedures and/or standards relevant under Legislative Decree 231/2001.

**Reports must be substantiated and based on factual, precise and concordant evidence.**

Specifically, also for the purpose of eligibility screening, the following **essential elements of the report** must be clear:

- identification data of the reporting person (name, surname, place and date of birth), as well as an address to which subsequent updates should be communicated;
- circumstances of time and place in which the reported fact occurred, i.e., description of the facts that are the subject of the report, with specification of details regarding the circumstantial news and - where possible - the manner in which the reporting person became aware of the facts that are the subject of the report;
- generalities or other elements that make it possible to identify the person to whom the reported facts are attributed.

It is also helpful to attach documents that may provide evidence of the facts being reported, as well as to name other individuals with potential knowledge of the facts.

In the case of reporting by **regular mail (infra)**, it is also appropriate for the reporter to expressly indicate that he or she wishes to benefit from whistleblowing protections (e.g., by inserting the words "confidential to the reporting manager").

Excluded from the scope of reporting are:

- disputes, claims or requests related to a personal interest of the whistleblower that relates exclusively to his or her employment relationship or that pertains to working relationships with hierarchically superior figures (e.g., labor disputes, discrimination, interpersonal conflicts between colleagues, reports on data processing carried out in the context of the individual employment relationship in the absence of an injury to the public interest or the integrity of the private entity or public administration). Allegations excluded because they relate to a personal interest of the reporter are, therefore, not considered whistleblowing reports;
- in matters of national security and defense;
- disclosures related to violations already mandatorily regulated in certain special sectors, to which the ad hoc whistleblowing regulations therefore continue to apply (financial services, money laundering prevention, terrorism, transportation safety, environmental protection).

Reports that are NOT considered whistleblowing may be forwarded to the Supervisory Board at the following alternative contact details:

- **electronic mail** via the Supervisory Board's e.mail address: [odv@secondomona.com](mailto:odv@secondomona.com)
- **ordinary mail** to the address of the Company's registered office (via C. del Prete, 1 - 21019 Somma Lombardo (VA)) for the attention of the Supervisory Board.

#### Recipients of the discipline

It is incumbent on **all members of the Company**, apical and non-apical, and **on third parties who operate, in any capacity, on behalf of or in the interest of the Company**, the obligation to report violations - even if only "suspected" - of the Model and operating procedures of which they become aware, under penalty of disciplinary sanctions.

The report can therefore be made by **any person who has acquired information about potential wrongdoing within the work context**, including but not limited to employees, collaborators, members of the administrative, management or supervisory body, volunteers, trainees, contractors and subcontractors,

suppliers, former employees with terminated employment, if the information has been acquired during its conduct, or candidates not yet hired, if information on violations was acquired during the selection or other pre-contractual stages.

### Protected Subjects

The whistleblowing provisions protect the following individuals:

- employees of the Company;
- self-employed workers and holders of a collaborative relationship who perform their work activities at the Company;
- workers and collaborators who perform their work activities at entities that provide goods or services or perform works in favor of the Company;
- freelancers and consultants who perform their work for the Company;
- any volunteers and trainees, paid and unpaid, who perform their activities at the Company;
- persons with functions of administration, management, control, supervision or representation of the Company, even if such functions are exercised on a mere de facto basis, such as members of the Board of Directors, the Board of Statutory Auditors and the Supervisory Board.

The protection of reporting persons referred to in the preceding paragraph also applies:

- when the legal relationship does not yet appear to have begun, if information on violations was acquired during the selection process or other pre-contractual stages;
- during the probationary period;
- after the dissolution of the legal relationship, if information on violations was nevertheless acquired during the course of the said relationship.

The protective measures in this Procedure also apply:

- to facilitators, understood as the physical persons who assist a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- to persons in the same work context as the reporter or related to them by a stable emotional or kinship link within the fourth degree;
- to co-workers of the reporter who have a regular and current relationship with the reporter.

### **Internal reporting channel**

#### Designation of the person in charge

The Company identifies the person responsible for establishing, implementing, managing and monitoring the internal whistleblowing channel (hereinafter referred to as "**Whistleblowing Manager**") **as the internal**

**member of the Supervisory Board**, which is endowed with autonomy and specifically and adequately trained in the handling of reports.

The Company, on the one hand, is committed to guaranteeing the autonomy and independence of the Whistleblowing Manager and, on the other hand, the latter has the duty to ensure at all times that he or she is placed in a position to carry out investigations and, in general, his or her tasks autonomously with respect to other corporate functions, that he or she is not subject to interference of any kind in the performance of the same and that he or she has all the personal and material resources necessary to carry them out. Therefore, in the event that the report itself or the subsequent investigation reveals elements such as to suggest that a conflict of interest - even if only potential - exists with the Whistleblowing Manager, he/she will be required to refrain from any further activity related to that report.

Conflict of interest may exist if the Whistleblowing Manager coincides with the whistleblower, the reported person, or is otherwise a person involved or affected by the report.

**In such situations, the report is addressed to the Chairman of the Supervisory Board**, who is required to comply with the obligation of confidentiality under the regulations.

#### Establishment of the reporting channel

The Company adapts its reporting channel to the standards prescribed by current regulations, so as to make it accessible not only to employees but also to all additional stakeholders, such as suppliers and acquired or potential customers, as well as to ensure the confidentiality of the identity of the reporter, the person mentioned in the report and the contents of the report, in the terms detailed below.

Reports can be made:

- **in writing** by **regular mail** to the address.

Dr. Cinzia Petroni  
c/o Secondo Mona s.p.a.  
Via Carlo del Prete, 1  
21019 - Somma Lombardo (VA)

In such a case, the report must be placed in two sealed envelopes, including in the first the identifying data of the reporter, together with an identity document, and in the second the subject of the report. Both envelopes should be placed in a third envelope with the words "**confidential to the reporting manager**" on the outside.

- **orally**, through a **dedicated telephone line having the number 3499881993, active h24 7/7, in exclusive use of the Manager**, or, by **appointment**, through in-person meeting or simultaneous audio-video remote communication.

As for the implementation of the **telephone line**, since it is an **unrecorded** telephone call, upon receipt of the report, the Manager must document it by means of a detailed account of the message, and the content must be countersigned by the reporter, subject to verification and possible rectification, through modes of sending and sharing that will be agreed by the latter with the Manager. A copy of the signed report must be provided to the reporter.

As indicated above, it is clarified that it is the whistleblower's option to use this channel as the first point of contact to request an **appointment**, so that the former can report the report orally in person or, upon agreement, also remotely via online video communication platforms.

If the whistleblower makes a request for oral reporting by **meeting**, the Whistleblowing Manager shall arrange an appointment within fifteen days so that the former can report the report in person or, upon agreement, also remotely via online video communication platforms. In the case of deferred oral reporting:

- a suitable place is identified to ensure the confidentiality of the reporter;
- the reporter is warned that the conversation will be recorded;
- if the whistleblower objects to the recording, the Whistleblowing Manager will prepare an appropriate record, signed by the whistleblower, to whom a copy will be given;
- the whistleblower will have the opportunity to verify, rectify and accept with signature the transcript of the conversation.

#### **References to the reporting channel adopted are published on the Company's website.**

In the event that the reporter prefers not to reveal his or her identity, he or she may make an **anonymous report**. In this case, it will still be necessary to identify the persons involved in the reported facts, in order to ensure that the investigation resulting from the report is as effective as possible. In any case, anonymous reports must be recorded by the Whistleblowing Manager and the documentation received must be retained; where the anonymous whistleblower is subsequently identified and has suffered retaliation, the whistleblower must be guaranteed the protections provided for the whistleblower. Therefore, the Whistleblowing Manager shall ensure that strictest confidentiality is observed even in such cases.

#### **Handling of whistleblowing**

According to the provisions of Article 5 of Legislative Decree 24/2023, once the report is received, the Whistleblowing Manager:

- a. issues an **acknowledgement of receipt** to the whistleblower within seven days of receipt of the report, unless anonymous reports with reference to which it is in no way possible to identify and/or establish a channel of communication with the whistleblower (i.e. anonymous report by mail in which no address is given to which any necessary communication should be sent);

- b. maintains **interlocutions with the reporter** and, if necessary, requests **additions** from the reporter;
- c. diligently **follows up on the reports received**;
- d. provides an **acknowledgement** of the report within three months from the date of the notice of receipt or, in the absence of such notice, within three months from the expiration of the seven-day period from the submission of the report. In cases of particular complexity, within the aforementioned deadline the Whistleblowing Manager shall inform the whistleblower that the investigation is still in progress.

The Whistleblowing Manager is also required to give notice of the report to the other members of the Supervisory Board.

With specific reference to point c), the Whistleblowing Manager assesses, also on the basis of any documentary analysis, the existence of the prerequisites for the start of the next investigative phase, resulting in:

- **initiation of the investigation stage**, in the case of admissibility of the report;
- **closing of the report**, in the case of inadmissibility of the report, with specific indication of the reason.

For **admissibility**, it is necessary for the report to be clear :

- the **circumstances of time and place** in which the fact that is the subject of the report occurred, by means of a description of the facts that are the subject of the report that contains details of the circumstantial news and, if any, the manner in which the reporter became aware of the facts;
- **personal details** or **other elements** that enable the identification of the person to whom the reported facts are attributed.

Conversely, the report is deemed **inadmissible** in case of:

- lack of data constituting the essential elements of the report;
- manifest groundlessness of the factual elements attributable to the violations typified by the legislator;
- exposition of facts of generic content such that they do not allow the Whistleblowing Manager to understand them;
- production of only documentation without the actual reporting of violations.

In the event that the Whistleblowing Manager decides not to initiate the investigation phase, he or she shall inform the whistleblower within three months from the date of the notice of receipt or, in the absence of such notice, within three months from the expiration of the seven-day period from the submission of the report. In cases where the reporter cannot be contacted due to anonymous reporting, it shall close the file.

Reports that are closed as manifestly unfounded, even if anonymous, are immediately forwarded to the SB and, except in the case of anonymous reports, also to the HR Manager so that he/she may assess whether the reports were made for the sole purpose of damaging the reputation or otherwise to cause injury to the

reported person and/or Company, in which case disciplinary proceedings will be initiated.

### Conduct of the preliminary investigation

During the investigation phase, the Whistleblowing Manager:

- proceeds to specific investigations and analyses aimed at verifying the reasonable grounds for the reported violation;
- reconstructs the management and decision-making processes, followed on the basis of the documentation and additional elements it deems necessary;
- requests any additions or clarifications from the reporter;
- acquires any information from the corporate structures concerned and the persons involved in the report, who may ask to be heard as well as to produce written comments or documents;
- acquires any information from the persons involved in the report, including persons to whom the report attributes responsibility for the reported violations. Such persons must be involved at the appropriate time and in the appropriate manner to ensure the proper conduct of the investigation, and have the right to be heard as well as to produce written comments or documents. In the event that they are heard orally, such persons shall be advised that the conversation will be recorded or reported in appropriate minutes, which the registrant will have the opportunity to verify, rectify and accept by signature, but without receiving a copy;
- elaborates any indications regarding the adoption of the necessary remedial actions aimed at correcting possible control deficiencies, anomalies or irregularities detected on the company areas and processes examined.

Should technical expertise not possessed by the Whistleblowing Manager be necessary or even appropriate for the analysis and proper handling of the report, the latter has the right to be assisted by external consultants of proven experience and professionalism. These external consultants, as well as all persons involved in the investigative activity, are also bound, after specific warning by the Whistleblowing Manager and possible signing of appropriate documents, to confidentiality obligations better detailed below.

In any case, if it proves necessary to make use of the technical assistance of third-party professionals, as well as the specialized support of the personnel of other company functions, the Whistleblowing Manager is required to obscure any type of data that may allow the identification of the whistleblower or any other person involved, unless it is data necessary for the investigation conducted by such persons.

It is understood that the scope of analysis of the investigation does not include, except to the extent of manifest unreasonableness, discretionary or technical-discretionary evaluations of merit or opportunity of the decision-making and management aspects made by the various corporate functions.

All stages of the investigative activity must be tracked and archived, depending on the type of reporting channel used.



### Closing of the investigation

Once the investigation is completed and a decision on its outcome is made, **the reporter is informed of the outcome of the investigation or the need to continue the investigation**. In the latter case, the reporter is subsequently informed of the actual closure of the investigation and its outcome.

With specific reference to the nature of this information, the Whistleblowing Manager shall indicate to the whistleblower that the report (a) has been dismissed as it is deemed unfounded; or (b) has been brought to the attention of the competent bodies of the Company, together with all the elements and indications necessary for them to take the appropriate measures.

**In fact, the Whistleblowing Manager is not responsible for any assessment regarding individual responsibilities and any subsequent measures and/or consequent proceedings.**

At the conclusion of each investigative activity, after following up the communication to the whistleblower and having, if necessary, spoken with the reported person or evaluated the written comments submitted by the latter, **the Whistleblowing Manager prepares a report intended for the Company's Board of Directors and the Supervisory Board** in which are stated:

- the precise description of the reported facts and the individuals involved;
- the facts established as a result of the investigation activities and the manner in which the investigation was carried out;
- the evidence gathered, including recordings of the hearings, any testimonies taken in writing or minutes of the hearings as well as any other relevant documentation;
- the conclusions reached at the outcome of the investigative activities and therefore (a) an indication of the hypotheses of non-compliance with provisions, procedures or facts of relevance from a disciplinary or labor law perspective, as well as (b) any observations and indications regarding the necessary corrective actions to be taken.

**The details of the reporter or other elements that would allow his or her identification are not given, unless he or she explicitly agrees.**

### Good faith of reports

#### **Reports must be made in good faith.**

Bona fide reporters are those who report or disclose violations with the reasonable belief that the information reported is true or has been provided in accordance with the requirements of Legislative Decree 24/2023 and this procedure.

### Transmission of the report

Anyone who receives in any form a report that can be qualified as whistleblowing (e.g., is explicitly marked "whistleblowing" on the envelope, in the subject line, or in the text of the communication) is required to transmit the original, together with any supporting documentation, to the Whistleblowing Manager within

seven days of receipt through the reporting channels described above and to give simultaneous notice of the transmission to the whistleblower, if known.

The person receiving the report:

- Is prohibited from retaining hard copies of the same;
- Is obliged to delete any digital copies;
- Is prohibited from taking any independent initiative to analyze or investigate the same;
- It is obligatory to maintain the confidentiality of the identity of the reporter, the persons involved or otherwise mentioned in the report, the content of the report and the related documentation.

**Failure to report as well as violation of the obligation of confidentiality may result in the adoption of disciplinary measures provided for in this Model.**

#### Information and awareness-raising

In order to ensure the proper and efficient functioning of the whistleblowing system, it is necessary to promote a whistleblowing culture in the Company.

To this end, the Company provides, through appropriate training activities, to inform and raise awareness among employees about the whistleblowing system adopted, defining in a simple and understandable way the purposes and methods of using the internal channel.

#### **External signaling channel**

With reference only to violations of EU law and national transposition legislation, pursuant to art. 6 of Legislative Decree 24/2023, the reporter can also make an external report through the appropriate channel activated by ANAC if, at the time of its submission, one of the following conditions occurs:

- a. the mandatory activation of the internal reporting channel is not envisaged within his/her work context or this, even if mandatory, is not active or, even if activated, does not comply with the provisions of the art. 4 of the Decree;
- b. the reporting person has already made an internal report and it has not been followed up on;
- c. the reporting person has well-founded reasons to believe that, if he/she made an internal report, it would not be followed up effectively or that the same report could lead to the risk of retaliation, if these are reasons based on concrete circumstances which must be attached to the report and on information that can actually be acquired;
- d. the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

ANAC has regulated in its Guidelines and in a special Regulation how external reports should be submitted and handled.

With regard to the mode of submission, reports can be made:

- a. through an **IT platform**, which is outlined as a priority reporting channel as it is considered most appropriate to ensure the confidentiality of the reporter and the report;
- b. orally, through an **operator-led telephone service**;
- c. through **face-to-face meetings**, for which a reasoned request is required, set within a reasonable period of time, following which the operator enters the report into the platform.

For **eligibility purposes**, the report must state:

- the name and contact details of the reporter;
- the facts being reported and the entity in which they occurred;
- the entity in whose work context the reporter operates and the professional profile held by the reporter;
- a summary description of how the reporter became aware of the reported facts.

The external report is considered **inadmissible** for the following reasons:

- manifest groundlessness due to the absence of factual elements referable to the violations typified in art. 2, co. 1, lett. a), of the Decree;
- manifest lack of legal prerequisites for the exercise of the Authority's supervisory powers;
- manifest lack of competence of the Authority on the matters reported;
- ascertained generic content of the external report, i.e., such that it does not allow the understanding of the facts, or external report accompanied by inappropriate, irrelevant documentation or otherwise such as to make the very content of the report incomprehensible;
- production of only documentation in the absence of the external report;
- lack of data that constitute essential elements of the external report; vii) existence of minor violations.

The direct link to the dedicated ANAC page is: <https://whistleblowing.anticorruzione.it/#/>

## **Public disclosure**

With reference only to violations of EU law and national transposing legislation, pursuant to Article 15 of Legislative Decree 24/2023, the reporter may also resort to the tool of public disclosure, that is, making information about violations publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people.

The reporter benefits from the protection provided by this procedure if, at the time of public disclosure, one of the following conditions is met:

- a. has made an internal and external report in advance or has made an external report directly and no response has been received within the prescribed time limits regarding the measures planned or taken to follow up the reports;
- b. has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest, considered as a situation of emergency or risk of irreversible harm, including to the physical safety of one or more persons, requiring that the violation be promptly disclosed with wide resonance to prevent its effects. The reason must be based on concrete circumstances that must be attached to the report and on information that can actually be acquired;
- c. has well-founded reason to believe that the external report may involve the risk of retaliation or may not be effectively followed up due to the specific circumstances of the concrete case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the person who received the report may be colluding with or involved in the perpetrator of the violation.

Where the person making a public disclosure discloses his or her identity, a confidentiality protection issue does not arise, without prejudice to the application of the additional protections provided by the Decree; if the same person uses a pseudonym or nickname, ANAC will treat the report in the same way as an anonymous report and will take care to record it, for preservation purposes, in order to guarantee the discloser, in the event of subsequent disclosure of his or her identity and actual retaliation, the protections provided.

### **Confidentiality and personal data protection**

The internal reporting channel must ensure **the confidentiality of the identity of the reporter and any other persons involved in the report**, as well as **the content of the report and related documentation**.

Any processing of personal data must be carried out in compliance with Regulation (EU) 2016/679, Legislative Decree 196/2003 and Legislative Decree 51/2018. In any case, the report is exempt from access provided for by articles 22 et seq. of Law 241/1990, as well as articles 5 et seq. of Legislative Decree 33/2013.

The processing of personal data will be carried out by the Whistleblowing Manager as the Data Controller for the sole purpose of implementing the procedures established in this Model and, therefore, for the proper handling of the reports received.

A statement on the processing of personal data is made and published on the Company's website.

Reports may not be used beyond what is strictly necessary to follow up on them. For this reason, personal data manifestly not useful for the processing of a specific report are not collected or, if accidentally collected, are deleted immediately.

The Whistleblowing Manager oversees compliance with measures, of an organizational and technical nature, aimed at guaranteeing the confidentiality of the whistleblower and the integrity and confidentiality of the reported data; he also guarantees the security of the reporting channel in terms of confidentiality, integrity and availability of information, both with respect to the reported data and the identity of the whistleblower, even in the event that the report should subsequently prove to be erroneous or unfounded.

Any kind of threat, retaliation, sanction or discrimination against the reporter and the reported person or those who have cooperated in the activities of verifying the merits of the report is not tolerated.

Without prejudice to legal obligations, the identity of the whistleblower and any other information from which the identity of the whistleblower may be inferred, directly or indirectly, may not be disclosed, without the whistleblower's express consent, to persons other than those responsible for receiving or following up the reports, who are expressly authorized to process such data pursuant to Articles 29 and 32, par. 4 of Regulation (EU) 2016/679 and Article 2 quaterdecies of Legislative Decree 196/2003.

For the pursuit of these objectives, the Whistleblowing Manager carries out, on an annual basis, risk analysis activities regarding the protection of personal data, also taking into account the time limit of five years, starting from the communication of the outcome of the procedure, for the preservation of the reported data.

The identity of the whistleblower and any other information from which such identity may be inferred, directly or indirectly, may be disclosed only with the whistleblower's express consent:

- within the framework of disciplinary proceedings, if the charge appears to be founded on the basis of the report and knowledge of the identity of the reporter is indispensable for the defense of the accused;
- within the framework of the proceedings established as a result of the report, if the disclosure of the identity of the reporter or any other information from which such identity may be inferred, directly or indirectly, appears indispensable also for the defense of the person involved.

The reasons for the disclosure of confidential data shall be communicated to the reporter in advance in writing. If the reporter denies his or her consent, the report may not be used in the disciplinary proceedings, which therefore may not be initiated or continued in the absence of further elements on which to base the charge.

In any case, the obligation to protect the reporter may be exceeded if:

- the reporter gives express consent to the disclosure of his/her identity;
- the identity of the whistleblower is to be disclosed to the Judicial Authority, the Public Prosecutor's Office or other competent authority as part of a criminal, disciplinary or discipline investigation;
- the criminal liability of the reporter for the crimes of slander or defamation or otherwise offenses committed with the report, or his civil liability in cases of willful misconduct or gross negligence, has been established by a judgment of first instance;
- anonymity is not enforceable by law and the identity of the reporter is required by the Judicial Authority.

The violation of the obligation of confidentiality may result in the imposition by ANAC of administrative fines, as well as the adoption of disciplinary measures under this Model against the person concerned.

## **Prohibition of retaliation**

**With respect to the whistleblower, retaliatory acts are prohibited**, to be understood as any behavior, act or omission, even if only attempted or threatened, carried out on account of the internal report that causes or may cause the whistleblower, directly or indirectly, unfair harm.

The prohibition of retaliation against the whistleblower includes a number of cases, including but not limited to:

- dismissal, suspension or equivalent measures;
- demotion in rank or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction on access to training;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanction, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavorable treatment;
- failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the worker had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- placement on improper lists on the basis of a formal or informal sector or industry agreement, which may result in the person's inability to find employment in the sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the cancellation of a license or permit;
- the request for submission to psychiatric or medical examinations.

The Company shall take appropriate action against anyone who engages in or threatens to engage in acts of retaliation against those who have submitted reports in accordance with the requirements set forth in this Model, without prejudice to the right of the assignees to legal protection in the event that criminal or civil liabilities related to the falsity of what has been stated or reported have been found against the reporter.

**Retaliatory acts that may have been taken because of the report are null and void, and persons who have been fired because of the report have the right to be reinstated in their jobs.**

ANAC is the authority responsible for receiving from the reporter and handling communications about alleged retaliation by the reporter.

In order for this form of protection to be recognized:

- the whistleblower, at the time of the report, denunciation to the judicial or accounting authorities or public disclosure, must have well-founded reason to believe the information to be true and within the scope of application of the discipline;
- the report, denunciation or disclosure must have been made in accordance with the discipline provided by Legislative Decree 24/2023 and this Procedure.

Eventuali ritorsioni derivanti dalla segnalazione costituiscono una violazione molto grave che può comportare l'irrogazione da parte di ANAC di sanzioni amministrative pecuniarie a carico della Società da 10.000 a 50.000 euro.

Without prejudice to the exclusive competence of ANAC regarding the possible application of administrative sanctions under Article 21 of Legislative Decree 24/2023, the Company may take the most appropriate disciplinary and/or legal measures to protect its rights, assets and image, against anyone who in bad faith has made false reports that are unfounded or opportunistic and for the sole purpose of defaming or causing prejudice to the reported person or other persons mentioned in the report.

On the other hand, it remains within the competence of the judicial authority to order the necessary measures to ensure the protection of the reporter (e.g., reinstatement in the workplace, compensation for damages, the order to cease the conduct, as well as the declaration of nullity of the acts adopted).

As already specified, the whistleblower loses protection:

- in case the criminal liability of the whistleblower for the crimes of defamation or slander is established, even by a judgment of first instance, or in case such crimes are committed by reporting to the judicial or accounting authority;
- in case of civil liability for the same title due to malice or gross negligence.

In these cases a disciplinary sanction is imposed on the whistleblower.

However, protection, even if delayed, must also be applied in the case of a first instance judgment not upheld in subsequent levels of judgment, dismissal, and ascertained slight misconduct.

### **Limitations of liability**

According to the provisions of Legislative Decree 24/2023, the whistleblower cannot be held accountable either criminally, civilly or administratively:

- Of disclosure and use of official secrecy (Article 326 of the Criminal Code);
- Of disclosure of professional secrecy (art. 622 of the Criminal Code);
- Of disclosure of scientific and industrial secrets (Article 623 of the Criminal Code);
- Of violation of the duty of loyalty and loyalty (Article 2105 of the Civil Code);
- Of violation of the provisions relating to the protection of copyright;
- Of violation of provisions relating to the protection of personal data;

- Of disclosure or dissemination of information about violations that offend the reputation of the person involved.

The above limitations on liability operate only if:

- at the time of the disclosure or dissemination there are reasonable grounds to believe that the information is necessary to disclose the reported violation;
- the report is made in compliance with the conditions provided for benefiting from the protection against retaliation (well-founded reasons for believing the facts reported to be true, the violation is among those that can be reported, and the terms and conditions of access to the report are complied with).

In any case, liability is not excluded for conduct that:

- are not related to the reporting;
- are not strictly necessary to disclose the violation;
- configure an acquisition of information or access to documents in an unlawful manner.

Where the acquisition takes the form of a crime (e.g., abusive access to a computer system or an act of hacking), criminal liability and any other civil, administrative and disciplinary liability of the reporter remains unaffected. Conversely, it is not punishable, for example, the extraction (for copying, photography, removal) of documents to which one had lawful access.

## Penalty system

**The disciplinary system provided by this Model also applies to those responsible for retaliation, obstruction (even if only attempted) of reporting, violation of confidentiality duties, failure to establish reporting channels, adoption of reporting procedures that do not comply with the provisions of Legislative Decree 24/2023.**

**The whistleblower may also report to ANAC the retaliation he or she believes he or she has suffered, and the latter, in the cases indicated in the previous points, is obliged to apply the following administrative pecuniary sanctions to the person responsible:**

- 10,000 to 50,000 euros, when it ascertains that retaliation has been committed, that the report has been obstructed or an attempt has been made to obstruct it, or that the obligation of confidentiality has been violated;
- 10,000 to 50,000 euros, when it ascertains that reporting channels have not been established, that procedures for making and handling reports have not been adopted, or that the adoption of such procedures does not comply with the regulations in force, as well as when it ascertains that the activity of verification and analysis of the reports received has not been carried out;
- from 500 to 2,500 euros, in the cases referred to in Article 16, paragraph 3 of Legislative Decree 24/2023, unless the reporting person has been convicted, even at first instance, for the crimes of defamation or slander or otherwise for the same crimes committed with the report to the judicial or accounting authority.





**Information pursuant to Articles 13 and 14 of Regulation (EU) 2016/679  
of the European Parliament and the European Council**

**Processing of personal data related to whistleblowing pursuant to Legislative Decree No. 24 of March 10, 2023, on the "implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law and on provisions regarding the protection of persons who report breaches of national laws (Whistleblowing Decree).**

**1. Whistleblowing reports mode of data retention.**

The management of both internal and external reporting channels is governed by the **MOG - Management and Control Organizational Model - General Part revision 4 of December 18, 2023.**

The data controller is SECONDO MONA S.p.A., based in Via Carlo del Prete, 1 - 21019 Somma Lombardo (VA), tel. 0331 756111 - e-mail address: hr-secondomona@pec.weblink.it, in the person of Dr. Claudia Mona.

The processing of personal data will be carried out by the Whistleblowing Manager for the sole purpose of implementing the procedures established in the aforementioned Model and, therefore, for the proper handling of reports receipts.

Internal Reports and related documentation are filed by the Whistleblowing Manager in special archives, paper and electronic, managed in a manner that ensures that only the Whistleblowing Manager can access them.

Internal Reports, the related documentation and the personal data contained therein are processed for the time necessary to follow up on the reports themselves and subsequently retained for the time determined from time to time by the Whistleblowing Manager in relation to the nature of the report and the consequent need to monitor the repetition over time of similar reports and/or assess the merits of related reports, in any case for no longer than five years from the date of the communication of the final outcome of the reporting procedure.

In the event that as a result of an Internal Report, the Company decides to initiate disciplinary proceedings or to initiate judicial or administrative proceedings or arbitration or conciliation proceedings, the Internal Reports and related documentation will be retained for a period of time equal to the duration of the **proceedings** or the period of limitation of the rights for the establishment of which, exercise or defense, retention becomes necessary, even if it exceeds the retention periods indicated above.

## 2. Protection Of Personal Data (ex art. 13 and 14 EU Reg. 2016/679) - Disclosure.

Given that this document already provides in its entirety detailed information on the purposes and methods of the processing of personal data resulting from the sending of an Internal Report and its subsequent management, in this paragraph are given more details and additional elements in compliance with the principle of transparency and guarantee of the interested parties and in accordance with the **Privacy Management System adopted by the company**.

The data processed, the provision of which by the data subject is obviously optional, may concern the Reporting Person and other individuals involved by the subject of the report and will consist of:

- data/documents provided by the Data Subject;
- data acquired from the later stages of the management of the report and necessary for its evaluation;
- data from public registers, lists, acts or documents knowable by anyone, always if necessary in reference to the provisions of this policy;
- other data from sources legitimately accessible in relation to the purposes pursued.

The processing operations in question may be carried out:

- insofar as necessary to pursue a legitimate interest of the Data Controller coinciding with the purposes of this document (to protect the integrity of the Company);
- insofar as necessary to assert or defend a right in court or to assess whether there is a right to be usefully protected in court;
- insofar as necessary to comply with obligations arising from laws, a regulation or EU legislation.

In addition to the individuals already mentioned above, data may be processed on behalf of the owners by:

- any auxiliaries of the Whistleblowing Manager;
- personnel assigned to verification, inspection, assessment, expertise and evaluation activities with the exclusion of consultation; personnel assigned to the maintenance of IT systems;
- subjects (companies/professionals, including outside the European Union where this is necessary in relation to the nature of the report or the subjects involved) who collaborate as Managers ex art. 28 Reg. EU 679/2016 to the activities, or who provide services functional to them, such as: legal advice and assistance, expert opinions, specialist advice, management of information systems, audits and investigative activities; in this regard, it should be noted that these subjects will always and in any case be bound to full compliance with the rules and procedures aimed at ensuring the widest protection and safeguarding of personal data adopted and imposed by the Data Controller also and not only in compliance with the regulations in force.

Personal data may be communicated or made available to:

- subjects indicated by the data subjects themselves;
- subjects involved in any judicial or disciplinary proceedings resulting from or related to the reporting in compliance with current regulations;
- to subjects who can access the data by virtue of a provision of law, regulation or EU legislation, within the limits provided for by these rules;
- judicial authorities, judicial police;
- subjects (Companies/professionals, also outside the European Union where this is necessary in relation to the nature of the fact reported and/or the subjects involved) who participate as Managers in the activities, or who provide services functional to them, such as: legal advice and assistance, audits and investigation activities;

- to the extent necessary, to the recipient body/office (which will remain the autonomous Holder for all consequent processing) for the performance of its tasks and/or to achieve the purposes related to the communication itself.

Personal data will not be disseminated.

### 3. Rights of the data subject.

The data subject may assert his or her rights, recognized by the mandatory regulations, such as:

- Right of access: right to obtain from the data controller confirmation as to whether or not personal data is being processed and if so, to obtain access to personal data and further information on the origin, purposes, category of data processed, recipients of communication and/or transfer of data, etc.
- Right to rectification: right to obtain from the data controller the rectification of inaccurate personal data without undue delay, as well as the integration of incomplete personal data, including by providing a supplementary declaration.
- Right to erasure: right to obtain from the data controller the erasure of personal data without undue delay in the event that:
  - the personal data are not longer necessary in relation to the purposes of the processing;
  - the consent on which the processing is based is revoked and there is no other legal basis for the processing;
  - personal data have been processed unlawfully;
  - personal data must be deleted to fulfill a legal obligation.
- Right to object to processing: right to object at any time to the processing of personal data that have as their legal basis a legitimate interest of the data controller.
- Right to restrict processing: right to obtain from the data controller the restriction of processing, in cases where the accuracy of personal data is contested (for the period necessary for the data controller to verify the accuracy of such personal data), if the processing is unlawful and/or the data subject has objected to the processing.
- Right to data portability: right to receive in a structured, commonly used and machine-readable format personal data and to transmit such data to another data controller, only for cases where the processing is based on consent and only for data processed by electronic means.
- Right to lodge a complaint with a supervisory authority: without prejudice to any other administrative or judicial remedy, a data subject who considers that the processing concerning him or her is in breach of the GDPR has the right to lodge a complaint with the supervisory authority of the Member State where he or she resides or usually works, or of the State where the alleged breach occurred.