Speak Up and Whistleblowing Policy

Purpose

This policy establishes the framework for submitting, receiving, managing, and monitoring reports of misconduct, thereby enhancing transparency, protecting whistleblowers, and ensuring the effective resolution of issues within the company.

This policy also supports the Company's commitment to fostering a "Speak Up" culture, encouraging employees and external stakeholders to raise concerns, questions or suspicions in good faith, even where these may not necessarily constitute a breach of law but may be inconsistent with the Company's values or ethical standards.

Forvis Mazars

This policy applies to the companies "Forvis Mazars Certified Public Accountants Business Advisors S.A", "Forvis Mazars Consulting Single Member P.C." and "Forvis Mazars Accounting Tax Single Member P.C." (hereinafter collectively "Forvis Mazars" or the "Company").

Policy Definitions

For the purposes of this Policy, the following terms have the following meanings:

- **"Report"**: Any information or complaint regarding an actual or potential violation of laws, regulations, internal policies, or practices of the Company, submitted through one of the approved reporting channels.
- "**Reporter**": The individual who submits a report, either by name or anonymously, under this policy. The term includes employees, contractors, suppliers, third parties, and any other person covered by the Scope of this policy.
- **"Individual Reported"**: The individual to whom the report relates or whose conduct is being examined as part of the investigation process.
- "Retaliation": Any form of adverse treatment, direct or indirect, directed against the reporter due to the submission of a report or cooperation in the investigation process, such as dismissal, demotion, threats, harassment, or discriminatory treatment. Retaliation is strictly prohibited under this policy.
- "**Reporting Channels**": The means and procedures established by the Company for submitting reports (electronically, in writing, verbally, by telephone, via a platform, or by mail).
- "**Report Receiving and Monitoring Officer (RRMO)**": The designated person appointed by the Company to receive, log, evaluate, anonymize, forward, and monitor the report, as well as to communicate with the reporter.
- "**Investigation**": The process of evaluating the details of the report, gathering additional information, examining the facts, and making a decision regarding the necessary corrective measures or other actions.
- "**Anonymous Report**": A report submitted without disclosing the reporter's identity. The Company takes appropriate measures at all stages of the process, to ensure the confidentiality and protection of the reporter, even when the reporter may become identifiable through additional information.
- "**Confidentiality**": The obligation to protect the identity of the reporter, the subject of the report, and any information related to the process, in accordance with data protection laws and the Company's internal procedures.

Subjects and Scope of Application

- This policy covers employees (salaried, non-salaried, self-employed, consultants, work-from-home shareholders, volunteers, paid and unpaid interns), executives, partners, suppliers, and third parties.
- Subject matter: violations of laws, regulations, and internal policies concerning, among other things, reports of violations of public contracts, the prevention of money laundering and terrorist financing, environmental protection, public health, the protection of privacy—including personal data—and the security of network and information systems, infringements affecting the financial interests of the European Union, infringements of European Union competition rules and breaches of corporate tax legislation.
- This policy also covers concerns relating to unethical behavior, inappropriate conduct, breaches of professional standards or any matter that may impact the integrity, reputation or values of the Company.
- Reports that fall outside the scope of this policy (e.g. personal employment grievances) may be redirected to the appropriate internal processes, where applicable.

Reporting Channels

- The Company has appointed a Report Receiving and Monitoring Officer (RRMO).
- Reports may be submitted in writing, electronically (email:*whistleblowing.gr@forvismazars.com* or via the platform on the website), by phone at +30 210699374 (ext. 211), in person, or by mail to the Company's headquarters in an envelope marked "For the Attention of the RRMO"
- For verbal reports, the Officer prepares a written summary, which the reporter may review, correct, and sign.
- The report may be submitted either by name or anonymously, with confidentiality guaranteed in all cases.
- Access to messages received at the above email address is restricted to authorized Company personnel with the right to handle reports of misconduct. The whistleblowing management team consists of four Company members, one of whom is the Compliance Officer, who act with complete confidentiality and integrity. The members of this team have signed a Confidentiality Agreement, particularly regarding the information they receive as members of the whistleblowing management team.

Role of the Report Receiving and Monitoring Officer (RRMO)

- Receives and logs reports.
- Ensures that receipt of the report is confirmed to the reporter within seven (7) business days of the date of receipt.
- Confirms that the complainant is provided with an update on the actions taken within a reasonable period of time, not exceeding three (3) months from the date of acknowledgment of receipt.
- Evaluates the report and decides whether to forward the report for investigation
- anonymized and in accordance with confidentiality and personal data protection provisions, or to file it with justification (e.g., manifestly vague or outside the scope).
- In cases of suspected criminal offenses subject to mandatory reporting, forwards the report to the competent prosecutor immediately, informing the complainant.
- It cooperates with the competent investigative authorities.

Management and Investigation

- The investigation is conducted with objectivity, confidentiality, and impartiality.
- The reporter and the person reported have the right to fair treatment, the presumption of innocence, and protection of personal data.
- Individuals subject to a report are granted the right to be informed and to provide their views, in accordance with applicable laws and without compromising the confidentiality of the reporting process.
- If the report is dismissed or closed, the reporter is notified.

Protection of Whistleblowers

- Retaliation or unlawful actions against the reporter are strictly prohibited.
- Identity protection, monitoring of any retaliation, and the possibility of legal support are provided.
- Additional complaints may be filed with the Hellenic Authority for Public Integrity in the event of retaliation.

Archiving

All data related to reports are retained and remain secure for a period of at least five (5) years. Archiving is carried out in accordance with all applicable legal obligations regarding personal data protection and confidentiality, ensuring that access to the data is restricted and that the required security procedures are in place.

Data Protection

- Throughout the report investigation process, the DPO and the incident management team are expected to receive Personal Data, either from the incident report or from subsequent communications with the reporter.
- “Personal Data” is defined as any information relating to an identified or
- identifiable natural person (“Data Subject”). An identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- The processing of Personal Data will be carried out in accordance with Regulation (EU) No. 679/2016, the European General Data Protection Regulation (“GDPR”), Law 4624/2019, as currently in force or as it may be replaced, and any other applicable Greek and
- European legislation on the protection of personal data (“Applicable Legislation”).
- The Personal Data of the Data Subject (e.g., the individual against whom a report of misconduct has been filed) will be processed exclusively for the purposes of the whistleblowing system, that is, for the proper management and further investigation of reports of misconduct.

Information and Training

This policy is available on the Company's website so that all employees, partners, and third parties have direct access to its content and are fully informed about the procedures for misconduct and the rights granted to them.

In addition, the Company conducts regular training and awareness campaigns to strengthen understanding and ensure proper use of the reporting channels to its employees. Finally, the policy is continuously evaluated and updated to ensure compliance with applicable laws and the effective operation of whistleblower protection mechanisms.

Alignment with Group Policy

This policy is aligned with the Forvis Mazars Group Whistleblowing Policy and applicable legal and regulatory requirements.

This external-facing policy is designed to provide an accessible reporting framework for external stakeholders. Additional internal procedures, governance structures and reporting obligations are defined in the Company's internal policies, in accordance with the Forvis Mazars Group requirements. This policy is periodically reviewed and updated to ensure continued compliance with applicable laws, regulations and Group requirements.

External Reporting Channel

Individuals have the right to report directly to the National Transparency Authority (NTA) via digital platforms, telephone, or written submission.