



WHISTLEBLOWING POLICY

Law 4990/2022

APRIL 2025

CONTENTS

Version Control	3
1. INTRODUCTION	4
2. PURPOSE	4
3. SCOPE	4
4. ROLES AND RESPONSIBILITIES	5
4.1. Reports Receipt and Monitoring Officer	5
4.2. Reports Management Committee	6
5. SCOPE OF THE POLICY – TYPES OF BREACHES	7
6. RULES AND REGULATIONS	8
7. MEASURES FOR THE PREVENTION, CONTROL, MITIGATION AND MANAGEMENT OF RISKS ...	8
8. GUIDELINES FOR SUBMITTING REPORTS	9
9. CONFIDENTIALITY AND DATA PROTECTION	10
9.1. Confidentiality – Anonymity	10
9.2. Personal Data	10
10. SANCTIONS	11
10.1. Submission of a false report	11
10.2. Obstruction in report submission	11
10.3. Retaliation	11
10.4. Breach of report confidentiality	11
11. POLICY DISCLOSURE	12
12. VALIDITY AND REVISION	12
ΠΑΡΑΡΤΗΜΑ 1 - Definitions	13
ΠΑΡΑΡΤΗΜΑ 2 - Reporting Channels	14

WHISTLEBLOWING POLICY

Version 1: APRIL 2025



Version Control

Version Number	Version Date / Last Modified	Points that changed
01	15/04/2025	<i>Original Version</i>
02		

1. INTRODUCTION

The company under the name "ADMIE HOLDING S.A." (hereinafter referred to as the "Company") has prepared and implements this **Whistleblowing Policy**, in accordance with the requirements of Law 4990/2022 on the "Protection of persons who report breaches of Union law - Transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (L 305) and other urgent provisions", as well as international best practices.

This policy contributes in strengthening the integrity, transparency and accountability, as well as the protection of employees and Company interests.

The Company encourages the submission of confidential or anonymous reports regarding any form of unacceptable behaviour taking place within the Company, through designated reporting channels. The management and investigation of such reports takes place in an independent, objective and impartial manner.

The private data of everyone involved are protected, pursuant to the legislative and regulatory framework on Data Protection.

The terms referred to herein are analysed in Annex 1 – Definitions.

2. PURPOSE

The purpose of the Whistleblowing Policy is:

- α. To establish a system for the internal and external reporting of EU law breaches, the protection of the people reporting these violations, the organisation of the report submission, receipt and monitoring procedure and the sanctions imposed in the event of a breach (Law 4990/2022).
- β. To encourage those covered by the scope of this Policy to submit a report, if they become aware of any illegal behaviour according to Article 5 hereof.
- γ. To determine the rights and obligations of the parties involved.
- δ. To define the principles and framework for the management and investigation of reports.
- ε. To achieve the prevention and timely suppression of the breaches within the Company.

3. SCOPE

The scope of this Policy covers the following parties (hereinafter the “involved parties¹»):

3.1. The members of the Board of Directors and its committees, all employees (including employees in subsidiaries or affiliates) and the shareholders. The same applies to those reporting breaches based on information acquired during the recruitment process or at another negotiation stage before the conclusion of a contract.

3.2. Third parties contractually linked to the Company, as well as any persons employed under their supervision and instructions (referred to herein as “external associates”), and more specifically consultants, contractors, subcontractors, suppliers and associates of any nature.

4. ROLES AND RESPONSIBILITIES

With this Policy, the Company establishes the role of the Reports Receipt and Monitoring Officer (hereinafter the “RRMO”), which has been assigned to the Company’s Legal Advisor, in addition to their other responsibilities. The exercise of these duties does not affect independence and does not lead to a conflict of interests.

It also establishes the Report Management Committee (hereinafter “RMC”).

Specifically,

4.1. Reports Receipt and Monitoring Officer

The RRMO is responsible for:

- a) providing appropriate information regarding the report submission options within the Company and displaying such information in a clearly visible location,
- b) receiving reports concerning breaches that fall within the scope of this Policy,
- c) confirming receipt of the report to the reporting person **within seven (7) working days from the date of receipt**,
- d) taking the necessary actions so that the competent Company bodies or the competent authorities, as the case may be, handle the report, or concluding the process by filing the report if it is unintelligible, submitted abusively, does not contain facts that establish a breach of Union law, or if there are no serious indications of such a breach, and notifying the

¹ The persons referred to in paragraph 1 of Article 6, Law 4990/2022

reporting person of the relevant decision. In the latter case, if the whistle-blower considers that the matter was not handled effectively, they may resubmit it to the National Transparency Authority (NTA), which, acting as an external reporting channel, exercises the competences of Article 12 of Law 4990/2022.

e) ensuring the protection of the confidentiality of the identity of the whistle-blower and any third party named in the report, preventing access to this information by unauthorised persons,

f) monitoring reports and maintaining communication with the whistle-blower and, where necessary, requesting further information from them,

g) providing the whistleblower with information on the actions taken within a reasonable period of time, which shall not exceed **three (3) months from the acknowledgement of receipt, or, if no acknowledgement has been provided, three (3) months from the expiry of the seven (7) working days following the submission of the report,**

h) provides clear and easily accessible information on the procedures under which reports may be submitted to the National Transparency Authority (hereinafter “NTA”) and, where applicable, to public authorities or to institutional and other bodies or organisations of the European Union.

4.2. Reports Management Committee

The Reports Management Committee is responsible for:

- Supporting the work of the RRMO with specialised expertise.
- Determining the appropriate timing for informing the reported person regarding the subject matter of the investigation and its examination.
- Ensuring compliance with the legally prescribed deadlines for the investigation.
- Ensuring the preparation of the investigation conclusions and the formulation of recommendations for corrective measures.
- Informing the Board of Directors upon completion of the investigation for the approval of corrective measures and ensuring their implementation.

The work of the RRMO and the Reports Management Committee may also be supported by other parties (hereinafter the “investigation team”), with the following supporting responsibilities:

- Designing and conducting the investigation to assess the grounds of the report.
- Identifying specialised and experienced internal or external experts, depending on the needs of the investigation, in order to staff the investigation team.
- Identifying, collecting and analysing the necessary evidence.

- Conducting interviews to investigate the factual circumstances of the report.

The Chief Executive Officer is informed of the outcome of the investigation in each case and decides on the recommendations included in the investigation report. In cases where the outcome of the investigation concerns **high-risk**² reports, the competent body to decide on the recommendations included in the investigation report is the Board of Directors.

5. SCOPE OF THE POLICY – TYPES OF BREACHES

If any of the involved parties becomes aware that any of the following breaches is being committed or is very likely to be committed within the Company, they must immediately proceed with submitting a report:

- a) breaches of Union law in the following areas:
 - aa) public procurement,
 - ab) financial services, products and markets, as well as the prevention of money laundering and terrorist financing,
 - ac) product safety and compliance,
 - ad) transport safety,
 - ae) environmental protection,
 - af) protection against radiation and nuclear safety,
 - ag) food and feed safety, as well as animal health and welfare,
 - ah) public health,
 - ai) consumer protection,
 - aj) the protection of privacy and personal data, as well as the security of network and information systems,
- b) breaches affecting the financial interests of the Union, as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU), and those further specified in the relevant Union measures,
- c) breaches relating to the internal market, as referred to in paragraph 2 of Article 26 of the TFEU, including breaches of Union rules on competition and State aid, as well as breaches concerning the internal market related to acts that infringe rules on corporate taxation or arrangements aimed at securing a tax advantage that defeats the object or purpose of the applicable corporate tax legislation.

²High-risk reports are defined as those that significantly affect the achievement of the Company's strategic objectives and may potentially impact its reputation.

- d) breaches of national law relating to offences of bribery and trading in influence, as defined in Articles 159, 159A, 235, 236, 237, 237A and 396 of the Criminal Code.
- Breach of health and safety requirements
- Breach of confidentiality and non-compete clauses

The whistleblowing policy does not cover:

- Disagreements regarding management policies and decisions,
- Personal issues or disputes with colleagues or supervisors,
- Rumours

6. RULES AND REGULATIONS

At the time of submitting a report, whistleblowers must have reasonable grounds to believe that the information regarding the reported breaches is true and falls within the scope of this Policy.

Personal data and any type of information that directly or indirectly leads to the identification of the whistleblower shall not be disclosed to anyone other than the authorised personnel responsible for receiving or monitoring reports, unless the whistleblower provides explicit consent.

³ as specifically provided in Part I of the Annex to Law 4990/2022

7. MEASURES FOR THE PREVENTION, CONTROL, MITIGATION AND MANAGEMENT OF RISKS

The Company, having as its primary aim the prevention, control, mitigation and management of risks related to the subject matter of this Policy, implements the following measures:

- α. assessment of risks,
- β. establishment of this Policy with the objective of preventing, controlling, mitigating and managing such risks,
- γ. conducting information sessions / trainings and raising awareness among employees and other involved parties,
- δ. Providing information regarding the rights and obligations of employees and the employer, as well as of individuals exercising managerial authority or representing the employer, to the extent and degree of their own responsibility, in the event of the occurrence, reporting or disclosure of such incidents, as well as information on the relevant procedure,

- ε. Appointment of a designated person as the responsible officer (“RRMO”) at Company level, responsible for guiding and informing employees on the prevention and management of situations falling within the scope of this Policy.

8. GUIDELINES FOR SUBMITTING REPORTS

Reports may be submitted to the RRMO in accordance with the ANNEX 2.ΠΑΡΑΡΤΗΜΑ 2 -

Below are general guidelines and instructions for submitting reports:

- The report of a breach must be made in good faith and without delay, immediately upon its detection.
- The report must be clear, specific and include as much information and detail as possible, in order to facilitate its investigation. It must include at least the name of the person or persons who committed the breach, its type, the date/time period and the place where the incidents constituting the breach occurred, the department to which the incident relates, and the most detailed possible description of the breach.
- Sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data, data concerning a person's sexual life or sexual orientation, and, more generally, information that is unrelated to the incident must not be included in the report.
- The whistleblower does not need to be absolutely certain about the validity of their report. It is sufficient to have reasonable concerns or suspicions and act in good faith. They must not engage in unlawful actions that could place themselves, the Company or any third party at risk in order to search for or collect additional evidence to support their report.
- The whistleblower must be available and reachable, either confidentially or anonymously, in order to provide further information if requested.
- If the report is deemed unfounded, the reported person will not be informed that a report was made against them, for the purpose of protecting the working environment within the Company.
- If the report is ultimately deemed malicious and the reported person has become aware of its content in the context of the investigation, then they have the right to be informed of the identity of the whistleblower (provided that the report was not anonymous), to allow them to exercise their rights.

The Company's relevant Reporting and Report Management Procedure involves the following steps:

1. Investigation of Incidents – Reports
2. Record Keeping of Reports
3. Protection of the Whistleblower
4. Rights of whistleblowers and reported persons
5. Corrective Actions

9. CONFIDENTIALITY AND DATA PROTECTION

9.1. Confidentiality – Anonymity

The Company encourages and protects its employees and external associates to submit reports of breaches through the established reporting channels. The submission of confidential reports under the whistleblower's name is encouraged. However, it is clarified that anonymous reports are treated with the exact same attention and seriousness.

The Company also commits to making every possible effort and taking all appropriate measures to protect the identity of both the whistleblowers and the reported persons, as well as any third parties involved, and to handle the matter with complete discretion, confidentiality and secrecy.

In any case, during the handling and investigation of a report, the identity of the whistleblower (provided the report is not anonymous) shall not be disclosed to anyone other than the authorised persons responsible for receiving, monitoring and investigating reports, unless the whistleblower has given explicit consent or the report is proven to be malicious.

9.2. Personal Data

Any processing of personal data under this Policy is carried out in accordance with the applicable national and European legislation on personal data, as well as the Company's relevant policies on data protection and confidentiality. The data of all involved parties are protected and processed exclusively in relation to the specific report, solely for the purpose of investigating the report and determining whether it is substantiated.

The Company takes all necessary technical and organisational measures to protect personal data. Access to the data contained in the reports is granted only to those involved in their

management and investigation. Sensitive personal data and other data not directly related to the report must not be included in it, and if such data are included, they will not be taken into consideration. Personal data are deleted within a reasonable period of time following the completion of the investigation.

10. SANCTIONS

10.1. Submission of a false report

A prerequisite for the protection of the whistleblower is that, at the time of submitting the report, they had reasonable grounds to believe that the information concerning the reported breaches was true and fell within the scope of Law 4990/2022. Otherwise, there is provision for a penalty of at least two (2) years of imprisonment and a monetary fine for persons who knowingly submit false reports or false public disclosures, without excluding their liability under other applicable provisions.

10.2. Obstruction in report submission

Persons who obstruct or attempt to obstruct the submission of a report shall be punished with imprisonment and a monetary fine, without excluding their liability under other applicable provisions.

10.3. Retaliation

Persons who engage in retaliation or initiate malicious proceedings against whistleblowers shall be punished with imprisonment and a monetary fine, without excluding their liability under other applicable provisions.

10.4. Breach of report confidentiality

Persons who breach the obligation for confidentiality of the whistleblower's identity, in violation of Article 14 of Law 4990/2022, shall be punished with imprisonment and a monetary fine, without excluding their liability under other applicable provisions.

If any of the above violations is committed for the benefit of or on behalf of a legal entity, an administrative fine shall be imposed on that entity, the amount of which may not be less than ten thousand (10,000) euros nor exceed five hundred thousand (500,000) euros. When

determining the above sanction, particular consideration is given to the severity of the violation and the degree of fault.

11. POLICY DISCLOSURE

All persons involved under this Policy are required to comply with it. The RRMO ensures that the Company's employees are informed about the content of this Policy and ensures that the Policy is published in a visible location on the Company's internal network.

Information may be provided through e-learning, distribution of informational material, email, or any other appropriate means.

12. VALIDITY AND REVISION

The Whistleblowing Policy has been approved by the Company's Board of Directors and may be amended or revoked only by it.

Any amendments or revocations shall be communicated accordingly.

ΠΑΡΑΡΤΗΜΑ 1 - Definitions

For a better understanding of this Policy, the main definitions are set out in this section as follows:

- **Report:** The internal submission of information related to breaches within the Company.
 - a) “Internal report”: the oral or written provision of information regarding breaches to the Company’s Reports Receipt and Monitoring Officer (hereinafter the “RRMO”)
 - b) “External report”: the oral or written provision of information, or provision through an electronic platform, regarding breaches to the National Transparency Authority (N.T.A.).
- **Malicious report:** A report made by the reporting person knowingly containing information that is not true.
- **Good faith:** A reasonable belief by the whistleblower, based on the circumstances and the information available to them, that the information they provide is true.
- **Whistleblower or reporting person:** The individual who reports or discloses information regarding breaches which they acquired in the context of their work.
- **Reported person:** A natural or legal person who is named in an internal or external report, or in a public disclosure, as the person to whom the alleged breach is attributed, or who is connected to the person to whom the breach, falling within the scope of this Policy, is attributed.
- **External partners:** Third parties contractually connected with the Company, as well as their personnel, specifically including consultants, subcontractors, contractors, suppliers and any type of associates.
- **Reasonable grounds:** The justified belief of a person with similar knowledge, training and experience as the whistleblower that the information they possess is true and constitutes a breach of Union law falling within the scope of this Policy.
- **Retaliation:** Any direct or indirect act or omission occurring in a work-related context as a result of a Report, which causes or is likely to cause unjustified harm to the Whistleblower or place them at a disadvantage, and which is connected with an internal or external report or a public disclosure.
- **Follow-up actions:** Any act carried out by the recipient of a report, or by any authority or body to which the report is referred due to competence, for the purpose of assessing the accuracy of the allegations contained in the report and addressing the reported breach, such as internal investigation, inquiry, prosecution, legal action for the recovery of funds, or closure of the procedure.

ΠΑΡΑΡΤΗΜΑ 2 - Reporting Channels

Reports may be submitted to the Company's Reports Receipt and Monitoring Officer (RRMO).

Communication and Reporting Channels	Contact Information
Reports Receipt and Monitoring Officer (RRMO) - Legal Advisor	<p>The Reports Receipt and Monitoring Officer is appointed by a decision of the Board of Directors</p> <p>Contact them via:</p> <ul style="list-style-type: none"> E-mail: whistleblowing@admieholding.gr (Only the responsible RRMO has access to this email) By correspondence at the address: ADMIE HOLDING S.A. 89 Dyrachiou and Kifissou St. 104 43, Athens
Reports Management Committee	<p>The Reports Management Committee is established by decision of the Board of Directors as a three-member committee consisting of:</p> <ul style="list-style-type: none"> The RRMO The Regulatory Compliance Officer The Head of the Internal Audit Unit
Every employee may always contact their immediate supervisor or the Director of the Department to which they belong.	