

## Contents

1. PURPOSE OF THE PROCEDURE
2. SCOPE OF APPLICATION OF THE PROCEDURE
3. RESPONSIBILITIES
4. SUBJECT AND CONTENT OF THE REPORT
5. CHANNELS
6. RETALIATION AND DATA PRIVACY
7. CASE MANAGEMENT
8. CASE ASSESSMENT AND RESOLUTION
9. DATA RETENTION
10. APPLICATION OF THIS POLICY BY OTHER COMER INDUSTRIES COMPANIES
11. DEFINITIONS
12. ATTACHMENTS

## 1. PURPOSE OF THE PROCEDURE

At Comer Industries, we undertake to respect laws in force, as well as principles and regulations.

Comer Industries promotes a “speak up” culture, or the freedom to speak with colleagues and/or hierarchical superiors if anyone believes it appropriate or necessary to express doubts or concerns, or report problems, in order to improve work within our organization.

This regulatory document governs the process of receiving, analyzing and managing reports from anyone, stakeholders, Comer Industries people and other third parties, sent or submitted, even in confidential or anonymous form.

This procedure also aims to govern the methods for evaluating the validity and grounds of reports and, as a result, for undertaking the appropriate corrective and disciplinary actions to protect Comer Industries.

Furthermore, this procedure is intended to:

- guarantee the confidentiality of the personal data of the whistleblower and the party allegedly responsible for the violation, without prejudice to the rules governing investigations or proceedings initiated by the judicial authority in relation to the events subject to the report, or in any event disciplinary proceedings in the event of reports made in bad faith;
- adequately protect the whistleblower against direct or indirect retaliatory and/or discriminatory conduct for reasons linked directly or indirectly to the report;
- guarantee that a specific, independent, autonomous channel accessible to all is available for whistleblowing.

Furthermore, all cases received via the available channels will be tracked until they are fully closed.

## 2. SCOPE OF APPLICATION OF THE PROCEDURE

This procedure has been approved by the Board of Directors of the Parent Company and its adoption and implementation is therefore compulsory for all Comer Industries Companies all over the world, including any associates and affiliates.

This Policy applies to all employees, including executives and members of the Board of Directors, as well as the business partners of Comer Industries (i.e., suppliers, advisors, customers and, in general, any other third party that engages in contractual relationships with Comer Industries), wherever they are located.

It is the right of each Comer Industries company required to adopt this procedure to adopt different or additional rules with respect to those set forth in this procedure, also in light of local regulations.

In any event, the principles and rules required by legislation are binding, including those concerning the protection of the confidentiality of the whistleblower's identity and the prohibition against direct or indirect acts of retaliation or discrimination against that individual for reasons directly or indirectly linked to the report made.

This procedure will enter into force for Comer Industries at the date of its approval by the Parent Company's Board of Directors.

### 3. RESPONSIBILITIES

The reports received are sent, on the basis of the location of origin, to the expressly authorized and appropriately trained functions responsible for managing them.

Only the functions authorized for this purpose will conduct investigations relating to the reports received.

### 4. SUBJECT AND CONTENT OF THE REPORT

The report should concern all conduct or practices not compliant with what is set forth in the Group Code of Conduct, the Supplier Code of Conduct, laws, regulations and standards, as well as the internal procedural structure in force at Comer Industries.

The report may also be sent in anonymous form.

In any event, however, reports must be circumstantiated and based on precise and concordant elements, regard identifiable facts and contain all elements useful for conducting the verifications and assessments required to evaluate their validity.

Therefore, it is important for the whistleblower to:

- clearly and comprehensively specify in detail where and when the reported events took place;
- provide general information or other elements that make it possible to identify who committed the reported offense;
- indicate any other parties who can provide information about the facts subject to the report;
- indicate/provide any documents that can confirm the validity of the report;
- provide any other information or proof that can confirm the veracity of what has been reported.

### 5. CHANNELS

Whistleblowers who have the reasonable suspicion that one of the violations indicated has taken place or may take place may send a report via [the disclosure web portal](#).

This is a whistleblowing tool compliant with best practices and ethical compliance policies, which require dedicated, secure channel for the reporting of ethical violations.

[This channel](#) is managed by an independent external company, which has the binding duty to protect the identity of all parties using the [portal](#).

[This portal](#) uses encryption systems that guarantee the confidentiality of the whistleblower, the reported party and the information contained in the report.

All information received will be managed in absolute confidentiality, in compliance with legal standards in force.

The access to the disclosure web portal is: [comerindustries.whistlelink.com](https://comerindustries.whistlelink.com).

Via the above-mentioned [portal](#), it is also possible for a non-anonymous whistleblower to request a face-to-face meeting, to be scheduled within a reasonable timeframe.

For any additional details or clarifications concerning disclosure [portal](#), it is possible to contact the Global Compliance function: [integratedsystem\\_compliance@comerindustries.com](mailto:integratedsystem_compliance@comerindustries.com).

### 6. RETALIATION AND DATA PRIVACY

All reports received will be processed in a confidential manner.

The report is secure, and Comer Industries will always protect the person who made the report in good faith from any form of retaliation.

Anyone enacting retaliatory conduct against a good faith whistleblower will be subject to disciplinary measures. The compliance of the [portal](#) with laws in force on Data Privacy is also guaranteed; furthermore, the personal data of the people involved and/or cited in the reports made pursuant to this Policy will be processed, insofar as is possible, in compliance with regulations in force and company procedures on the protection of personal data.

## 7. CASE MANAGEMENT

All reports received by means of [the web portal](#) will be assigned a protocol [number](#) and will be examined. Whistleblowers may request information, provide additional details or monitor case progress by accessing the [portal](#).

## 8. CASE ASSESSMENT AND RESOLUTION

Reports will be investigated at regional level by trained experts in a manner that guarantees the utmost confidentiality.

## 9. DATA RETENTION

The data processed in compliance with this Policy will be stored for the period of time deemed strictly necessary to meet the purposes of the Policy, in compliance with local laws.

## 10. APPLICATION OF THIS POLICY BY OTHER COMER INDUSTRIES COMPANIES

This Policy is to act as a reference for all Comer Industries companies. If local laws impose stricter regulatory obligations on the matter, a local Policy must be prepared in line with this Policy and in keeping with the principles it contains.

## 11. DEFINITIONS

**Good faith:** the genuine conviction that there is a potential violation of the Group Code of Conduct or the Supplier Code of Conduct or that incorrect conduct has been enacted. A report made in good faith must be complete and accurate.

**Supplier Code of Conduct:** expresses the minimum set of requirements concerning: a) labor and human rights, b) business ethics, c) health and safety, d) environment, which any supplier or anyone working in the name or on behalf of suppliers including but not limited to agents, advisors, contractors, interns and temporary workers, must meet to begin and maintain long-term relationships with Comer Industries.

**Group Code of Conduct:** a document adopted by the Group which establishes the principles or fundamental values that express the commitment of Comer Industries to integrity in business and personal conduct.

**Group:** Comer Group, consisting of Comer Industries S.p.A. and the Group companies (hereinafter also referred to as "Comer Industries").

**Retaliation:** any negative action undertaken against a person for having reported a problem or improper conduct in good faith or for having participated in an investigation. These actions include threats, intimidation, exclusion from events involving the team, harassment, discrimination, restriction of career opportunities, placement in a new job, negative performance feedback regardless of real performance shortcomings, or dismissal.

**Whistleblower:** the party sending the Report, be they an employee (including the top management), collaborator, member of the corporate bodies, third party (partner, customer, supplier, advisor, etc.) and, in general, anyone in a business relationship with Comer Industries.

**Report or to report:** the written or verbal communication of information about violations.

**Confidential report:** when the identity of the whistleblower is not specified, but in any event it is possible to determine it in the specific and established cases set forth below.

**Unlawful report:** report which based on the results of the investigation phase is found to be groundless in light

of objective elements, and with respect to which the concrete circumstances verified in the course of that investigation lead to the belief that it was submitted in bad faith or with gross negligence.

**Circumstantiated/verifiable report:** report in which the narration by the author of the facts, events or circumstances constituting the elements underlying the alleged offense (for example, type of offense committed, reference period, value, causes and purposes of the offense, companies/areas/people/units/entities concerned or involved, anomaly in the internal control system, etc.) is provided with a sufficient degree of detail to concretely permit, on the basis of available investigatory tools, the competent company bodies to verify the grounds or otherwise of the facts or circumstances reported.

**Follow-up:** the action undertaken by the party entrusted with the management of the whistleblowing channel to evaluate the veracity of the facts reported, the outcome of the investigations and any measures adopted.

**Reported parties:** anyone whom the whistleblower claims committed the unlawful act/irregularity described in the report.

**Third Parties:** contractual counterparties of Comer Industries, be they natural persons or legal entities, with which the Company agrees upon any form of contractually governed collaboration and which are planning to cooperate with the Company. [for example but not limited to: collaborators; suppliers; advisors (such as advisory firms or lawyers); other third parties that have contractual relationships with Comer Industries (e.g., outsourcing companies, temporary employment agencies and temporary employees)].

**Stakeholders:** all parties with legitimate interests in the company's activities.

## 12. ATTACHMENTS

ATT 1 – PI 7.4 04 ITALIAN REGULATIONS

## ANNEX 1 – ITALIAN REGULATIONS

### DEFINITIONS

**Supplier Code of Conduct:** expresses the minimum set of requirements concerning: a) labor and human rights, b) business ethics, c) health and safety, d) environment, which any supplier or anyone working in the name or on behalf of suppliers including but not limited to agents, advisors, contractors, interns and temporary workers, must meet to begin and maintain long-term relationships with Comer Industries.

**Group Code of Conduct:** a document adopted by the Group which establishes the principles or fundamental values that express the commitment of Comer Industries to integrity in business and personal conduct.

**Work context:** the current or past work or professional activities carried out within the scope of the relationships pursuant to article 3, paragraphs 3 or 4 of Legislative Decree no. 24/2023, through which, irrespective of the nature of such activities, a person obtains information on violations and in the scope of which they could suffer from retaliation in the case of whistleblowing or public disclosure or reporting to the judicial or accounting authority.

**Legislative Decree 196/03:** Legislative Decree no. 196 of June 30, 2003 - Personal Data Protection Code.

**Legislative Decree 231/01 or Decree:** Legislative Decree no. 231 of June 8, 2001, regarding "Regulations of the administrative liability of legal entities, companies and associations, even without legal personality", as amended.

**Public disclosure or to publicly disclose:** to place information on violations in the public domain through the press or electronic means or in any event via means of distribution capable of reaching a high number of people.

**Facilitator:** a natural person who assists a whistleblower in the whistleblowing process, operating within the same work context and whose assistance must be kept confidential.

**GDPR:** Regulation (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

**Group:** the Comer Group, consisting of Comer Industries S.p.A. and the Group companies (hereinafter also referred to as "Comer Industries").

**Information on violations:** information, included justified suspicions, regarding violations committed or which, on the basis of concrete elements, could be committed in the organization with which the whistleblower or the person making the report to the judicial or accounting authority has a legal relationship pursuant to article 3, paragraph 11 or 2 of Legislative Decree no. 24/2023, as well as elements concerning conduct aimed at concealing such violations;

**Internal Audit:** internal and autonomous office with specifically trained personnel assigned the duty of managing the whistleblowing channels activated by Comer Industries pursuant to Legislative Decree no. 24/2023;

**Law 146/2006:** Law no. 146 of March 16, 2006 (Ratification and execution of the United Nations Convention and Protocols against Transnational Organized Crime adopted by the General Assembly on November 15, 2000 and May 31, 2001).

**Model:** Organization and Management Model in accordance with articles 6 and 7 of Legislative Decree 231/01.

**S.B.:** Supervisory Body required under articles 6, paragraph 1, letter b) and 7 of Legislative Decree 231/2001, which is assigned the duty of supervising the functioning and observance of the Model and handling its updating.

**Person involved:** the natural person or legal entity mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or the person otherwise implicated in the violation reported or publicly disclosed.

**Whistleblower:** the natural person making the report or public disclosure of information on violations obtained within their work context.

**Platform:** IT tool for the management of reports.

**Retaliation:** any conduct, act or omission, even only attempted or threatened, carried out as a result of whistleblowing, the report to the judicial or accounting authority or the public disclosure and which provokes or may provoke, directly or indirectly, unfair harm for the whistleblower or the person who made the report.

**Report or to report:** the written or verbal communication of information about violations.

**Anonymous report:** when the general information of the whistleblower is not provided or cannot be otherwise

determined.

**Open report:** when the whistleblower openly raises a problem with no confidentiality restrictions.

**External report:** the written or verbal communication of information on violations submitted via the external whistleblowing channel pursuant to article 7 of Legislative Decree no. 24/2023.

**Internal report:** the written or verbal communication of information on violations submitted via the internal whistleblowing channel pursuant to article 4 of Legislative Decree no. 24/2023.

**Confidential report:** when the identity of the whistleblower is not specified, but in any event it is possible to determine it in the specific and established cases set forth below.

**Unlawful report:** report which based on the results of the investigation phase is found to be groundless in light of objective elements, and with respect to which the concrete circumstances verified in the course of that investigation lead to the belief that it was submitted in bad faith or with gross negligence.

**Circumstantiated/verifiable report:** report in which the narration by the author of the facts, events or circumstances constituting the elements underlying the alleged offense (for example, type of offense committed, reference period, value, causes and purposes of the offense, companies/areas/people/units/entities concerned or involved, anomaly in the internal control system, etc.) is provided with a sufficient degree of detail to concretely permit, on the basis of available investigatory tools, the competent company bodies to verify the grounds or otherwise of the facts or circumstances reported.

**Follow-up:** the action undertaken by the party entrusted with the management of the whistleblowing channel to evaluate the veracity of the facts reported, the outcome of the investigations and any measures adopted.

**Company:** [all Comer Industries companies with registered offices and operations in Italy.](#)

**Private sector parties:** parties other than those defined as public sector parties which: 1) have employed, in the last year, an average of at least fifty subordinate employees with permanent or temporary labor contracts; 2) fall within the scope of application of the acts of the Union pursuant to parts I.B and II of the annex, even if in the last year they did not have the average number of subordinate employees pursuant to number 1); 3) are not the parties pursuant to number 2), fall within the scope of application of Legislative Decree no. 231 of June 8, 2001, and adopt the organization and management models set forth therein, even if in the last year they did not have the average number of subordinate employees pursuant to number 1).

**Public sector parties:** the public administrations pursuant to article 1, paragraph 2 of Legislative Decree no. 165 of March 30, 2001, the independent guarantee, supervisory or regulatory administrative authorities, public economic entities, bodies under public law pursuant to article 3, paragraph 1, letter d) of Legislative Decree no. 50 of April 18, 2016, public service concessionaires, companies under public control and in-house companies as defined in article 2, paragraph 1, letters m) and o), respectively, of Legislative Decree no. 175 of August 19, 2016, even if listed.

**Reported parties:** anyone whom the whistleblower claims committed the unlawful act/irregularity described in the report.

**Third Parties:** contractual counterparties of Comer Industries, be they natural persons or legal entities, with which the Company agrees upon any form of contractually governed collaboration and which are planning to cooperate with the Company. [for example but not limited to: collaborators; suppliers; advisors (such as advisory firms or lawyers); other third parties that have contractual relationships with Comer Industries (e.g., outsourcing companies, temporary employment agencies and temporary employees)].

**Stakeholders:** all parties with legitimate interests in the company's activities.

**Response:** communication to the whistleblower of information relating to the follow-up that has been or will be made to the report.

**Violations:** conduct, acts or omissions that harm the public interest or the integrity of the public administration or the private entity and which consist of: 1) administrative, accounting, civil or criminal offenses that are not included in numbers 3), 4), 5) and 6); 2) unlawful conduct relevant pursuant to Legislative Decree no. 231 of June 8, 2001 or violations of the organization and management models established therein that are not included in numbers 3), 4), 5) and 6); 3) offenses that fall within the scope of application of the acts of the European Union or national acts specified in the annex to Legislative Decree no. 24/2023 or the national acts that constitute the implementation of the acts of the European Union specified in the annex to Directive (EU) 2019/1937, even if not specified in the annex to Legislative Decree no. 24/2023, relating to the following sectors: public contracts;

financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and well-being; public health, consumer protection; protection of privacy and protection of personal data and network and IT system security; 4) acts or omissions that harm the financial interests of the Union pursuant to article 325 of the Treaty on the Functioning of the European Union specified in secondary EU legislation; 5) acts or omissions regarding the internal market, pursuant to article 26, paragraph 2 of the Treaty on the Functioning of the European Union, including violations of the rules of the European Union concerning competition and State aid, as well as violations regarding the internal market connected to acts that violate rules on corporate taxes or mechanisms aimed at obtaining a tax advantage which undermines the subject or purpose of regulations applicable on the matter of corporate taxes; 6) acts or conduct undermining the subject or purpose of the provisions pursuant to the acts of the Union in the sectors specified in numbers 3), 4) and 5).

## REGULATORY FRAMEWORK

The introduction within the national legal system of a system for the management of whistleblowing and adequate protection of employees who report unlawful conduct in the work context is established in international conventions (UN, OECD, Council of Europe) ratified by Italy, as well as recommendations of the Parliamentary Assembly of the Council of Europe.

Specifically, with article 1, paragraph 51, Law no. 190 of November 6, 2012 introduced art. 54-*bis* within Legislative Decree 165/2001, by virtue of which a measure was established aimed at favoring the reporting of offenses, known as whistleblowing.

With the Regulation for the management of whistleblowing and the exercise of sanctioning power with regard to the protection of parties reporting offenses or irregularities of which they become aware within the scope of an employment relationship pursuant to art. 54-*bis* of Legislative Decree 165/2001, ANAC (the Italian National Anti-Corruption Authority) has defined further operational instructions on the matter.

The obligation, established for public administrations, to adopt corruption prevention systems, including a whistleblowing mechanism, was then extended, in part, to the private sector with Law no. 179 of November 30, 2017.

The European Union subsequently released European Directive 2019/1937 on the protection of persons who report breaches of Union law, in order to create a minimum standard for the protection of whistleblower rights in all Member States.

Italy implemented the European Directive with Legislative Decree no. 24 of March 10, 2023.

With the adoption of this Policy, the Comer Industries Companies with headquarters and operations in the Italian territory intend to come into compliance with the above-mentioned regulations, a) clarifying the principles inspiring the mechanism, b) specifying the methods for managing reports, c) indicating the procedures followed to protect the confidentiality of the whistleblower's identity, the content of the report and the identity of any other parties mentioned.

This Policy therefore intends to remove factors that may disincentivize or hinder recourse to the mechanism, such as doubts or uncertainties as to the procedures to be followed and fears of retaliation or discrimination.

The objective pursued is to provide the whistleblower with clear operational instructions concerning the subject, content, recipients and methods for transmitting reports, as well as the forms of protection offered under our legal system.

The whistleblowing management procedure guarantees the confidentiality of the whistleblower's identity starting from receipt of the report and during all subsequent contacts.

## AREA OF APPLICATION

This Policy is intended as a reference for all Comer Industries companies having their registered office and operations in the Italian territory and, therefore, obliged to comply with the regulations set out in Legislative Decree no. 24/23 (hereinafter also referred to as the "Companies").

## REFERENCE PRINCIPLES

## **Knowledge and awareness**

This whistleblowing procedure represents a fundamental element in order to guarantee full awareness for effective monitoring of risks and their interrelationships and to orient changes in the strategy and the organizational context.

## **Guarantee of confidentiality of personal data**

Reports cannot be used beyond what is necessary to adequately follow up on them.

All parties who receive, examine and evaluate the reports and any other party involved in the whistleblowing management process are required to guarantee the utmost confidentiality of the facts reported as well as the identity of the reported party, the whistleblower and the facilitator, who are appropriately protected from retaliatory, discriminatory or in any event unfair conduct.

## **Personal data processing**

All data must be processed in a lawful, fair and transparent manner with respect to the data subjects.

Data must be collected only in order to manage and follow up on whistleblowing reports, public disclosures or official reports.

It is necessary to guarantee that the data are appropriate, pertinent and limited to what is necessary for the purposes for which they are processed, as well as guarantee that they are accurate and updated.

Data processing must take place in a manner which can guarantee personal data security as well as protection, by means of appropriate technical and organizational measures, from unauthorized or unlawful processing and accidental loss, destruction and damage.

It is prohibited to perform whistleblowing channel tracking activities.

It is necessary to guarantee, when possible, the tracking of the activities of authorized personnel in compliance with the safeguards intended to protect the whistleblower.

## **Impartiality, autonomy and independence of opinion**

All parties who receive, examine and evaluate reports must meet moral and professional requirements and ensure their continued fulfillment of the necessary conditions of independence and the due objectivity, competence and diligence in the performance of their activities.

## **The whistleblower protection system**

There are various protections recognized to whistleblowers for reports made in compliance with the regulations, provided that:

- it is a party included in the group of parties authorized to make reports;
- the party reported, officially reported or made a public disclosure on the basis of a reasonable conviction that the information on violations reported, disclosed or officially reported is truthful and falling within the objective scope of application of the decree;
- the report or public disclosure was made in compliance with the rules set forth in Legislative Decree 24/2023;
- there is a relationship of consequentiality between the whistleblowing report, public disclosure and official report made and the retaliatory measures suffered.

This system also applies in cases of anonymous whistleblowing or reporting to the judicial or accounting authority or public disclosure, if the whistleblower has been subsequently identified and suffered from retaliation, as well as in cases of external whistleblowing.

The personal and specific reasons that led the person to make a whistleblowing or official report or public disclosure are irrelevant as far as the management of the report and their protection from retaliatory measures are concerned.

The protection measures also apply to:

- the facilitator (natural person who assists a whistleblower in the whistleblowing process, operating within the same work context and whose assistance must be kept confidential);
- the people in the same work context as the whistleblower, the person who submitted an official report or



the person who made the public disclosure and who are linked to them by a stable emotional bond or family relationship within the fourth degree;

- work colleagues of the whistleblower or the person who submitted an official report or made a public disclosure, who work in the same work context as that person and who have a habitual and current relationship with that person;
- entities owned - exclusively or under majority joint ownership with third parties - by the whistleblower, the reporting party or the party making a public disclosure;
- entities where the whistleblower, reporting party or party making a public disclosure work;
- entities operating in the same work context as the whistleblower, reporting party or party making a public disclosure.

### **Prohibition of discrimination against the whistleblower**

No form of retaliation, even attempted or threatened, which provokes or may provoke, either directly or indirectly, unfair damages for the person/entity for reasons directly or indirectly linked to the report is permitted or tolerated against employees who make a report pursuant to this procedure <sup>(1)</sup> .

The management of communications of retaliation in the public sector and private sector is the responsibility of ANAC; when the communication of retaliation is erroneously received by public or private parties instead of ANAC, such parties are required to guarantee the confidentiality of the identity of the person that sent them and transmit the communication to ANAC, simultaneously providing information of such transmission to the party that sent it.

Whistleblowers are required to provide ANAC with objective information from which it is possible to infer the consequentiality between the whistleblowing report, official report or public disclosure made and the claimed retaliation.

The declaration of nullity of retaliatory acts is the responsibility of the judicial authority, which adopts all measures, including provisional, necessary to ensure the protection of the legal situation of the individual, including compensation for damages, job reinstatement and an order to discontinue the retaliatory conduct.

Within the scope of legal or administrative proceedings concerning the assessment of any retaliation against whistleblowers, it is presumed that it is carried out as a result of the whistleblowing; the burden of proof that such conduct or acts are justified by reasons extraneous to the whistleblowing, public disclosure or official report is under the responsibility of the party that initiated them.

This benefit does not apply to facilitators, people in the same work context with a stable emotional bond or family relationship within the fourth degree with the whistleblower or the party making the official report or public disclosure, work colleagues who work in the same work context and who have a habitual and current relationship with the whistleblower, and also legal entities in cases in which they are entities owned by the whistleblower or party making the official report or public disclosure or entities where they work or entities that work in the same work context: if any of these parties claim that they have suffered from retaliation or damage, they therefore bear the burden of proof.

In the case of a demand for compensation submitted to the judicial authority by whistleblowers, if such people

---

<sup>(1)</sup> The cases listed in art. 17, par. 4 of Legislative Decree 24/2023 constitute retaliation, specifically: a. dismissal, suspension or equivalent measures; b. demotion or passing over for promotion; c. change in functions, change in workplace, reduction in wages, change in working hours; d. suspension of training or any restriction of access to it; e. negative reference letters or negative references; f. the adoption of disciplinary measures or other penalties, including financial; g. coercion, intimidation, harassment or ostracism; h. discrimination or other unfavorable treatment; i. non-conversion of a temporary labor agreement into a permanent labor agreement, when the worker has the legitimate expectation of such conversion; l. non-renewal or early termination of a temporary labor agreement; m. damages, also to the person's reputation, particularly on social media, or economic or financial harm, including the loss of economic opportunity and the loss of income; n. the early conclusion or cancellation of a contract for the supply of goods or services; o. the cancellation of a license or a permit; p. request for subsection to psychiatric or medical assessments.

demonstrate that they have made, pursuant to Legislative Decree 24/2023, a report, a public disclosure or a report to the judicial or accounting authority and that they have suffered from damages, it is presumed, unless proved otherwise, that the damage is the result of that report, public disclosure or report to the judicial or accounting authority.

People who have been dismissed due to whistleblowing, public disclosure or a report to the judicial or accounting authority are entitled to job reinstatement.

Whistleblowers who believe that they have suffered from discrimination or retaliation may also provide circumstantiated information about the discrimination to: a) their Manager; b) Internal Audit; c) the Supervisory Body; d) the Public Prosecutor's office in the case of any criminally relevant facts.

This is without prejudice to the whistleblower's right to provide information about what took place to the trade unions or the competent Judicial Authority.

### **Obligation of confidentiality with regard to whistleblower and facilitator identity and non-applicability of the right to access the report**

With the exception of cases in which there is liability for defamation and slander pursuant to the provisions of the criminal code or art. 2043 of the Civil Code and the cases in which anonymity is not applicable by law (e.g., criminal, tax or administrative investigations, inspections of the control bodies), the identity of the whistleblower is protected in any context subsequent to when the report is made.

Therefore, without prejudice to the above-mentioned cases, the identity of the whistleblower and any other information from which this identity can be inferred either directly or indirectly cannot be revealed without the express consent of the whistleblower to people other than those responsible for receiving or following up on reports, who are expressly authorized to process such data.

Confidentiality is also guaranteed in the case of internal or external reports made verbally through telephone lines or, alternatively, voice messaging systems or, at the request of the whistleblower, during a direct meeting with the party handling the report.

The confidentiality of the whistleblower is also protected when the report is received by personnel other than authorized personnel responsible for managing whistleblowing reports, to whom, in any event, they must be transmitted without delay.

The same confidentiality obligations are guaranteed with respect to the facilitator who supports the whistleblower, as concerns their identity as well as the assistance concretely provided.

Everyone who receives or is involved in whistleblowing management is required to protect the confidentiality of such information.

The violation of the duty of confidentiality is a source of disciplinary liability, without prejudice to the additional forms of liability established in our legal system.

Insofar as criminal proceedings are concerned, the identity of the whistleblower is covered by secrecy in the methods and within the limits established by article 329 of the code of criminal procedure.

Within the scope of proceedings before the Court of Auditors, the identity of the whistleblower cannot be revealed until the closure of the investigatory phase.

As concerns disciplinary proceedings, the identity of the whistleblower cannot be revealed when the disciplinary charge is based on distinct and additional assessments with respect to the report, even if resulting from it. If the charge is founded, all or in part, on the report and knowledge of the whistleblower's identity is indispensable for the defense of the accused, the report will be usable for the disciplinary proceedings only if the whistleblower has provided consent to the disclosure of their identity.

The whistleblower is notified by means of written communication of the reasons for the disclosure of confidential data, if the disclosure of the identity of the whistleblower and the connected information is also indispensable for the defense of the person involved.

As concerns proceedings initiated following internal or external reports, the identity of the whistleblower may be revealed if such revelation is indispensable also in order to defend the person involved, only if the whistleblower provides consent to the revelation of their identity.

The whistleblower is notified by means of written communication of the reasons for the disclosure of confidential data, if the disclosure of the identity of the whistleblower and the connected information is also indispensable for the defense of the person involved.

The report is also not subject to the right to access administrative deeds or the generalized right of public access.

Particularly with reference to privacy, personal data will be processed exclusively in order to manage the report made and verify the information contained in it.

The data will also be processed with hard copy as well as electronic/computerized/IT tools/media, in full compliance with legal standards, according to principles of lawfulness and fairness and so as to protect the confidentiality of the whistleblower.

Any revelation of the identity of the whistleblower to people other than those responsible for receiving or following up on reports must always take place with the whistleblower's express consent.

### **The reported party protection system**

#### **Obligation of confidentiality with respect to the identity of the reported party and all people mentioned in the report**

In compliance with regulations in force, the Companies have adopted the same forms of protection to guarantee the privacy of the whistleblower for the party allegedly responsible for the violation as well as all people mentioned in the report, without prejudice to any additional form of responsibility established by law which imposes the obligation to communicate the name of the reported party (e.g., requests to the judicial authority). Without prejudice to cases in which an appeal is made to the judicial authority, pending the assessment of any disciplinary liability of the reported party, and until the conclusion of proceedings initiated on the basis of the whistleblowing report, the function responsible for managing the report must handle the identity of the reported party and all people mentioned in the report with privacy, secrecy and confidentiality; in particular, their names should not be revealed without their consent and third parties should not be allowed to access the report and their identities.

Confidentiality is also guaranteed: a) in the case of internal or external reports made verbally through telephone lines or, alternatively, voice messaging systems or, at the request of the whistleblower, during a direct meeting with the party handling the report; b) when the report is made with methods other than those established by the administrations/entities and ANAC in compliance with the decree; c) when the report is received by personnel other than those authorized and responsible for handling the report, to whom, in any event, it must be transmitted without delay.

The Companies do not apply disciplinary penalties to the reported party on the basis of what is affirmed by the whistleblower without first finding objective evidence of it and without there having been an investigation of the facts subject to the report and until the conclusion of the proceedings initiated on the basis of the report, in line with the same guarantees established in favor of the whistleblower.

#### **Possibility of interviewing the reported party**

The reported person may be interviewed or, at their request, is interviewed, also by means of written proceedings through the acquisition of written observations and documents.

This party does not have the right to always be informed of the report regarding them, but only within the scope of any proceedings initiated against them following the conclusion of the whistleblowing management process and if such proceedings are based all or in part on the report.

#### **Protection of the reported party from whistleblowing in bad faith**

All parties are required to respect the dignity, honor and reputation of all. To this end, the whistleblower is required to specify whether they have a private interest associated with the report.

More generally, the Companies must guarantee adequate protection from bad faith whistleblowing, objecting to such conduct and disclosing the fact that reports sent in order to harm or otherwise damage others as well as any other form of abuse of this document are a source of liability, in disciplinary proceedings as well as in the other competent fora.

## **DISTRIBUTION**

This Policy is published on the website of Comer Industries, when present. Furthermore, each subsidiary must translate this regulation into their local language to ensure more widespread distribution and understanding of the document.

The same distribution procedures set forth above are adopted for subsequent revisions and additions to the procedure.

This procedure must be subject to large-scale communication, such so as to become a constant reference in company activities.

In order to enact the procedure, personnel training and information is managed by the competent function responsible in close coordination with the HR function.

For collaborators, similar procedure information and disclosure is required, potentially using different methods, for example by providing a hard copy and requesting acknowledgment that they have viewed it, possibly distinguishing between parties based on the type of contractual relationship they have with the Companies.

## FOR WHISTLEBLOWERS: HOW AND WHEN TO MAKE A REPORT USING THE INTERNAL WHISTLEBLOWING CHANNEL

### Who can report

The whistleblowing system can be activated by the following parties:

- subordinate employees of the Companies;
- independent workers who work at the Companies;
- collaborators and workers who work for parties providing goods or services or carrying out work for the Companies;
- independent professionals and consultants who work for the Companies;
- volunteers and interns, paid and unpaid;
- shareholders and people with administration, management, control, supervisory or representation functions, even if such functions are exercised on a merely de facto basis for the Companies;
- In relationships with the Companies and according to what is set forth in the Model and the Code of Ethics, whistleblowers must report what is set forth in the "Subject of the report" section.

### When can a report be submitted?

- when the legal relationship is ongoing;
- during the trial period;
- when the legal relationship has not yet started, if the information about violations has been acquired during the selection process or in other pre-contractual phases;
- subsequent to the dissolution of the legal relationship if the information about violations was acquired prior to such dissolution.

### What can be subject to a report?

Whistleblowing should concern information about violations, including grounded suspicions, of national and European Union law which harm the public interest or the integrity of the public administration or the private entity, committed within the organization of the entity with which the whistleblower or reporting party has one of the qualified legal relationships considered by the legislature, consisting of:

- administrative, accounting, civil or criminal offenses;
- unlawful conduct relevant pursuant to Legislative Decree 231/2001, or violations of Organizational models;
- offenses that fall within the scope of application of EU acts relating to the following (sensitive) sectors: public contracts; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and well-being; public health; consumer protection; protection of privacy and protection of personal data and network and IT system security;
- acts or omissions that harm the financial interests of the Union as identified in EU regulations, directives, decisions, recommendations and opinions;
- acts or omissions regarding the internal market, which compromise the free movement of goods, people, services and capital;
- acts or conduct undermining the subject or purpose of the provisions of the Union in the sectors specified in the previous points.

The report may also include:

- information concerning conduct aimed at concealing the violations listed above;
- unlawful activities not yet carried out but which the whistleblower reasonably believes could take place in the presence of precise and concordant concrete elements;
- founded suspicions, as defined by the ANAC Guidelines.

Reportable information about violations does not include information that is clearly groundless, information already fully in the public domain or information acquired only on the basis of low-reliability leaks or rumors ("gossip").

The regulatory provisions do not apply:

- to charges, claims or requests linked to a personal interest of the whistleblower or the person who made a report to the judicial or accounting authority which relate exclusively to their own individual work or public employment relationships, or concerning their work relationships with hierarchically superior individuals;
- to reports of violations when already governed on a binding basis by acts of the European Union or national acts specified in part II of the annex to Legislative Decree no. 24 of March 23, 2023 or those national acts which constitute the implementation of the acts of the European Union specified in part II of the annex to Directive (EU) 2019/1937, even if not specified in part II of the annex cited above;
- to reports of violations concerning national security, as well as contracts relating to defense or national security aspects, unless such aspects fall within the scope of secondary EU legislation.

Provisions on the exercise of the right of workers to consult their representatives or unions, protection against unlawful conduct or acts carried out on the basis of such consultations, the autonomy of the social partners and their right to enter into collective agreements, as well as repression of anti-union conduct pursuant to article 28 of law no. 300 of May 20, 1970, shall continue to apply.

### **Reported parties**

The reports may regard members of the corporate bodies, the management, employees, shareholders, external collaborators, non-subordinate collaborators of the Companies, as well as commercial partners, suppliers and everyone that engages in relations with them and refer to any type of unlawful conduct of which they may become aware.

### **Content of the report**

Whistleblowers are required to provide all information needed to allow for the competent offices to proceed with the required and appropriate investigations to verify the facts subject to the report. To this end, the report must preferably contain the following information:

- general information of the whistleblower, with an indication of their position or function carried out in the Company;
- a clear and complete description of the facts subject to the report;
- if known, the time and place where the facts took place;
- if known, the general information of or other aspects (like role and department) that make it possible to identify the party that carried out the facts subject to the report;
- an indication of any other parties who can provide information about the facts subject to the report;
- an indication of any documents that can confirm the validity of these facts;
- any other information that can confirm the veracity of the facts reported.

Reports from which it is not possible to infer the identity of the whistleblower are considered anonymous.

Anonymous reports, or those without information that makes it possible to verify their author, even if sent via the methods specified below, will be taken into consideration for further verification only if:

- adequately circumstantiated and capable of identifying specific facts and situations;
- they do not appear prima facie to be irrelevant, groundless or uncircumstantiated;
- they relate to particularly serious facts and have content that is adequately detailed, circumstantiated or related to specific contexts (e.g., indication of names or specific roles, mention of specific offices, particular proceedings or events).

Anonymous reports will therefore be managed according to the criteria established for ordinary reports.

This is without prejudice to the requirement of good faith and the truthfulness of the facts or situations reported, for the protection of the reported party.

The report must not regard personal complaints of the whistleblower or claims/requests falling within the regulation of the employment relationship or relationships with a hierarchical superior or colleagues, should not

take on injurious tones or contain personal offenses or moral judgments aimed at offending or harming the personal and/or professional honor and/or respectability of the person or people to whom the facts reported are allegedly ascribed.

### **Whistleblowing methods**

Whistleblowers who have the reasonable suspicion that one of the violations indicated has taken place or may take place may send a report via the Disclosure Hotline.

This is a whistleblowing tool shared with the trade union representatives and organizations that is compliant with best practices and ethical compliance policies, which require dedicated, secure channel for the reporting of ethical violations.

This channel is managed by an independent external company, [Whistlelink](#), which has the binding duty to protect the identity of all parties using the Hotline.

This channel uses encryption systems that guarantees the confidentiality of the whistleblower, the reported party and the information contained in the report.

All information received will be managed in absolute confidentiality, in compliance with legal standards in force.

The access to the disclosure web portal is: [comerindustries.whistlelink.com](https://comerindustries.whistlelink.com)

Via the above-mentioned channel, it is also possible for a non-anonymous whistleblower to request a face-to-face meeting, to be scheduled within a reasonable timeframe.

For any additional details or clarifications concerning communication channels, it is possible to contact the Global Compliance function: [integratedsystem\\_compliance@comerindustries.com](mailto:integratedsystem_compliance@comerindustries.com).

## FOR THE REPORT RECIPIENT: WHAT HAPPENS AFTER THE REPORT IS MADE

The competent function ensures that all of the appropriate verifications have been performed on the verifiable reported facts, through one or more of the following activities, guaranteeing that such phases are carried out in as little time as possible and in compliance with the principles of objectivity, competence and professional diligence; furthermore, methods suited to guarantee transparency and fairness in the performance of report management activities will be ensured.

The phases of the report management process are described below.

### Receipt

Once the report has been received, the function responsible for managing reports must issue to the whistleblower a notice of receipt of the report within seven days of the date of receipt in order to inform them that it has been taken into consideration.

If the internal report regards violations of the Organization and Management Model, the function responsible for report management orders its transmission to the Supervisory Body within seven days of receipt.

The Supervisory Body may perform a parallel investigation for the purposes of the 231 Model.

The Personnel of both Companies that receive a report sent outside of the established channels should send it within seven days of its receipt, in the original with any annexes, to the competent unit established, while also notifying the whistleblower of this transmission, in compliance with criteria of utmost confidentiality and with methods suitable to protect the whistleblower and the identity and integrity of the reported parties, without prejudice to the effectiveness of subsequent assessment activities.

### Preliminary review

The objective of the preliminary review is to classify the communications received in order to identify the reports to be processed in application of this regulation, as well as evaluate the fulfillment of the prerequisites required to launch the subsequent assessment phase.

In order to distinguish a report from a mere personal complaint, the function responsible for report management carries out an initial report eligibility screening, evaluating:

- if the report is meant to call conduct that puts its activity and/or third parties at risk to the attention of the Company;
- how serious and urgent the risk is for the Companies and/or third parties;
- if the subject of the report has already been evaluated in the past;
- if the report contains sufficient elements to be able to be verified or if, to the contrary, it is too generic or lacks the elements required for a subsequent investigation.

Once the appropriate investigations and analyses have been performed, the function responsible for managing the report alternatively:

- proposes, sending a notice of this to the whistleblower - if known - the dismissal of reports: i) not qualifiable as verifiable circumstantiated reports, so that it is not considered possible to initiate the investigation phase; ii) that are clearly groundless and unlawful; iii) containing facts already subject to specific investigation activity in the past and already dismissed, when no new information emerges from the preliminary assessments performed such so as to make additional verifications necessary; iv) that are verifiable and circumstantiated for which, in light of the results of the preliminary assessments performed, it is not deemed necessary to initiate the subsequent investigation phase;
- contacts the whistleblower if it believes that the report is excessively generic in order to ask them to provide the information needed for the investigation, then proceeding with the dismissal of the report if no additional information is provided or the information provided is in any event considered insufficient;
- sends the communications received not identified as whistleblowing reports to the company functions responsible for receiving and processing them on the basis of reference regulations, informing the sender when possible that the issue reported does not constitute one of the cases set forth in this regulation and that it will be handled by the competent company functions.



## Investigation

The objective of report assessment activities is to proceed with specific verifications, analyses and assessments concerning the grounds or otherwise of the facts reported, as well as to make any recommendations concerning the adoption of the necessary corrective actions in the areas and company processes concerned by the report.

After the report is sent, non-anonymous whistleblowers may be contacted by the competent body if it is necessary to obtain the information needed in the investigation phase.

Whistleblowers may send additional information of which they may become aware concerning the facts subject to the report and may also request updates on report status: thus, it is possible to establish a sort of direct interaction with the whistleblower.

The management and verification of the validity of the circumstances described in the report are assigned to the competent body, which handles these activities in compliance with the principles of impartiality and confidentiality, by carrying out all activity deemed appropriate, including personally interviewing the whistleblower and any other parties who can provide information about the reported facts.

The body directly performs all activities aimed at evaluating the facts subject to the report.

It may also rely on the support and collaboration of company structures and functions, including the Supervisory Body, when, due to the nature and complexity of the assessments, their involvement is required; as well as external advisors.

It may speak directly with the whistleblower - if known - or the parties mentioned in the report.

During the report investigation, the right to confidentiality and respect for the anonymity of the whistleblower shall be ensured, unless this is not possible due to the characteristics of the investigations to be performed. In which case the party working to support the body shall be subject to the same duties of conduct aimed at guaranteeing the confidentiality of the whistleblower.

If, after the investigation phase, it is found that the report is: (i) not founded on the basis of objective elements, and (ii) made in bad faith or with gross negligence, the function responsible for report management:

- may decide, by a justified measure, to dismiss it, deleting the names and elements that may allow for the identification of the reported parties,
- sends it to the competent functions for an assessment concerning whether any disciplinary penalties or other measures should be adopted against the whistleblower,
- monitors their implementation and ensures that the reported party is promptly informed.

If, after verification, the report is found to be grounded, the function that received the report, in relation to the violation, will:

- communicate the result of the assessment and its evaluations promptly to: a) the Chairman of the Board of Directors and, at the next possible meeting, the entire Board and the Board of Statutory Auditors; b) the Sole Director and, at the next possible meeting, the Board of Statutory Auditors;
- provide a summary disclosure of report management activities, with an indication of the results of the relative investigations and the progress status of the corrective actions identified to the Supervisory Body;
- indicate the result of the assessment to the Manager of the structure to which the perpetrator of the confirmed violation belongs so that they may, if necessary, perform an additional assessment, possibly with the support of legal advisors, as well as adopt the management measures within their purview including, when the relative requirements are met, the exercise of disciplinary actions;
- adopt any additional measures and/or actions necessary to protect the company in the concrete case including, when necessary, the submission of the report to the competent judicial authority.

If the investigation phases bring to light corrective actions in the Internal Control and Risk Management System, the management of the areas/processes subject to assessment is responsible for preparing a plan of corrective actions to remove the critical issues identified.

The Supervisory Body will be informed of the relevant cases insofar as the 231 Model is concerned and may supplement the Action Plan with the corrective measures deemed necessary.

The function responsible for report management monitors the relative implementation status of corrective actions by means of follow-ups.

### **Feedback to the whistleblower**

Once the investigation phase has been completed and the appropriate decisions have been made concerning the report, the function responsible for report management will need to:

- provide feedback to the whistleblower within three months of the date of the notice of receipt or, lacking such notice, within three months of the end of the seven-day term from the submission of the report, in order to inform them about the management and assessment of the report and the activity carried out;
- complete a final investigation report.

## **FOR WHISTLEBLOWERS: HOW AND WHEN TO MAKE A REPORT USING THE EXTERNAL WHISTLEBLOWING CHANNEL**

The competent Authority for external reports, including for the private sector, is ANAC.

It is possible to report to the Authority only when one of the following conditions is met:

- within the work context, there is no compulsory activation of the internal reporting channel or, even if compulsory, it is not active or, even if activated, it is not compliant with what is set forth in this annex;
- if the whistleblower has already sent an internal report but there was no follow-up;
- if the whistleblower has justified reasons to believe that, if an internal report were made, it would not be effectively followed up or that the report could give rise to retaliation;
- if the whistleblower has a justified reason to believe that the violation could constitute a clear or present danger for the public interest.

Like internal channels, the whistleblowing channel established by ANAC must be suitable to ensure, including through encryption instruments, the confidentiality of the identity of the whistleblower and those involved in the report, as well as the content of the report and the relative documentation.

Also in this case, reports may be made via the IT platform or verbally (through telephone lines or voice messaging systems) and, if requested by the whistleblower, during a face-to-face meeting to be scheduled within a reasonable timeframe.

If the external report was submitted to the incorrect party, it is transmitted within seven days of receipt to ANAC, informing the whistleblower of such transmission.

ANAC is required to:

- provide any person concerned with information on the use of the external whistleblowing channel and the internal whistleblowing channel, as well as on the protection measures pursuant to Legislative Decree no. 24/23;
- send a notice of receipt of the report to the party concerned within seven days of the date of its receipt, unless explicitly requested otherwise by the whistleblower or without prejudice to the case in which ANAC believes that the notice would harm the protection of the confidentiality of the identity of the whistleblower;
- hold discussions with the whistleblower and request additional information from them if necessary;
- diligently follow up on the reports received;
- perform the investigations required to follow up on the report, including through interviews and the acquisition of documents;
- provide a response concerning the report within three months or, if there are justified and grounded reasons, within six months of the date of the notice of receipt of the external report or, lacking such notice, the term of seven days as of receipt;
- notify the whistleblower of the final outcome.

ANAC may not follow up on reports that describe minor violations and proceed with their dismissal.

Obligations of confidentiality must be ensured even if the report is received through channels other than those provided or via personnel other than those responsible, to which in any event the report must be transmitted without delay.

For report management, ANAC must employ adequately trained personnel to provide the people concerned with information on the use of internal and external whistleblowing systems and the protections to which they are entitled.

## FOR WHISTLEBLOWERS: HOW AND WHEN TO MAKE A REPORT USING PUBLIC DISCLOSURE

It is possible for the whistleblower to make a public disclosure with the benefit of protection.

Whistleblowers who make a public disclosure benefit from protection if one of the following conditions is met:

- the whistleblower has previously sent an internal and external report or has directly made an external report and did not receive a response within the timeframes established concerning the measures planned or adopted to follow up on the reports;
- the whistleblower has a justified reason to reasonably believe, on the basis of concrete circumstances and therefore not based on mere conjecture, that the violation could constitute a clear or present danger for the public interest;
- the whistleblower has a justified reason to believe that the external report may entail the risk of retaliation or may not be effectively followed up on due to the specific circumstances of the actual case, such as those in which proof may be concealed or destroyed or in which there is a justified concern that the person who received the report may be colluding with the perpetrator of the violation or involved in the violation.

The protection of confidentiality does not apply if the whistleblower has intentionally revealed their identity, for example through web or social media platforms. The same is also true if the party contacts a journalist directly. Indeed, in this case, the rules on the professional secrecy of journalists, with reference to the news source, shall apply.

On the other hand, if the party making the disclosure does not reveal their identity (e.g., using a pseudonym or a nickname on social media), such disclosures will be deemed equivalent to anonymous reports.

## **CONTROLS, ARCHIVING AND STORAGE OF DOCUMENTATION, TRACEABILITY**

All documentation is stored for the time necessary to process the report and in any event for no more than five years as of the date of the communication of the final outcome of the whistleblowing procedure, in compliance with the confidentiality obligations established by law.

For reports made via telephone:

- if for the report a recorded telephone line or another recorded voice messaging system is used, the report, with the consent of the whistleblower, is documented by the responsible personnel via recording on a storage and listening device or via full transcription. For transcriptions, whistleblowers may verify, rectify or confirm the content of the transcription by signing it;
- if for the report a non-recorded telephone line or another non-recorded voice messaging system is used, the report is documented in writing in a detailed report of the conversation drafted by the responsible personnel. Whistleblowers may verify, rectify and confirm the content of the transcription by signing it.

When, at the request of the whistleblower, the report is made verbally during an interview with the responsible personnel, it, with the consent of the whistleblower, is documented by the responsible personnel via recording on a storage and listening device or in minutes.

For minutes, whistleblowers may verify, rectify and confirm the meeting minutes by signing them.

In order to guarantee the management and traceability of reports and the relative investigation activities, the function responsible for report management will prepare and update the system dedicated to report management, monitoring and reporting, ensuring that all of the relative supporting documentation is archived.

To this end, the function responsible for report management ensures that the original report documentation is stored, in addition to the work papers relating to the investigations and assessments performed on the reports, in dedicated hard copy/electronic archives with the highest security/confidentiality standards, consistent with regulations and according to specific internal rules.

Pursuant to laws in force and company procedures on privacy, the processing of the personal data of the people involved and/or cited in the reports will be protected.

## **PENALTY MECHANISM**

### **Loss of protection**

The whistleblower will maintain criminal and disciplinary liability:

- if the criminal liability of the whistleblower is confirmed, even with a non-definitive ruling in the first instance, for the offenses of defamation or slander or if such offenses have been committed with a report made to the judicial or accounting authority;
- in the case of civil liability for the same reason due to willful misconduct or gross negligence;

Whistleblowers may also be found liable, in terms of disciplinary proceedings and in the other applicable fora, if it is confirmed that there have been any types of abuse of this procedure, such as reports found to be groundless, or those which are clearly opportunistic and/or made with the sole purpose of harming the reported party or other parties, and if there is any other case of improper use or intentionally self-serving use of this Policy.

All confirmed violations of the measures established to protect the whistleblower and the reported party are likewise penalized.

Disciplinary measures, as established by law and applicable collective agreements, will be proportionate to the extent and severity of the unlawful conduct confirmed and may even include termination of the employment relationship, in compliance with applicable provisions of law and the national collective labor agreement.

In particular, in evaluating the disciplinary penalty to be adopted against those adopting retaliatory or discriminatory measures against the whistleblower, the severity of such retaliatory or discriminatory measures, any damage to health suffered by the whistleblower as a result of such measures and whether such measures have been adopted repeatedly or with the participation of two or more people will be taken into account.

In the event of reports clearly made in bad faith, the function responsible for report management reserves the right to dismiss them, deleting the names and elements that may allow for the identification of the reported parties.

### **Limitations of liability**

Anyone disclosing or disseminating information on violations covered by the obligation of secrecy or relating to the protection of copyright or the protection of personal data, or disclosing or disseminating information about violations that harm the reputation of the person involved or reported, shall not be punishable.

This criminal exemption from liability applies “when, at the moment of disclosure or dissemination, there were justified reasons to believe that the disclosure or dissemination of the information was necessary to reveal the violation and the whistleblowing report, public disclosure or report to the judicial or accounting authority was made in the required manners”.

When the conditions set forth above are met, any additional liability is excluded, even civil or administrative in nature.

Unless the fact constitutes a crime, liability is excluded, including civil or administrative in nature, for the acquisition of information on violations or for lawful access to it.

Criminal liability and any other liability, including civil or administrative in nature, is also excluded for conduct, acts or omissions if linked to the whistleblowing report, official report or the public disclosure and strictly necessary to disclose the violation.

Criminal liability and any other liability, including civil or administrative in nature, is not excluded for conduct, acts or omissions not linked to the whistleblowing report, the report to the judicial or accounting authority or the public disclosure or which is not strictly necessary to disclose the violation.

### **Additional provisions**

Disciplinary penalties are applied for retaliation, cases in which the report is obstructed or an attempt was made to obstruct it, violations of the obligation of confidentiality, failure to assess and analyze the reports

received and reports that are clearly opportunistic and made for the sole purpose of defaming and/or slandering the reported party or other parties.

Waivers and settlements, full or partial, concerning the rights and protections set forth in this Policy and, in general, in Legislative Decree 24/2023, are not valid unless made in the forms and manners pursuant to article 2113, par. 4 of the Civil Code.

In compliance with what is set forth in art. 18 of Legislative Decree 24/2023, ANAC has a list of third sector entities that provide support to whistleblowers.

Please refer to Legislative Decree 24/2023 for any matters not expressly addressed.

## **DISCLOSURE PURSUANT TO ART.13 OF EU REGULATION 2016/679 (GENERAL DATA PROTECTION REGULATION, or GDPR)**

The processing of the personal data in reports will take place pursuant to Regulation (EU) 2016/679 on the protection of natural persons in relation to the processing of personal data (GDPR), as well as any other applicable laws and/or regulations within the limits of what is compatible with the GDPR and the specific policy published on the website of Comer Industries.

Any exchange and transmission of information entailing personal data processing by EU institutions, bodies or entities must also take place in compliance with Regulation (EU) 2018/1725.

The protection of personal data is ensured not only to the whistleblower or reporting party, but also to the other parties to whom the protection of confidentiality applies, such as the facilitator, the person involved and the person mentioned in the report insofar as they are “data subjects”.

During report management, the personal data of the whistleblower will be processed, if their name has been provided, in addition to the personal data of the reported party, such as name, surname, role, etc. and the personal data of any third parties, as well as any other information gathered in the context of the investigations that is necessary and adequate to assess and verify the grounds or otherwise of the report.

Each Comer Industries Company will act as an autonomous Data Controller for the personal data of its employees within the scope of their employment relationship.

In the management of reports, Comer Industries also acts in the interest of the subsidiaries, in compliance with applicable provisions of law including, in particular, the principles of necessity, proportionality and lawfulness of processing as set forth in the GDPR, as well as consistent with what is set forth in the Privacy Code.

Any personal data processing carried out by different functions of the companies concerned, Control Bodies and Supervisory Bodies and as part of the report management process falls under the responsibility of the Data Processors and the persons authorized to process personal data for their respective areas in compliance with provisions of law and what is set forth in these regulations.

The report management process is inspired by the principle of “guarantee of confidentiality and anonymity” and the “principle of confidentiality of the whistleblower”, and therefore pending the internal assessment process the utmost confidentiality will be guaranteed.

The parties concerned may exercise, if established by applicable provisions of law, the rights set forth under the GDPR by sending an email to the following addresses: [privacy@comerindustries.com](mailto:privacy@comerindustries.com) and [infodpo@kncm.it](mailto:infodpo@kncm.it).

The right to contact the data protection authority competent for matters concerning unlawful data processing is also guaranteed. When there is a risk that the exercise of the rights recognized to the data subject in Chapter III of the GDPR may result in actual and concrete harm to the confidentiality of the whistleblower’s identity, which may compromise the capacity to effectively verify the grounds of the Report or collect the necessary evidence, we reserve the right to limit or delay the exercise of such rights, in compliance with what is set forth in applicable provisions of law.

In no circumstance may the reported person or the person mentioned in the report, with reference to their personal data processed within the whistleblowing report, public disclosure or official report, exercise the rights that Regulation (EU) 2016/679 normally recognizes to data subjects. The exercise of such rights may give rise to actual and concrete harm to the protection of the confidentiality of the whistleblower’s identity. Therefore, in such cases the reported party or the person mentioned in the whistleblowing report is also precluded from the possibility, if they believe that the processing of their data violates the above-mentioned rights, of contacting





---

DOCUMENT TYPE: **Integrated Procedure**

CODE: ATT 1 PI 7.4 04

---

TITLE: **Whistleblowing**

REV: **02** DATE: **2024/04/23**

---

PROCESS: **Communication**

PAGE: **21 / 21**

---

the data controller and, in lacking a response from the latter, of lodging a complaint with the Data Protection Authority.