1. Purpose

The CMSA reporting system allows employees to report, also anonymously, behaviours or facts that may damage the Company, even just from a reputational standpoint. This tool is compliant with Legislative Decree 24/2003, which protects whoever reports breaches of national / European Union laws learned in professional settings, both public and private.

Through the IT platform dedicated to whistleblowing, the CMSA personnel and third parties can report facts (including omissions) that have already happened or are likely to happen, and that are attributable to colleagues or third parties or may damage CMSA. The report may involve:

• Breaches of the Organization, Management and Control Model, pursuant to Legislative Decree 231/2001.

• Violations of CMSA Code of Conduct.

• Illegitimate actions or misconduct in breach of internal laws, regulations or procedures.

2. Who can report

A report may be submitted by:

• Both fixed-term and permanent CMSA employees, including candidates in the recruitment stage or in probation period.

• Trainees, while performing their activities.

• External coworkers and consultants.

• Workers from suppliers or subcontractors working for CMSA.

• Former coworkers or employees of suppliers, if the relevant information has been acquired during the professional relationship.

CMSA ensures the confidential management of anonymous reports, as long as the latter are detailed and relevant enough. The anonymous whistleblower may, at any time, decide to reveal his/her identity to access the protections in place against any retaliation.

3. What can be reported

The reports should involve facts (including omissions) that are attributable to CMSA external or internal people and may constitute:

• Breaches of Model 231, the Code of Conduct or internal laws.

• Offenses under Legislative Decree 231/2001 or European Union acts.

• Acts prejudicial to the EU financial interests or the internal market.

• Behaviours that may compromise the goals of European laws.

• Illegitimate actions falling within the scope of European Union or national acts (reported in the annex to Legislative Decree 24/23), with specific focus on:

- Public contracts.

- Prevention of recycling and funding of terrorism.

- Product safety and compliance.

- Transport safety.

- Protection of the environment.

- Protection of private life and personal data.

- Safety of networks and information systems.

The reports should be based on facts personally known and reasonable grounds to think that the information is truthful.

The following shouldn't be regarded as valid reports:

• Complaints or personal disputes related to one's own professional relationship.

• Interpersonal conflicts which aren't related to breaches of Model 231.

• Private events which aren't relevant for one's own professional activity.

The reports should be submitted as soon as possible, to allow an effective assessment of facts.

4. Internal reporting channels

The reports can be submitted through the following channels:

1. IT platform accessible from the company website (preferential channel);

2. Paper format, according to the ANAC guidelines (Deliberation no. 311, of 12 July 2023);

3. Verbal meeting with the designated staff (Internal Auditing or President of the Board of Directors).

The IT platform is the recommended tool, since it ensures more confidentiality as regards the whistleblower's identity and adequate IT safety measures.

The platform allows to:

• Send a new report.

• Update or integrate a report that had already been sent.

• Assess the progress status.

• Receive feedback on the outcome of the report.

5. External reporting and public disclosure

Legislative Decree 24/2023 allows to submit external reports to the Italian National Anti-Corruption Authority (ANAC) or to publicly disclose breaches, but only in the following cases:

• The internal channel isn't active or compliant to the law.

• The internal report did not lead to further action.

• The whistleblower has reasonable grounds to think that the internal report isn't effective or may lead to retaliation.

• The breach constitutes an impending or clear danger for public interest.

6. Protection of whistleblowers

The protections provided for by Legislative Decree 24/2023 do not just apply to the whistleblower, but also to:

• Whoever assists the whistleblower (facilitator) in the same professional setting.

• Family members and cohabiting persons, up to the fourth degree of kinship.

• Colleagues with a current and regular professional relationship with the whistleblower.

• Legal entities related to the whistleblower (e.g., companies owned by the whistleblower or where the latter works).

with the term retaliation, we refer to any acts, behaviours or omissions – even just threatened – which, following the report, may lead to wrongful (direct or indirect) damage to the whistleblower or any related subjects.

Examples of retaliatory behaviours

The following are regarded as retaliatory acts, among others:

• Dismissal, suspension or equivalent measures.

• Downgrading or non-promotion.

• Change of duties, relocation, reduction in salary or change of working hours.

• Limitation or exclusion from educational pathways.

• Negative assessments or unfavorable references.

• Disciplinary or financial penalties.

• Intimidation, harassment, isolation or coercion.

• Discriminatory or unfavorable treatments.

• Failure to convert a fixed-term contract into a permanent one, in presence of legitimate expectations.

• Failure to renew or terminate the contract early.

• Reputational damage, also through social media, or economic and professional losses.

• Insertion into informal lists that may impair future professional opportunities.

• Early termination of supply contracts.

• Revocation of licenses or permits.

7. Management of reports

Reports are received by Whistleblowing Managers and assessed jointly with the Legal Department. Their management is entrusted to a dedicated team, whose structure is defined periodically, in function of the crime to be reported.

• Feedback to the whistleblower: within 7 days of receipt of report (article 5, paragraph a, Legislative Decree 24/2023).

• Conclusion of the investigation: within 3 months of receipt of report or, in the absence of confirmation, within 3 months of the deadline of 7 days from the date of submission (article 5, paragraph d, Legislative Decree 24/2023).

8. Data retention

All reports are retained for 5 years, in a safe manner and compliant to the General Data Protection Regulation (GDPR).

9. Training and awareness

CMSA promotes the continuous training of staff members on reporting methods and rights and protections of the whistleblower, aimed at promoting a company culture focused on transparency and lawfulness.