STUDIO LEGALE
TRIBUTARIO
CONSULENZA
FINANZIARIA

WHISTLEBLOWING POLICY

PACKAGING AUTOMATION

Approved on 14 December 2023

Florence - Piazza Libertà 9, 50129 - Tel. +39 055 483448 - Fax +39 055 488674 - **Rome** - Via in Arcione 71, 00187 - Tel. +39 06 69924880 - Fax +39 06 69380330
Milan - Via Fratelli Gabba 5, 20121 - Tel. +39 02 86891146 - segreteria@bllex.it - **www.bllex.it**

STUDIO LEGALE
TRIBUTARIO
CONSULENZA
FINANZIARIA

Index

1. Introduction

Law No. 179 "Provisions for the protection of persons who report crimes or irregularities that have come to their attention in the course of a public or private employment relationship" (published in the Official Journal, General Series No. 291 of 14 December 2017) entered into force on 29 December 2017. The structure of the measure differentiates between the public sector (Art. 1) and the private sector (Art. 2) and adds a provision on the obligation of official, corporate, professional, scientific and industrial secrecy (Art. 3).
As far as the private sector is concerned, Article 2 of Law No. 179/17 intervened in regard to Decree 231/2001 and introduced a new provision in Article 6 ("Persons in top management positions and organisational models of the entity"), which also framed the measures related to the submission and management of reports within the Organisational Model pursuant to Legislative Decree 231/01.
Subsequently, on 10 March 2023, Legislative Decree No. 24 of 10 March 2023 (hereinafter the "Decree") was published in the Official Journal, implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, concerning the "protection of persons who report breaches of national or European Union law affecting the public interest or the integrity of the public administration or private entity, of which they have become aware in a public or private context" (hereinafter the "Directive").
In summary, the new rules provide for:
- the obligation for all private entities with more than 50 employees to establish internal reporting channels;
- the possibility, not only for employees but also for other persons referred to in Article 4 of the Directive, to report breaches of Union law in several areas, including: (i) public procurement; (ii) financial services, products and markets and the prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) environmental protection; etc.;
- the activation of reporting channels that are “designed, implemented and operated in a secure manner that ensures the confidentiality of the reporting person's identity and the protection of any third party named in the report, and that prevents access by unauthorised personnel”; and that include “notice of receipt of the report to the reporting person within seven days of receipt”;

- the need to appoint impartial persons to receive and handle reports;
- the obligation to provide final feedback to the reporting person within 90 days;
- the obligation to take the necessary measures to prohibit any form of retaliation against persons who report breaches;
- the possibility for interested parties to resort to “external” reporting to ANAC and “disclosure” of the report in certain cases;
- the need to provide interested parties with clear information on the reporting channel, the procedures and the conditions for making “internal” and “external” reports (the information must be displayed and easily visible in the workplace and accessible to persons who do not frequent the workplace but have a legal relationship with the entity in one of the forms provided for by the Decree).

In order to give concrete application to the legislation in force, CMC provides whistleblowers with various reporting channels, including a specific “Whistleblowing Portal” capable of guaranteeing, by computerised means, the confidentiality of the reporting person’s identity in the management of whistleblowing activities.

2. Purpose of the Policy and addressees

The purpose of this Whistleblowing Policy (hereinafter the "Policy") is to govern the process of receiving, analysing and processing "internal" Reports, regardless of who submits and transmits such communications, including anonymously.

This Whistleblowing Policy (adopted after consultation with trade union representatives where established pursuant to Article 4, paragraph 1 of Legislative Decree No. 24/2023) is adopted by CMC. In particular, the addressees of this procedure (hereinafter referred to as "addressees") are:

- the top management and members of CMC's corporate bodies;
- employees;
- partners, clients, suppliers, consultants, collaborators and, in general, anyone who has a relationship of interest with CMC.

The "Reporting Person" [pursuant to Article 2(1)(g) of Legislative Decree No. 24/23 - "Reporting Person"] who has knowledge of facts that may be the subject of a report is requested to make the report immediately, using the procedures described below, and to refrain from carrying out any independent analysis and/or investigation.

3. Definitions

For the purposes of this policy, the following definitions apply:

«**ANAC**»: National Anti-Corruption Authority;

«**working environment**»: work or professional activities, present or past, carried out in connection with the relationships referred to in Article 3(3) or (4) of Legislative Decree 24/2023, in the context of which, irrespective of the nature of the same activity, a person acquires information on violations and in respect of which he/she could risk suffering retaliation in the event of a public disclosure or report to the judicial or accounting authorities;

«**public disclosure**»: the release of information on breaches into the public domain through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people;

«**facilitator**»: a natural person who assists a reporting person in the reporting process and who works in the same work context and whose assistance must be kept confidential;

«**information on violations**»: information, including well-founded suspicion, on violations that have been committed or which, on the basis of concrete elements, it is believed may have been committed, concerning the context of the Entity with which the reporting person has a legal relationship within the meaning of Article 3(1) or (2) of Legislative Decree 24/2023, as well as elements concerning conduct aimed at concealing such violations;

«**person concerned**» or «**reported person**»: a natural or legal person identified in the report as the person to whom the violation is attributed or as a person otherwise involved in the reported violation;

«**reporting person**»: a natural person who makes a report of a violation acquired in the course of his or her work;

«**Report Manager**»: a specially trained, independent external person responsible for managing the reporting channel;

«**Supervisory Board** (“**OdV”**)»: an external party with the required independence, professionalism and competence, appointed by the company to supervise the effective implementation of the Organisational, Management and Control Model adopted by the company pursuant to Legislative Decree no. 231/2001;

«**feedback**»: communication to the reporting person of information related to the handling of the report;

«**retaliation**»: any conduct, act or omission, even if only attempted or threatened, committed by reason of the report, which causes or is likely to cause unfair harm to the reporting person, directly or indirectly;

«**report**»: written or verbal communication through the channels indicated in the policy of information on violations;

«**external reporting**»: the communication of information on violations, submitted through the external reporting channel referred to in Article 7 of Legislative Decree 24/2023;

«**internal reporting**»: written or verbal communication of information on violations, submitted through the internal reporting channels referred to in Article 4 of Legislative Decree 24/2023;
«**investigation**»: the report handling process undertaken by the Report Manager to assess the existence of the reported facts, the outcome of the investigation and any measures taken;
«**violations**»: conduct, acts or omissions detrimental to the public interest or the integrity of the public administration or private entity and consisting of a breach of national and European law, as set out in detail in the following paragraph.

4. Whistleblowing

Whistleblowing means any report made in order to protect the integrity of the Company regarding irregularities, acts that are legally, administratively or criminally unlawful, as well as violations of the Code of Ethics/Conduct/Behaviour, Organisational Model 231, and internal procedures adopted by CMC, or any external regulations applicable to CMC, based on precise and concordant elements of fact, of which the Addressees have become aware by reason of the functions they perform. Reports must be made in good faith and must be supported by precise information so as to be easily verifiable.
In general, CMC encourages its employees to resolve any labour disputes through dialogue, including informal dialogue, with their colleagues and/or immediate supervisor.
Reports must be made in a spirit of responsibility, be in the public interest and fall within the types of non-compliance for which the system has been implemented.

4.1. Reporting channels

The Reporting Person must immediately report any breach or reasonable suspicion of a breach, through the channels indicated in the Policy.

Reports must be submitted through the following channels:
1. by e-mail to odv@cmcsolutions.com (solely with regard to reports of violations of the 231 Model);
2. by ordinary post, registered letter addressed to the Report Manager, Emanuele Boschi, and made out to “CMC Whistleblowing Report Manager” to be delivered to the following address: Piazza della Libertà no. 9, 50129 - Florence, at Studio BL, stating that the correspondence is "confidential";
3. via the Whistleblowing Portal adopted by CMC, the link to which can be found on the company's website in the 'sustainability' section;

4. with exclusive reference to the violations of the Model, via any other channels provided for by the Organisational Models adopted by the Company in accordance with Legislative Decree 231/01.

Anyone receiving a report outside the aforementioned channels is required to forward it without delay through those channels.
Reports made through channels 1 and 2 (e-mail: odv@cmcsolutions.com; registered letter to the Report Manager Emanuele Boschi and made out to "CMC Whistleblowing Report Manager" to be delivered to the following address: Piazza della Libertà no. 9, 50129 - Florence, at Studio BL) will be received by the Supervisory Board in its capacity as Report Manager.
Reports made through channel 3 (Whistleblowing Portal set up by CMC) will be received by the Supervisory Board in its capacity as Report Manager.
Reports - relating exclusively to violations of the MOGC and its attachments - sent through channel no. 4 (any other channels provided for by the Organisational Models) will be received by the Supervisory Board.
Reports may also be made verbally to the aforementioned individual as described above. Internal verbal reports can be made:

i. through the portal, via a special voice recording function, with the option of altering the reporting person's voice, if the latter wished to make an anonymous and not merely confidential report;
ii. via phone line (Tel. 055 483448) through which it is possible to request to speak directly with the Report Manager;
iii. at the request of the reporting person, by means of a face-to-face meeting requested from the Supervisory Board in its capacity as Report Manager, and arranged by the latter within a reasonable time frame at a location, necessarily different from CMC's premises, to be agreed in advance with the reporting person, favouring the needs of the same. With the reporting person's consent, the manager will prepare minutes of the meeting, which the reporting person will review, correct and sign. The minutes of the meeting, the report with any supporting documentation, and any other communication will be kept in a secure location accessible only to the Report Manager.

4.2. Content of reports

Reports should be as detailed as possible in order to allow for proper verification. For example, a report should contain the following elements:
• the identity of the person making the report (where the report is confidential and not anonymous), with an indication of the organisational unit to which they belong and/or the activity carried out for CMC;
• a clear and complete description of the facts reported and the circumstances of the time and place in which the facts occurred;

• elements that make it possible to identify the person who committed the reported facts;
• any other person who may have knowledge of the facts that are the subject of the report;
• any documents that may confirm the accuracy of the reported facts.

Reports must not concern grievances of a personal nature or claims/complaints that fall within the discipline of the employment relationship or relations with hierarchical superiors or colleagues, for which reference should be made to the various communication channels provided by CMC.
All substantiated anonymous reports (containing all objective elements necessary for the subsequent verification phase) will be considered for further investigation. Any reports received and deemed irrelevant will be archived without further investigation, without prejudice to the feedback to the person concerned, which must be provided within the deadlines established by Legislative Decree 24/23.

4.3. Handling of reports

Upon receipt of the report, the Supervisory Board, in its capacity as Report Manager, will acknowledge receipt of the report – via the IT platform – to the reporting party within 7 (seven) days and will then deal with the report itself. The Report Manager then verifies whether the report falls within the subjective and objective scope of Legislative Decree 24/2023. If, as a result, the report does not fall within the scope of the aforementioned Legislative Decree, the Report Manager will archive the report and notify the reporting person via the IT platform.
If the report falls within the scope of application of the aforementioned Legislative Decree, but is not sufficiently detailed, the Report Manager will formulate the appropriate requests for additions/clarifications to the reporting person through the Platform.
Reports are subject to the following procedure, aimed at establishing the reported facts.

4.4. Investigation

Preliminary phase:
The Supervisory Board in its capacity as Manager undertakes to provide initial feedback to the reporting person within a reasonable time and in any case not exceeding 90 days (3 months) from the date of issue of the acknowledgement of receipt.
Reports will be subject to a preliminary analysis in order to verify the existence of data and information useful for the assessment of the merits of the case.

In carrying out the aforementioned analysis, the Manager may request further information or documentation from the reporting party and, for specific aspects dealt with in the report and if deemed necessary, may seek the assistance of Company departments and/or external experts. The Manager may also obtain information from the persons involved in the report, who may also ask to be heard or produce written representations or documents. If, at the end of the preliminary analysis phase, it emerges that there are no sufficiently substantiated elements or that the facts reported are unfounded, the report will be archived with an explanation of the reasons. If, as a result of this phase, useful and sufficient elements emerge or can be inferred to assess the report as well-founded, the next stage of specific investigations will be initiated.

Specific investigations:

The Supervisory Board in its capacity as Report Manager shall:

i. initiate specific analyses, if deemed appropriate, using the Company's competent structures or external experts and appraisers;
ii. notify the person involved of the existence of the report, in order to protect his/her right of defence, always guaranteeing the confidentiality of the identity of the reporting person and of the other people involved and/or mentioned in the report;
iii. access all company data and documents relevant to the investigation, where deemed appropriate for the proper handling of the case;
iv. agree with the management in charge of the department concerned by the report on any "action plan" necessary to remedy the control "weaknesses" identified;
v. agree with the departments concerned on any initiatives to be taken to protect the Company's interests (e.g. legal action, suspension/deletion from the supplier register, etc.). The corporate departments involved must guarantee full cooperation to the Manager insofar as necessary to carry out the investigation, in compliance with the principles and guarantees provided for by the regulations;
vi. request, if possible, the initiation of disciplinary proceedings against the reporting person in the case of reports where bad faith and/or purely defamatory intent on the part of the reporting person is established, possibly also confirmed by the unfounded nature of the report itself.

The activities described above do not necessarily have to be carried out in order.

Conclusion of the investigation:

At the conclusion of the investigation, the Supervisory Board, in its capacity as Manager, will provide written feedback to the reporting person:

i. If it finds elements of manifest groundlessness in the report, it will proceed with duly motivated filing. If the Manager considers that the report is made for the sole purpose of damaging the reputation or harming or otherwise prejudicing the person concerned, it shall inform the CMC

Board of Directors so that any appropriate action can be taken against the reporting person.

ii. Should the report be deemed well-founded, the Manager shall prepare a report summarising the results of the investigation and the reasons for which the report was deemed well-founded, which shall be sent to the Board of Directors for it to take the measures it deems necessary. At the same time, the Manager shall inform the reporting person of the outcome of the report.

The aforementioned activities necessarily take place within 90 days of the report being acknowledged. The acknowledgement may also be merely interlocutory, since information may be provided on the investigative activities that the Report Manager intends to undertake and the progress of the investigation. Once the investigation has been completed, the reporting person should in any case be informed of the outcome.

5. Protection and liability of reporting persons

Valuing good faith and fairness on the part of the reporting person at the time of the report, he or she will only benefit from the protections if, at the time of the report, he or she had reasonable grounds to believe that the information about the reported, publicly disclosed or denounced violations was true.
In such cases, the identity of the reporting person must not be disclosed (this also applies to all the elements contained in the report from which the identification of the reporting person can be deduced, even indirectly), with the exception of the Report Manager, and the content of the report is not subject to access to administrative documents or to the right of generalised civic access.
This protection is also guaranteed in any criminal, accounting and disciplinary proceedings that may arise from the report.
The identity of the persons concerned and mentioned in the report shall also be protected.
No retaliation or discrimination, whether direct or indirect, even if only attempted or threatened, may be suffered by a person who has in good faith made a report. Any discrimination or retaliation will be declared null and void by the judicial authority.
In the context of any judicial or administrative proceedings or out-of-court disputes concerning the ascertainment of the conduct, acts or omissions prohibited under the Decree, the burden of proof is reversed and shall therefore be placed on the person who has carried out the aforementioned conduct, acts or omissions. The reversal of the burden of proof does not apply in favour of persons and entities other than the reporting person under Art. 5(3) (e.g. facilitators, colleagues).

It is not a punishable offence for a person to disclose or disseminate information on breaches that are:

i. Covered by the obligation of secrecy;
ii. Related to copyright protection;
iii. Relating to the protection of personal data;
iv. Such as to offend the reputation of the person concerned or denounced.

This exemption operates where "*at the time of disclosure or dissemination, there were reasonable grounds to believe that the disclosure or dissemination of the same information was necessary to disclose the breach and the reporting, public disclosure or denunciation to the judicial or accounting authorities was made in the required manner*".

In such cases, any further liability, whether civil or administrative, is also excluded. Furthermore, unless the act constitutes a criminal offence, liability, including civil or administrative liability, for the acquisition of or access to information on violations is excluded.

In addition, penalties are provided for those who violate the whistleblower protection measures, as well as penalties against the reporting person in the event that reports are made with malice or gross negligence, or are found to be false, unfounded, defamatory, or in any case made with the sole purpose of harming the Company, the reported person, or other persons affected by the report.

The same measures are extended to facilitators, persons in the same work environment as the reporting person or the complainant who have a stable emotional or family relationship up to the fourth degree of kinship, co-workers of the reporting person or the complainant who work in the same work environment and have a regular and current relationship, entities owned by or for which the reporting person or the complainant works, and entities operating in the same work environment as the reporting person or the complainant.

A reporting person who believes that he or she has suffered retaliation as a result of the report may inform ANAC of this fact.

Without prejudice to the administrative pecuniary sanctions falling within the competence of ANAC, if it finds that retaliation has been committed, the Company may take disciplinary measures against the person responsible.

By way of example, retaliation includes:

among others:

a) dismissal, suspension or equivalent measures;
b) downgrading or non-promotion;
c) change of duties, change of workplace, reduction of salary, change of working hours;
d) suspension of training or any restriction of access to it;
e) negative merit notes or references;
f) the adoption of disciplinary measures or any other sanction, including a fine;

g) coercion, intimidation, harassment or ostracism;
h) discrimination or otherwise unfavourable treatment;
i) failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
j) non-renewal or early termination of a fixed-term employment contract;
k) damage, including to the person's reputation, particularly on social media, or economic or financial loss, including loss of economic opportunities and loss of income;
l) improper listing on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
m) the early termination or cancellation of a contract for the supply of goods or services;
n) the cancellation of a licence or permit;
o) the request to undergo psychiatric or medical examinations.

6. Protection of persons concerned

The report is not sufficient to initiate any disciplinary proceedings against the person concerned. If, following concrete findings concerning the report, it is decided to proceed with the investigation, the person concerned may be contacted and given the opportunity to provide any necessary clarification.

7. Support measures

The support measures consist of information, assistance and advice free of charge on how to report and the protection against possible retaliation offered by national and European legislation; on the rights granted to those involved in reporting; on the terms and conditions of access to legal aid.
In this sense «*A list of Third Sector entities that provide reporting persons with support measures is established at ANAC. The list, published by ANAC on its website, contains the Third Sector entities that carry out, according to the provisions of their respective statutes, the activities referred to in Article 5(1)(v) and (w) of Legislative Decree No. 117 of 3 July 2017, and that have entered into agreements with ANAC*»

8. Reporting Methods

8.1 Whistleblowing Portal

The Whistleblowing Portal, referred to in Article 4(1) of Legislative Decree No. 24/23, can be accessed through the link (xxx) provided on the Company's website in the "sustainability" section. Access to the Whistleblowing Portal is subject to a "no-log" policy in order to prevent the identification of whistleblowers who wish to remain anonymous: this means that the Company's IT systems are not able to identify the access point (IP address) to the Portal, even if it is accessed from a computer connected to the Company's network. Reports submitted through the Whistleblowing Portal, whether written or verbal and in the language chosen by the reporting person, will be received and managed by the Supervisory Board of CMC in its capacity as Report Manager.

The personal data contained in the database are encrypted through the use of dedicated and different encryption keys. Only the Report Manager, enabled with specific functional profiles to access the system, tracked through logs, is allowed to consult the information on the platform.

With regard to written reports, the reporting person, after choosing whether to make a confidential or anonymous report, shall provide a brief description of the facts reported and the persons involved in the report. The reference category of the reported breach must then be chosen and any documents (e.g. pdf, images, videos) in the reporting person's possession that are suitable to support the report must be attached.

With regard to verbal reports, the reporting person will click on the appropriate box to start recording the voice message and, at the end of the recording, will be able to choose the option of distorting his/her voice in order to make the report anonymous. Also in this case, the reference category of the reported breach shall be chosen and any documents (e.g. pdf, images, videos) in the reporting person's possession that are suitable to support the report shall be attached.

At the time of submitting the report, the reporting person will be issued with an access code which must be retained in order to:

- Have access to the report made;
- Monitor its progress;
- Communicate with the Report Manager;
- Enter additional elements to substantiate the report;
- View the status of the report;
- Transmit further documents relevant to the report;

Send new messages - both written and verbal - to the Report Manager.

It will be the responsibility of the reporting person to keep the aforementioned code, as it cannot be recovered in the event of loss.

The Report Manager will be provided with a password to access the Portal and will be notified by e-mail or phone when a report is made, depending on the option selected.

Once received by the Report Manager, reports will be subject to the investigation procedure already described in section 4.4.

8.2. Postal submission

In the case of submission by post, the reporting person shall send the report in writing to the address indicated in paragraph 4.1, in a sealed envelope containing another sealed envelope containing the reporting person's details and a copy of his or her identity document. The report must include an e-mail address or a postal address to which the Report Manager can send relevant notifications. If this procedure is not followed, the report submitted by mail will be considered inadmissible.

9. External reporting

9.1 Conditions for external reporting

An external report may be made by the reporting person - at https://whistleblowing.anticorruzione.it/#/ - if, at the time of submission, one of the following conditions is met:
a) there is no mandatory activation of the internal reporting channel in his or her work context or this channel, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4;
b) the reporting person has already made an internal report in accordance with Article 4 and the report has not been acted upon;
c) the reporting person has reasonable grounds to believe that, if he or she made an internal report, it would not be effectively followed up or that the report might lead to a risk of retaliation;
d) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

9.2 External reporting channels

The National Anti-Corruption Authority (ANAC) activates an external reporting channel that guarantees the confidentiality of the identity of the reporting person, the person concerned and any person mentioned in the report, as well as of the content of the report and of the relevant documentation, including through the use of encryption tools. The same confidentiality shall be guaranteed even if the report is made through channels other than those referred to in the first sentence or reaches personnel other than those responsible for handling reports, to whom it shall in any case be transmitted without delay.

External reports are made in writing via the IT platform or verbally via telephone or voice messaging systems or, at the request of the reporting person, by means of a face-to-face meeting scheduled within a reasonable period of time.
An external report submitted to a party other than ANAC will be forwarded to the latter, within seven days of its receipt, with simultaneous notification of the forwarding to the reporting person.

10. Public Disclosures

The Decree provides that whistleblowers may publicly disclose information about breaches through the press, electronic media or any other means of dissemination capable of reaching a large number of people.
A whistleblower who makes a public disclosure will benefit from the protection provided by the Decree if, at the time of the public disclosure, one of the following conditions is met:
a) the reporting person has previously made an internal and external report, or has made an external report directly, under the conditions and in the manner set forth in this Policy, and has not received a response to the report;
b) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
c) the reporting person has reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there are well-founded fears that the recipient of the report may be colluding with or involved in the violation.

11. Periodic reporting

In the annual report to the Board of Directors, envisaged by the Organisational Models pursuant to Legislative Decree 231/01, the Supervisory Board, also in its capacity as the Report Manager, provides a summary report of all reports received, whether anonymous or confidential. This report contains the investigation procedure followed and the outcome of the analyses carried out.

12. Penalties

Penalties will be applied to anyone who violates the whistleblower protection measures, as well as to the reporting person in the case of reports made with malicious intent or serious misconduct, or which turn out to be false, unfounded, defamatory or otherwise made with the sole purpose of harming the Company, the reported person or other persons concerned by the report.

Without prejudice to other liability profiles, ANAC will apply the following administrative financial penalties to the person responsible:
a) from 10,000 to 50,000 euro if it finds that there has been retaliation or if it finds that the report has been obstructed or that an attempt has been made to obstruct it or that the obligation of confidentiality referred to in Article 12 has been breached;
b) from 10,000 to 50,000 euro if it finds that reporting channels have not been established, that procedures for making and handling reports have not been adopted or that the adoption of such procedures does not comply with Articles 4 and 5, or that the reports received have not been verified and analysed;
c) from 500 to 2,500 euro, in the case referred to in Article 16(3), unless the reporting person has been convicted, even at first instance, of offences of defamation or slander or, in any event, of the same offence as that for which the report was made to the judicial or accounting authorities.
The private-sector entities referred to in Article 2(1)(q)(3) shall provide for penalties against those found responsible for the offences referred to in paragraph 1 in the disciplinary system adopted pursuant to Article 6(2)(e) of Decree No 231/2001.
In this context:
- CMC employees shall be subject to the penalties provided for in their employment contracts and in the applicable *pro tempore* National Collective Labour Agreement (or equivalent document);
- CMC employees and members of the management and control bodies are subject to the sanctions as set out in the Disciplinary System adopted by the organisation;
- persons dealing with CMC other than the above-mentioned persons shall incur the penalties provided for in the contracts concluded with the same.
The penalty is imposed by the competent bodies on each occasion, irrespective of the initiation of proceedings by the judicial authority.
The right to be heard is in any case guaranteed.

13. Record keeping and Protection of Privacy

In order to ensure the management and traceability of reports and related activities, the Supervisory Board, in its capacity as Report Manager, will ensure that all supporting documentation of the report is archived for a period of five years from the conclusion of the report.
All personal data contained in the report (including any special categories and/or data relating to criminal convictions or offences), will be processed in accordance with Regulation (EU) 2016/679 and applicable data protection legislation. Information on the processing of personal data collected during the handling of reports can be found in the privacy policy prepared by CMC and made available on

the Whistleblowing Portal as well as at CMC's premises. Furthermore, the information notice may be requested from the Manager in the case of a face-to-face meeting.

14. Updating of the Policy

The Policy and functionality of the Portal will be periodically reviewed by the Supervisory Board in consultation with the General Counsel of CMC to ensure its constant alignment with relevant regulations.