C.B.M. S.r.l. a socio unico
Address: Via Castello 10 26038 - Torre dé Picenardi (Cremona) Italy
Tel:++39 - (0)375 – 394095 Fax:++39 - (0)375 - 394098
E-Mail: info@cbm-srl.com – Web: http://www.cbm-srl.com

POLICY WHISTLEBLOWING CBM s.r.l. (English Version)

CBM s.r.l.
Located in Torre de' Picenardi (CR) , Via Castello nr.10 , CAP 26038
VAT nr: 00114010192

Last version: 13/12/2023

Summary

Background and context 2
1. Purpose of the Whistleblowing Policy 2
2. Persons who may make reports 2
3. Subjects covered by the Reports 3
4. Facts that CANNOT be reported 4
5. Elements to be included in the Report 5
7. The Telematics Channel: The Whistleblowing Portal 5
8. Channel in oral form. 7
9. Reporting Managers 7
10. Preliminary Examination of the Report. 8
11. Investigation and fact-finding 9
12. Feedback to the reporter 10
13. Protection of the reporter 11
(a) Duty of confidentiality 11
b) Prohibition of retaliation 12
c) Limitation of liability for the reporter 13
14. Data Processing and Retention of Reports 14
15. Information on the external reporting channel established at ANAC 14
16. Conditions for External Reporting 15
17. Training and Communication 15
18. Policy Update 15

Background and context

With Legislative Decree 24/2023, in implementation of the EU Directive 2019/1937, the legislator approved the discipline for the protection of persons who report violations of national or European Union rules that harm the public interest or the integrity of the public or private entity, of which they have become aware in a public or private employment context.

The aforementioned Decree, by providing for a specific discipline for the protection of whistleblowers, aims to incentivise the cooperation of workers and, in general, of the collaborators of the entities (as better identified below) in order to foster, within public and private entities, the emergence of acts or phenomena in conflict with European and national legislation.

In fact, the new regulation establishes for companies falling within its scope of application (e.g. those which have employed at least 50 employees in the last year), on the one hand, the obligation to set up an internal reporting channel providing adequate guarantees of confidentiality and security and, on the other hand, the guarantee of protection for whistleblowers by establishing the prohibition of retaliatory acts and the imposition of specific sanctions in the event of violation of the regulations.

Moreover, the same protection is provided for those who, under certain conditions - which will be illustrated below - report violations through the external reporting channel set up at the National Anti-Corruption Authority (ANAC) or for those who make public disclosures and reports to the judicial and accounting authorities.

1. Purpose of the Whistleblowing Policy

In compliance with the above-mentioned legislation, the company CBM s.r.l. (hereinafter also the "Company") has adopted its own internal reporting channel described in this procedure (hereinafter also the "Policy") which guarantees, also by means of encryption tools, the confidentiality of the identity of the reporting person, of the person involved and of the person in any case mentioned in the report, as well as the content of the report and of the relevant documentation.

With this Policy, the Company, in compliance with the provisions of Article 5(1)(e) of Legislative Decree no. 24/2023, provides clear information on the aforementioned channel, on the procedures and prerequisites for making internal reports, as well as, in Sections 15 and 16 below, on the channel, procedures and prerequisites for making external reports.

This Policy shall be displayed on the notice board in the workplace and, in order to be easily visible, shall be published in a special section of the Company's website, so as to be accessible also to persons who, although not frequenting the workplace, fall within the categories of possible whistleblowers, summarised below.

With this Policy and the adoption of the internal reporting channel, moreover, the Company does not limit itself to implementing tools to prevent possible unlawful conduct, but also intends to promote a corporate culture of combating illegality, through the active and responsible participation of all employees and third parties.

2. Persons who may make reports

2.1 The Company encourages its employees and third parties to promptly report conduct that constitutes or may constitute unlawful conduct and/or a violation of the law affecting the integrity of the Company of which they have become aware in the context of their work.

In accordance with and in compliance with the provisions of Legislative Decree 24/2023, the persons who may make a report are the following ('Whistleblowers')

- All personnel of the Company, including part-time, intermittent, fixed-term, temporary or apprenticeship workers or those performing occasional services
- Self-employed workers who work for the Company;

- The holders of an agency, commercial representation and other collaborative relationship with the Company that results in the performance of continuous and coordinated work, mainly personal, even if not of a subordinate nature;
- workers and collaborators who perform their work for third parties in the public or private sector that supply goods or services or perform works in favour of the Company;
- freelance professionals and consultants who work for the Company;
- volunteers and trainees, paid and unpaid, who work for the Company;
- shareholders and persons with functions of administration, management, control, supervision or representation of the Company, even if such functions are exercised on a de facto basis.

2.2. Reports may also concern facts known

a) before the establishment of the employment relationship, during the selection process or in other pre-contractual stages;
b) b) during the probationary period;
c) c) after termination of the legal relationship if the information on breaches was acquired during the course of the relationship.

2.3. It should be noted that, in accordance with the provisions of Legislative Decree no. 24/2023, the protection afforded to Whistleblowers under such legislation, as described in letter b) of paragraph 13 below of this Policy, also applies to the following persons:

I. facilitators, i.e. natural persons who assist a reporting person in the reporting process, working within the same employment context and whose assistance must be kept confidential
II. persons in the same employment context as the reporting person and who are bound to the reporting person by a stable emotional or family relationship up to the fourth degree of kinship
III. co-workers of the reporting person who work in the same work environment as the reporting person and who have a regular and current relationship with this person
IV. the entities owned by the reporting person for which the same person works, as well as the entities that work in the same work environment as the reporting person

3. Subjects covered by the Reports

3.1. The protection measures provided for by the legislation and described in paragraph b) of paragraph 13 below of this Policy shall apply to Whistleblowers and to the persons indicated in paragraph 2.3 above of this Policy if, at the time of the report, the Whistleblower had reasonable grounds to believe that the information on the reported breaches was true and fell within the objective scope of the whistleblowing legislation referred to in this Policy in this paragraph 3.

Therefore, mere supposition or rumours as well as news in the public domain are not sufficient.

The information on breaches to be reported may concern both breaches committed, including well-founded suspicions, and breaches not yet committed that the reporter reasonably believes could be committed on the basis of concrete elements. Elements concerning conduct aimed at concealing violations may also be reported.

It should also be noted that the reportable breaches must be capable of damaging the integrity of the Company and must be learnt by the Whistleblower in the context of his or her work, understood in a broad sense and therefore intended to include also the persons indicated in paragraph 2.1 above.

Reports made in the knowledge of the abuse/instrumentalisation of this Policy, e.g. those that are manifestly unfounded, opportunistic and/or made for the sole purpose of damaging the Reported Person or other persons mentioned in the Report (employees, members of corporate bodies, suppliers, partners, etc.) shall be considered to be in bad faith/grievous misconduct (and therefore a source of liability, in disciplinary and other competent fora).

3.2. Information on violations of specific national and European Union regulations identified by Legislative Decree 24/2023 and summarised below must be reported to the Company.
In particular, within the framework of the Company, taking into account its organisational and governance structure and in line with the indications contained in the Operating Guide adopted by Confindustria, the following violations may be reported (hereinafter, 'Reporting'):

(a) Offences committed in breach of the EU legislation listed in Annex 1 to Legislative Decree No. 24/2023 and of all national provisions implementing it (even if the latter are not expressly listed in the said Annex). In particular, these offences relate to the following areas:
i. public contracts;
ii. financial services, products and markets and prevention of money laundering and terrorist financing;
iii. product safety and compliance;
iv. transport safety;
v. environmental protection;
vi. radiation protection and nuclear safety;
vii. food and feed safety and animal health and welfare;
viii. public health;
ix. consumer protection;
x. privacy and protection of personal data and security of networks and information systems.

b) Acts or omissions affecting the financial interests of the European Union (Art. 325 TFEU fight against fraud and illegal activities affecting the financial interests of the EU) as identified in EU regulations, directives, decisions, recommendations and opinions.

(c) Acts or omissions relating to the internal market that jeopardise the free movement of goods, persons, services and capital (Article 26(2) TFEU). This includes violations of EU competition and state aid rules, corporate tax rules and mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law.

(d) Acts or conduct that frustrate the object or purpose of EU provisions in the areas indicated in the preceding points.

4. Facts that CANNOT be reported

The following circumstances are excluded from the scope of this Policy and therefore CANNOT be reported:
a) complaints, claims or requests linked to an interest of a personal nature of the Whistleblower that relate exclusively to his/her individual employment relationships, or inherent to his/her employment relationships with hierarchically superior figures, or concerning data processing carried out in the context of an individual employment relationship in the absence of an infringement of the integrity of the Company. Therefore, reports concerning, for example, labour disputes, discrimination between colleagues, interpersonal conflicts between the reporting person and another worker are excluded

b) reports of breaches that are already mandatorily regulated by specific regulations set out in Legislative Decree 24/2023 and which therefore do not fall within the scope of the latter decree (e.g. the banking and financial intermediation sector)

(c) reports of violations relating to national security, as well as of contracts relating to defence or national security aspects.

5. Elements to be included in the Report

The Company invites the Whistleblowers to make Reports that are as circumstantial as possible, so as to provide the useful and appropriate elements to allow an appropriate verification of the merits of the facts reported. It is particularly important that the Report includes, where such elements are known to the Reporting Party

- the circumstances of time and place in which the reported fact occurred
- the description of the fact
- the personal details or other elements allowing to identify the person to whom the reported facts are attributed.

These elements, in fact, are also relevant for the purpose of assessing the admissibility of the Report, as explained in paragraph 10 below of this Policy.

It is also useful to attach documents that may provide evidence of the facts being reported, as well as an indication of other persons potentially aware of the facts.

6. Channels for sending the Report

Reports may be made by various means described in the following paragraphs of this Policy and briefly summarised below:

a) telematically, through the special Portal made available by the Company and accessible at the following link https://private.mygovernance.it/mywhistleblowing/cbm/95900

b) orally, by means of a voice message recorded through the specific functionality available on the Portal;

c) by means of a direct meeting with the Managers (as identified below), at the request of the reporter.

7. The Telematics Channel: The Whistleblowing Portal

7.1. The Company has adopted its own internal whistleblowing channel by firstly providing an on-line platform for the telematic submission of whistleblowing Reports (hereinafter the "Portal"), which guarantees, also by means of encryption tools, the confidentiality of the identity of the person making the Report, of the person involved and of the person in any case mentioned in the Report, as well as of the content of the Report and of the relevant documentation.

The Portal can always be reached through the following link https://private.mygovernance.it/mywhistleblowing/cbm/95900 published on the Company's website, in the special section dedicated to Whistleblowing Reports.

In any case, both the Policy and the access link to the Portal for sending Reports will always be available in the special section of the Company's website at the following link:
https://www.cbm-srl.com/whistleblowing.html

7.2. The Whistleblower may send his/her Reports by means of the functions made available on the Portal and described below, which, in compliance with the prescribed confidentiality requirements, allow a Report to be sent electronically via the Portal itself.

Access to the Portal is subject to the "no-log" policy in order to prevent the identification of the Reporting Subject who wishes to remain anonymous. This means that the architecture of the Portal does not allow logging of access to the application, in order to protect the confidentiality of the identity of Whistleblowers even when using the company network.

The Company suggests that you send a Report providing your contact details in order to allow the Reporting Managers (as identified below) to acquire any further information and thus carry out investigations in a fruitful manner.

In any case, the anonymous report, if deemed admissible, shall be handled by the Company in the same way as a whistleblowing report according to the procedure described in this Policy, insofar as compatible. The anonymous Whistleblower, therefore, if subsequently identified, shall be guaranteed the safeguards and protection provided for by the whistleblowing legislation and referred to in this Policy.

7.3. In order to make a Whistleblowing Report through the Portal, the Whistleblower, subject to disclosure pursuant to Article 13 GDPR, must register on the Portal and create his/her own personal area. The Reporting Party will be assigned a unique user profile with confidential authentication credentials (User ID and password) in accordance with security standards that comply with industry best practices. In any case, the architecture of the Portal does not allow direct access to the registration data by the management functions.

On his or her personal page, the Reporting Officer will be able to view the status of the Reports he or she has sent, depending on the progress of the Report management process. In order to create a new Report, the Reporting Subject may click on the "Create Report" button and, through the Portal, he/she will be guided through each step of the Report creation process and will be asked to fill in a series of fields in order to better substantiate the Report, in compliance with the requirements.
In particular, the first page of the reporting process will open, which requires the reporting agent's data. The latter may choose to remain anonymous by ticking the relevant box. On the following screens, the reporter will be asked to provide more details of the facts, by filling in some fields, such as: the company where the event occurred (e.g. at a supplier), the date, place and author of the facts and the company function to which the facts refer. The Whistleblower must also provide a brief description of the facts reported, may attach documents and indicate from a drop-down menu the type of breach to which the Report refers. Finally, before sending the Report, the Reporting Party will be asked to indicate an e-mail address in order to receive notifications on the status of its Report. These notifications will not contain any data related to the Report, but will inform the reporter of the progress of the Report. In order to view the contents of the progress reports, the Reporting Party must access the Portal.
The Company requests that the company e-mail address not be used for such notifications, even if the e-mail address indicated on the Portal by the Reporting Party is not visible to Managers in any case.

The Portal also makes it possible to establish secure communication between the reporter and the recipient, ensuring, at the reporter's request, anonymity.

8. Channel in oral form.

(a) recorded voice message

In the case of a Report sent using the recorded voice messaging system available on the Portal, the voice will be automatically masked and rendered unrecognisable by special software. Subject to the Reporter's consent, the Report thus acquired will be documented by recording it through a special feature of the Portal that allows it to be stored and listened to, and by transcription by the Handlers (as identified below), a transcription that will also be stored on the Portal with the guarantees of security and confidentiality that this ensures. The reporter may verify, rectify or confirm the content of the transcript by signing it. In this case, the transcript will also be signed by the aforementioned Handlers.

b) face-to-face meeting

When, at the request of the Reporting Party, the Report is made orally in the course of a meeting with the Managers' Committee (as identified below) - also by means of a remote videoconference session, if any - it is documented by the Committee itself in minutes that the Reporting Party may verify, rectify and confirm by signing. The minutes will also be signed by the Handlers. The Whistleblower will be given the privacy notice at the beginning of the meeting. The notice is in any case always available as an annex to the Whistleblowing Policy.

The Whistleblower may request the meeting by voice message on the Portal, in order to ensure confidentiality. The meeting will be scheduled by the Manager within a reasonable time.

9. Reporting Managers

The Company has adopted the following method for handling Reports, taking into account the organisation of the company.

9.1. Reports sent through the Portal are received exclusively by a Committee made up of three managers, two of whom are appointed within the organisation and one represented by an external professional, specifically appointed by the Company. The two internal members of the Committee are specifically trained by the Company, both on the subject of whistleblowing and with regard to the related privacy implications, and authorised by the Company itself to manage the channel and the Reports. The Company guarantees that these persons operate autonomously and with guarantees of independence in the performance of these functions. The external professional has been identified by the Company because, by virtue of his experience and professionalism, he guarantees the requisites of autonomy, independence and specific training suitable to ensure the management of the Reports in compliance with the legislation and the respect of confidentiality, data protection and secrecy required.

The above-mentioned Managers' Committee (hereinafter also referred to as the "Committee") is specifically composed of:

-
- Technical, RSPP and Regulatory Manager of Società Sigurtà Gianluca
- Head of Human Resources and Administration Barbara Mussi
- Lawyer Maurizio Ruschetta of the Court of Milan

all expressly appointed and authorised by the Company to receive and handle Reports.

Should situations of conflict of interest, even if only potential, emerge upon receipt of the report by one or two of the Managers, the management of the Report shall be the responsibility of the Manager(s) not in conflict.
Therefore, the Company, by means of this Policy, requires all potential reporting parties to address - through the functions provided on the Portal - the Report to the non-conflicting Manager(s), if they have a well-founded suspicion that there is a situation of conflict of interest of one or more of the Managers.
The same Managers' Committee mentioned above is also competent to receive and handle Reports sent through the voice messaging system or through face-to-face meetings.

In any case, an internal Report submitted to a person other than the one indicated above is transmitted, within seven days of its receipt, to the competent person, with simultaneous notification of the transmission to the reporting person.

The Company, with this Policy, hereby instructs all its personnel to immediately forward to the aforementioned Committee and in strict confidence any Reports they may erroneously receive.

9.2. In carrying out its management activities, the Management Committee
(a) give the Reporting Party an acknowledgement of receipt of the Report within seven days from the date of receipt;
b) maintains the interlocutions with the Reporting Party and may ask the latter, if necessary, for additions;
c) diligently follows up the Reports received;
d) provide acknowledgement of the Report within three months from the date of the acknowledgement of receipt or, in the absence of such notice, within three months from the expiry of the period of seven days from the submission of the Report.

Managers are also responsible for providing information on the use of the internal whistleblowing channel, on the procedures and prerequisites for making internal whistleblowing reports, as described in this Policy, as well as, also by referring to the provisions of paragraphs 15 and 16 below, for providing information on the channel, procedures and prerequisites for making external whistleblowing reports.
It is also reiterated that any anonymous report, if deemed admissible, shall be handled by the Company in the same way as a whistleblowing report according to the procedure described in this Policy, insofar as compatible.
The anonymous Whistleblower, therefore, if subsequently identified, will be guaranteed the safeguards and protection provided for by the whistleblowing legislation and referred to in this Policy.

10. Preliminary Examination of the Report.

a) Verification of the admissibility of the Report

Upon receipt of the Report, the Committee of the Managers, as identified above, proceeds preliminarily to verify the existence of the subjective and objective conditions for making an internal report. At the end of this preliminary check, if none of the aforementioned conditions are met, the Committee dismisses the report as inadmissible.

b) Verification of admissibility of the Report

Once it has been verified that the Report meets the subjective and objective requirements defined by the legislator and is therefore admissible, it is necessary to check its admissibility as a whistleblowing report.

It should be noted that the Report must clearly indicate the circumstances of time and place in which the reported fact occurred, a clear and circumstantiated description of the facts, personal details or other elements enabling identification of the person to whom the reported facts are attributed.

The Report is considered inadmissible and is filed for the following reasons:
a) generic content of the Report such as not to allow comprehension of the facts, or report of offences accompanied by inappropriate or irrelevant documentation
b) lack of data constituting the essential elements of the report
c) manifest groundlessness of the facts constituting the essential elements of the report
d) production of only documentation in the absence of the report of unlawful conduct.

Where the Report is not adequately substantiated, the Handling Committee may request additional elements from the Whistleblower through the secure communication system of the Portal, or even in person, if the Whistleblower has requested a direct meeting.

At the end of this preliminary examination, if the Report proves to be inadmissible or inadmissible, the Committee archives the Report, ensuring the traceability of the supporting reasons.

11. Investigation and fact-finding

Once the admissibility of the Report has been assessed, the persons entrusted with the management of the reporting channel initiate the internal investigation of the reported facts or conduct in order to assess their existence.

The investigation activities will be carried out in compliance with the obligation of confidentiality of the identity of the Whistleblower and of the other protected persons, and ensuring timeliness and compliance with the principles of objectivity, competence and professional diligence.

The Committee of the Handlers must ensure that the necessary checks are carried out, always taking care that the confidentiality of the Whistleblower, of the reported person and of the other persons protected by the legislation (e.g. facilitators and persons mentioned in the report) is not compromised, by, for instance

- directly acquiring the information necessary for the assessments through the analysis of the documentation/information received;
- by involving other corporate structures or even external specialised subjects (e.g. IT specialists) in view of the specific technical and professional skills required;
- hearing of any internal/external subjects, etc.

If it proves necessary to avail itself of the technical assistance of third party professionals, as well as of the support of the staff of other corporate functions/departments - in order to guarantee the confidentiality obligations required by the legislation - the Committee of the Managers shall obscure any type of data that might allow the identification of the reporting person or of any other person involved (e.g. facilitator or other persons mentioned in the report).

At the end of the investigation, the Management Committee prepares a final report containing at least
- the facts established;
- the evidence gathered
- the causes and deficiencies that allowed the reported situation to occur.

If the report proves to be well-founded, the Committee of Managers - always in compliance with the confidentiality obligations established in this policy - activates the relevant company managers to take the due and most appropriate mitigating and/or corrective actions.

Moreover, in the event of a well-founded report, the Committee of Managers shall forward the outcome of the investigation to the competent function for the possible initiation of disciplinary proceedings aimed at imposing, where appropriate, disciplinary sanctions in line with the provisions of the applicable legislation and collective labour agreements of reference, as well as to the company management for the appropriate assessment of any further action to be taken, also for the protection of the Company.

In fact, it is not up to the Managers' Committee to assess individual responsibilities and any subsequent measures or proceedings.
The phases of the investigation activity are properly traced and filed depending on the type of reporting channel used (for example, if the Portal was used, the documentation will be filed within it according to the security measures adopted therein and, if the minutes of the hearing of the in-person meeting were drawn up, they will be filed within a folder accessible only to the Committee of Managers).
In any case, pursuant to the provisions of Legislative Decree no. 24/2023, during the investigation and assessment phases of the Report, the identity of the Reporting person, of the reported person and of all the persons involved and/or mentioned in the Report is always protected.

12. Feedback to the reporter

At the end of the preliminary investigation, and in any case within the aforementioned term of 3 (three) months, the Committee of the Managers shall provide feedback to the Whistleblower on the action taken or intended to be taken on the Report, giving an account of the action taken to assess the existence of the facts reported, the outcome of the investigations and any measures taken or to be taken.

At the expiry of the aforementioned deadline, the acknowledgement may be of a definitive nature if the investigation has been completed, or of an interlocutory nature on the progress of the investigation, if it has not yet been completed, for instance due to the complexity of the case.

Therefore, at the end of the three-month period, the Committee of Managers may inform the reporting person

- that the report has been dismissed, giving its reasons;
- whether the report is well-founded and forwarded to the competent internal bodies;
- the activity carried out so far and/or the activity it intends to carry out if the investigation has not yet been completed.

In the latter case, the Handling Committee will in any case also inform the Reporting Party of the subsequent final outcome of the investigation of the Report (archiving or ascertainment of the merits of the Report and transmission to the competent bodies).

13. Protection of the reporter

The first protection placed by the legislator in favour of the Whistleblower is the obligation to guarantee the confidentiality of the Whistleblower's identity from the moment of receipt of the Report and in any subsequent stage.
Moreover, the legislation prohibits any form of retaliation against the Whistleblower, understood as any conduct, act or omission, even if only attempted or threatened, occurring in the work context and causing - directly or indirectly - unfair damage to the protected persons.
To this end, in compliance with current legislation, the Company has set up a series of mechanisms aimed at protecting the non-anonymous Whistleblower, providing for
a. the protection of the confidentiality of the identity of the Whistleblower
b. the prohibition of retaliation against the Whistleblower
Finally, a further protection granted by Legislative Decree 24/2023 to the Whistleblower is the limitation of his liability with respect to the disclosure and dissemination of certain categories of information, which would otherwise expose him to criminal, civil and administrative liability.

(a) Duty of confidentiality

Confidentiality is guaranteed for every mode of reporting, therefore, whether it is made through the Portal or by voice message or face-to-face meeting.

In fact, it is specifically instructed to maintain the confidentiality of both the identity of the Whistleblower, the content of the Report and its documentation, and the identity of the Whistleblower and of any persons mentioned in the Report.

The Portal also guarantees the confidentiality of the reporter's identity by means of encryption tools, both in transit and at rest. The credentials assigned to users (both Whistleblowers and Managers) are unique and confidential and comply with the security requirements of industry best practices. Only the Committee of Managers can access the content of the Report.

The identity of the Reporting person and any other information from which such identity may be inferred, directly or indirectly, will not be disclosed without the express consent of the Reporting person himself or herself, to persons other than the Managers' Committee, competent to receive or follow up on the Reports, expressly authorised and instructed to process such data in accordance with Articles 29 and 32(4) of Regulation (EU) 2016/679 (GDPR) and Article 2-quaterdecies of the Personal Data Protection Code under Legislative Decree No 196 of 30 June 2003.

In the context of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the allegation of the disciplinary charge is based on separate investigations additional to the report, even if consequent to it.

If the accusation is based, in whole or in part, on the Report, and knowledge of the identity of the Reporting person is indispensable for the accused's defence, the Report will be usable for the purposes of the disciplinary proceedings only if the Reporting person has given his/her express consent to the disclosure of his/her identity.

Similarly, in the event that in the internal reporting procedures the disclosure of the identity of the Whistleblower is also indispensable for the defence of the person concerned, the identity of the Whistleblower may be disclosed only after obtaining the express consent of the Whistleblower.

In both the aforementioned cases, in addition to the acquisition of the Whistleblower's consent, the Whistleblower himself/herself shall in any case be notified, by written communication, of the reasons for the disclosure of the confidential data.

The Company shall protect the identity of the persons involved (the reported persons) and of the persons in any case mentioned in the report until the conclusion of the proceedings initiated on account of the report, in compliance with the same guarantees provided for in favour of the reporting person. This is without prejudice to the right of the Company to report the facts before the Judicial Authority.

Breach of the obligation of confidentiality constitutes a source of disciplinary liability under the provisions of the disciplinary system adopted by the Company, without prejudice to any further liability provided for by law.

b) Prohibition of retaliation

The Company guarantees the Whistleblower protection against any act of harassment, retaliation or discrimination for reasons directly or indirectly linked to the Report made in good faith. Any act of retaliation or discrimination against both the Whistleblower and the persons indicated in paragraph 2.3. above of this Policy (e.g. facilitators) is prohibited.

Retaliation is understood as any conduct, act or omission, even if only attempted or threatened, put in place by reason of the report, and which causes or may cause the Whistleblower, directly or indirectly, unjust damage.

Retaliatory acts resulting from a Whistleblowing are in any case null and void.

The protection provided by the legislation and set out in this paragraph also applies to anonymous Reports, if the Whistleblower is subsequently identified and retaliated against.
The Company shall take the actions it deems appropriate against anyone who carries out, or threatens to carry out, acts of retaliation against the Whistleblower. If an employee believes that he/she has suffered retaliation because of the report made, he/she may inform the Committee of Managers, which will take action to protect the Whistleblower in accordance with the law.

If the criminal liability of the Whistleblower for the offences of defamation or slander or his civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is ascertained, even in a court of first instance, the protections referred to in this letter b) are not guaranteed and a disciplinary sanction is imposed on the Whistleblower.

Whistleblowers and the persons indicated in paragraph 2.3. above of this Policy may also inform ANAC of the retaliation they believe they have suffered.

Therefore, any person who believes that he has suffered retaliation, even attempted or threatened retaliation, as a result of a report may communicate it to the ANAC, which will have to ascertain the causal link between the retaliation and the report and, therefore, adopt the consequent measures.

In particular, if the Authority considers the communication to be inadmissible, it will file it; if, on the other hand, it ascertains that it is well-founded and that there is a causal link between the report and the retaliation, it will initiate the sanctioning procedure.

The ANAC informs the National Labour Inspectorate for the measures falling within its competence.

There are some cases in which the Whistleblower loses protection: i) if the criminal liability of the Whistleblower for offences of defamation or slander is established, even by a judgment of first instance, or if such offences are committed with the report to the judicial or accounting authorities; ii) in case of civil liability for the same title due to wilful misconduct or gross negligence. In both cases, a disciplinary sanction shall be imposed on the reporting or whistleblowing person.

c) Limitation of liability for the reporter

Pursuant to Legislative Decree 24/2023, the Whistleblower shall not be held liable either criminally or in civil and administrative proceedings for the following cases

- disclosure of information on violations covered by secrecy other than professional forensic and medical secrecy and other types of secrecy provided for by Article 1, paragraph 3 of Legislative Decree 24/2023
- breach of the provisions on copyright protection;
- breach of the provisions on the protection of personal data;
- disclosure or dissemination of information on violations that offend the reputation of the person involved.

However, Legislative Decree 24/2023 imposes two conditions on the operation of the aforementioned limitations of liability:

1) that at the time of disclosure or dissemination there are reasonable grounds for believing that the information is necessary to disclose the reported breach
2) that the report is made in compliance with the conditions laid down in Legislative Decree 24/2023 for benefiting from the protection against retaliation (reasonable grounds for believing that the facts reported are true, the breach is among those reportable and the terms and conditions of access to the report are complied with).

In any case, it should be borne in mind that liability is not excluded for conduct that
- are not related to the reporting
- are not strictly necessary to disclose the breach; and
- constitute an unlawful acquisition of information or access to documents.

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

14. Data Processing and Retention of Reports

The processing of the personal data of the persons concerned (Whistleblowers, persons mentioned in paragraph 2.3 of this Policy above, person involved, persons mentioned in the Whistleblowing) for the purpose of managing the Whistleblowing is carried out by the Company, as Data Controller, in accordance with Regulation 679/2016 (GDPR) and for the sole purpose of managing and following up the Whistleblowing.

The processing is necessary in order to implement the legal obligations provided for by the whistleblowing regulations set out in Legislative Decree 24/2023, compliance with which is a condition for the lawfulness of the processing pursuant to Articles 6(1)(c) and (2) and (3), 9(2)(b) and Articles 10 and 88 of the GDPR.

Processing will be conducted in accordance with the principle of minimisation and, therefore, personal data that are manifestly not useful for the processing of a specific Report are not collected or, if accidentally collected, are deleted immediately.

The processing of personal data relating to the receipt and management of Reports shall be carried out, pursuant to Article 4 of Legislative Decree 24/2023, exclusively by the Manager, as a person expressly authorised and instructed by the Data Controller to manage the reporting channel pursuant to Article 29 of the GDPR, in compliance with the principles set out in Articles 5 and 25 of the GDPR.

The Company has also carried out a data protection impact assessment with reference to the processing connected to the management of the Reports and has therefore identified technical and organisational measures suitable to guarantee a level of security adequate to the specific risks arising from the processing carried out in this context.

Furthermore, the Company has regulated the relationship with the provider of the IT portal pursuant to Article 28 of the GDPR.

The Reports and the related documentation are kept for the time necessary for the processing of the Report and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with the aforementioned confidentiality obligations and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679.

For further details regarding the processing of data, please refer to the full privacy policy, published for all data subjects (including the reported person) on the Portal and available as an annex to this Policy and then disseminated to the recipients together with this Policy.

In any case, the privacy policy is always available on the Portal, as well as provided to the Reported Person, on the Portal itself, at the time of registration and at the end of the process for sending each Report.

15. Information on the external reporting channel established at ANAC

ANAC has activated an external reporting channel that guarantees, through the use of encryption tools, the confidentiality of the identity of the reporter, the person involved and the person mentioned in the report, as well as the content of the report and the related documentation.
External Reports must be transmitted only to ANAC as the only body competent to handle them. The IT platform and information on the procedures for sending external Reports to ANAC is available at the following link https://www.anticorruzione.it/-/whistleblowing.

16. Conditions for External Reporting

The Whistleblower may make an External Report if, at the time of its submission, one of the following conditions is met

a) the mandatory activation of the internal reporting channel is not envisaged within his/her work context, or this channel, even if mandatory, is not active or, even if activated, does not comply with the legislation;
b) the Whistleblower has already made an internal report in the manner set out in this Policy, and the report has not been followed up;
c) the Whistleblower has well-founded reasons to believe that, if he/she were to make an internal report, it would not be effectively followed up, or that the same report could give rise to the risk of retaliation
d) the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

17. Training and Communication

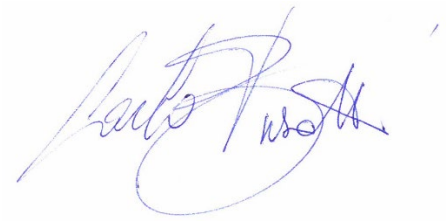
Training and communication are fundamental elements for the effective implementation and application of the Policy. In this regard, the Company undertakes to ensure that the Whistleblower is made aware of the provisions included in the Policy and to provide its staff with training programmes on whistleblowing legislation, confidentiality obligations and this Policy, including the procedures and operating methods adopted by the Company to manage the internal whistleblowing channel for all employees.

This Policy will in any case be published on the Company's website and available at the following link https://www.cbm-srl.com/whistleblowing.html.

18. Policy Update

The Policy and the Portal will be periodically updated in order to ensure constant alignment with the regulations and due to the evolution of the company's operations and organisation.

Torre de' Picenardi, 08/10/2026,



_____

Carlo Busatti
Amministratore Unico C.B.M. Srl

Attachment: Privacy Policy in accordance with Articles 13 and 14 of EU Regulation 679/2016 (GDPR)