NAVARONE S.A.

REPORTING POLICY

Contents

1 Introduction 3

2 Definitions 3

3 Scope - Reporting persons 6

4 Scope – Types of breaches 7

5 Reporting Channels 8

6 Guidelines for Reporting 10

7 Responsibilities of the Person for the Receipt of Reports (YPPA) 10

8 Responsibilities of the Reports Management Committee (EDA) 12

9 Appointment of members of the EDA 12

10 Report Management Process 13

11 Rights of Reporting person and person concerned. 14

12 Protection of Reporting Persons 14

13 Investigation of a report 15

14 Confidentiality - Anonymity 16

15 Personal Data 16

16 Corrective actions and disciplinary actions 17

17 Information and education 17

1 Introduction

The company under the name “NAVARONE S.A.” of the Republic of Panama, which maintains an established branch office in Greece by virtue of article 25 of L.27/1975 at Amaroussion, Attica at 6 Cheimarras Street, 15125 (hereinafter referred to as the “**Company**”) in accordance with the rules of professional ethics, integrity, transparency, and ethics. At the same time, it creates and implements policies to comply with the current legislative and regulatory framework.

With this **Reporting Policy**, the Company complies with Directive (EU) 2019/1937, on the protection of persons who report breaches of EU law, and National Law 4990/2022. The Reports Policy aims to establish a system for internal reporting of breaches of EU law, to protect persons reporting such breaches and to organize the submission process, receipt, and follow-up of reports.

The company has zero tolerance for actions that may disrupt its healthy working environment, harm it and jeopardize its reputation and credibility. It encourages reporting as soon as it is noticed. All reports are taken seriously and investigated with complete objectivity and independence. The Company assures those who make reports will be protected from any retaliation and that the personal data of all parties involved are protected by applying the necessary technical and organizational security measures.

2 Definitions

1. **'Report' means:**

oral or written or through an electronic platform provision of information regarding breaches of the present.

a) **"Internal reporting" means** the oral or written or through an electronic platform provision of information on breaches to the Person for the Receipt and Follow-up of Reports (YPPA) of a legal entity in the public or private sector.

b) **"External reporting"** means the oral or written or electronic provision of information on breaches to the **National Transparency Authority.**

2. **'Person concerned' means:**

the person named in the internal or external reporting or public disclosure as a person to whom the breach is been attributed or who is related to the person to whom the breach is attributed falling within the scope of this Directive.

3. **'Reporting person ' means:**

the person, who makes an internal or external reporting or public disclosure, providing information about breaches obtained in the context of his work activities.

4. **'Retaliation' means:**

any direct or indirect act or omission, occurring within the work-related context, which causes or is likely to cause unjustified damage to, or put the reporting person at a disadvantage, and relates to internal or external reporting or public disclosure.

5. **Good reasons:**

a legitimate belief by a person with similar knowledge, education, and experience to the reporting person that the information in his or her possession is true and constitutes a breach of Union law falling within the scope of this Directive.

6. **Public disclosure:**

making information about breaches directly available to the public.

7. **facilitator:**

the person assisting the reporting person in the reporting process within the employment context, whose assistance must be confidential.

8. **Investigation activities**

any action taken by the recipient of a report or any authority or organization to which the report is referred due to competence to assess the accuracy of the allegations

contained in the report and to address the reported breach, such as an internal investigation, investigation, prosecution, action for recovery of funds or termination of proceedings.

9. Update:

to inform reporting persons of the measures envisaged or taken in the context of monitoring and the reasons therefor.

10. Working context:

current, past or anticipated work activities in the public or private sector, irrespective of the nature of those activities, through which persons obtain information about breaches and where those persons are likely to suffer retaliation if they report them.

11. Breaches:

acts or omissions which are unlawful under Union law or contrary to the subject matter or purpose of rules of Union law falling within the material scope of this Directive.

12. Information about breaches:

information, including reasonable suspicions, about breaches that have occurred or are very likely to occur in the organization in which the reporting person works, has worked or will work or is in negotiations to work or in other bodies with which the reporting person has had contact through or in connection with his or her work; as well as information about attempts to conceal breaches.

13. External collaborators:

Third parties contractually linked to the Company as well as their staff, namely consultants, subcontractors, contractors, suppliers, all kinds of partners, shareholders, etc.

14. Person responsible for receiving and monitoring reports or YPPA.:

The person who receives and monitors the progress of reports.

15. Committee for the Management of Reports (EDA):

The committee responsible for managing and investigating Reports.

16. Employee:

The person who contracts with the company with an employment contract of fixed or indefinite duration or the person connected to the Company by another employment relationship or the person who is seasonal staff or the person employed as a trainee in the Company.

17. Reporting channels:

The channels through which reports are submitted include the means used for reporting and the persons to whom reporting persons can be contacted.

18. Malicious Reporting:

A Report made with the Reporting person's knowledge that it is not true.

19. Good faith:

The situation which gives rise to a reasonable belief in the Reporting person that he or she has reasonable faith that the information he provides is true.

20. Platform:

The specially designed electronic platform that is accessible online via computer or mobile device.

3 Scope - Reporting persons

In the reporting policy, reporting persons may be:

A) The Board of Directors and its Committees, as well as all employees, of fixed or indefinite contract duration or with any other employment relationship or mandate, seasonal staff, and trainees, who report in good faith illegal or contrary to the code of ethics. The same applies to those who report breaches based on information obtained during the recruitment process or at another stage of pre-contractual negotiation.

B) Third parties contractually linked to the Company and their staff (referred to as "external partners"), who have become aware of some illegal behavior within the Company, consultants, contractors, contractors, subcontractors, suppliers, and all kinds of partners. In addition, shareholders, and clients exclusively for issues of breaches of business principles and misconduct referred to in the article "Scope – Types of breaches". A prerequisite for falling within the scope of protection of this policy is that the report is made in good faith. Reporting persons must have reasonable grounds and a reasonable belief, based on the circumstances and the information available to them, that the information they provide is true. In any case, good faith is taken for granted, unless it is proven that the report was made maliciously. In case of malicious reporting, the protection described in this policy is not provided.

4 Scope – Types of breaches

References to this policy are acceptable when they concern the following types of misconduct - breaches. Any person within the "Scope of Reporting Persons" who becomes aware of any misconduct or violation within the Company for the following types of breaches should immediately make a Report.

1. Public procurement.
2. Money laundering.
3. Terrorist financing.
4. Financial services, products, and markets.
5. Product safety and compliance.
6. Transport safety.
7. Protection of the environment.
8. Radiation and nuclear safety.
9. Food and feed safety/animal health and welfare.
10. Public health.
11. Consumer protection.
12. Protection of privacy and personal data.

13. Security of networks and information systems.
14. Economic interests of the European Union.
15. Competition and State benefits.
16. Violation of rules, corporate taxation, or settlements.

Reporting Policy does not cover:

1. Disagreements on issues concerning management policies and decisions.
2. Personal issues and disagreements with colleagues or superiors.
3. Personal work matters that fall within the competence of HR.
4. Rumors.

5 Reporting Channels

The Company establishes easily accessible reporting channels, encourages the submission of incident reporting that falls within the scope of this Policy and guarantees that all reports received are treated confidentially. The report can be submitted confidentially or anonymously. By submitting a confidential report, the reporting person's personal details may be disclosed to the Person concerned if requested, under the terms and conditions of applicable personal data legislation. If the reporting person does not wish to submit the report confidentially, has the option to submit the report anonymously.

The ways to submit Reports are as follows:

A. Through the electronic platform for the submission of reports which meets all safety standards:
   - Information systems.
   - Personal data.
   - The confidentiality or anonymity of the reporting person if he so chooses.

It also provides the ability to monitor the status of the report from the beginning of the report until its completion. Access to the online platform is available on the Company's website and we encourage reporting persons to use it as it is the most comprehensive and secure means of managing reports.

B. In writing, confidentially by sending an e-mail to: **whistleblowing@navarone.gr**

C. In writing, confidentially or anonymously by sending a postal letter to the **YPPA** of the Company at the address: 6 Cheimarras Street, Amaroussion, Attica, PC 151 25 with the indication "personal and confidential". The letter should also indicate **the company** being reported.

D. Orally, by phone at **+30 210 41 01 700** or personal meeting with the **YPPA** at the request of the reporting person.

Regardless of the reporting channel, all reports are received and managed by the **YPPA** which is responsible for communicating with the reporting person.

6 Guidelines for Reporting

Here are general guidelines and guidelines for reporting:

1. Reporting of misconduct should be made in good faith and without delay, as soon as it becomes apparent.
2. The Report should be clear, defined and contain as much information and detail as possible in order to make it easier to investigate.
3. The Report should include the name of the person(s) who may have committed any misconduct, the date/time period and place where the incident took place the company to which the incident relates, the type of misconduct and as detailed a description as possible.
4. Any personal data and other sensitive information unrelated to the incident should not be included in the Report.
5. The Reporting persons need not be sure of the validity of his Report. They should not take any illegal actions that may endanger themselves, the company or any third party to seek and collect more evidence to support their Report.
6. The Reporting Person should be available, either confidentially or anonymously through the online reporting platform, to provide further information upon request.

7 Responsibilities of the Person for the Receipt of Reports (YPPA)

The Report Controller has the following responsibilities:

1. Provides appropriate information on the chance of reporting within the organization and communicates this information in a prominent place on the organization.
2. Receives reports of breaches falling within the scope of this Directive.
3. Acknowledges receipt of the report to the reporting person within seven (7) working days from the day of receipt.
4. Takes the necessary steps to deal with the complaint by the Reports Management Committee **(EDA)**, or close the procedure, by archiving the report if it is

5. unintelligible or abusively submitted or contains no facts constituting a breach of Union law or there are no serious indications of such a breach and notifying the relevant decision to the reporting person who, if it considers that it has not been dealt with effectively, it may resubmit it to the **National Transparency Authority** , which acts as an external reporting channel
6. Ensures the protection of the confidentiality of the identity of the reporting person and of any third parties named in the report by preventing access to it by unauthorized persons.
7. Monitors reports and maintains communication with the reporting person and, if necessary, requests further information from the reporting person.
8. Informs the reporting person of 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 sent to the reporting person , three (3) months from the end of seven (7) working days from the submission of the report.
9. Provides clear and easily accessible information on the procedures under which reports may be submitted to the **National Transparency Authority.** and, where applicable, public bodies or institutions, bodies, offices, or agencies of the European Union.
10. Plans and coordinates training activities on ethics and integrity, participates in the formulation of internal policies to enhance integrity and transparency in the institution.

The **YPPA shall:**

1. Carries out his/her duties with integrity, objectivity, impartiality, transparency and social responsibility.
2. Respects and observes the rules of secrecy and confidentiality for matters of which he/she has become aware in the performance of his/her duties.

3. Refrains from handling specific cases, declaring an impediment if there is a conflict of interest.

The Company ensures that if the YPPA performs other duties, that the execution of these duties does not affect their independence and does not lead to a conflict of interest in relation to his duties.

8 Responsibilities of the Reports Management Committee (EDA)

The management of reports submitted through the Reporting channels is carried out by the EDA, in accordance with the Complaint Management Process which has the following responsibilities:

- It examines the admissibility of reports brought to its attention by all established reporting channels of the Company.
- Evaluates reports.
- Communicates with the YPPA to exchange the necessary information.
- Takes all appropriate measures to protect the personal data of the subjects involved in the reports and ensure their deletion in accordance with the deadlines set.
- Supervises the Internal Investigation Process of Accepted Reports.
- Maintains a central register of Reports.

9 Appointment of members of the EDA

The following are defined as members of the EDA:

1. **Regular** members, who undertake the management of all Reports except in cases where alternate members take over.
   - Bei Iro
   - Sakellakos Konstantinos
   - Christodoulou Ioannis

2. **Substitute members,** who take up their duties in the event that one or more regular members are removed from the office for allegedly being involved in the report under consideration.

- Sotiriou Ioannis
- Kyrozi Maria Sofia

10 Report Management Process

The reporting process is described in the following steps:

1. The reporting person shall submit the report to one of the reporting channels.
2. YPPA receives the report and confirms to the reporting person that it has been received within 7 days.
3. YPPA evaluates the report if it falls within the scope of the Law and forwards it to the EDA.
4. If the report does not fall within the scope of the Law, informs the EDA and, unless there is a different assessment by the EDA, concludes the procedure and informs the reporting person .
5. If the report falls within the scope of the Law, forwards the report to the EDA which undertakes the management of the investigation of the complaint within the organization. If the reporting person is a member of the EDA, then he is relieved of his duties and one of the substitute members is appointed in his place.
6. YPPA informs the reporting person that his report has been accepted.
7. The investigation of the report is conducted.
8. The EDA informs the YPPA at regular intervals about the progress of the investigations, who must inform the reporting person no later than 3 months after receipt of the report, of the results of the investigation even if the investigation has not yet been completed.
9. Upon completion of the investigation, the EDA informs the YPPA and he, in turn, the reporting person of the final results of the investigation.

11 Rights of Reporting person and person concerned.

The Reporting person has the right to be informed both, of the receipt of his Report (at the latest within 7 working days) and of the outcome of the investigation (at the latest within 3 months).

The Company protects both, reporting person and person concerned. The investigation shall be conducted in full secrecy and confidentiality at all stages of the procedure, as far as possible, to avoid stigmatizing individuals.

The persons included in the reports have the right to be informed immediately of the misconduct of which they are accused, to the persons who have access to the data contained in the Report, and to the right to be called to apology. However, if there is a serious risk that such information could hamper the investigation of the case and the collection of the necessary evidence, the briefing of the persons included in the Report may be postponed until this risk ceases to exist.

The identity of the Reporting person shall remain confidential. Exceptionally, if the Report proves to be malicious, and if the reported person so requests, he/she may be informed of the identity of the Reporting Person to exercise his/her legal rights. It is clarified that reports that are proven to be manifestly malicious will be further investigated at the discretion of the Company both as to the motives and as to those involved in restoring order in any legal way and means.

12 Protection of Reporting Persons

The Company protects the reporting person who reports, in good faith, illegal or immoral behavior. In this context, any kind of negative behavior against anyone who has made a Report is prohibited, even if the Report turns out, as a result, to be incorrect. The Reports Management Committee and Management ensure that there is no retaliation if anyone in good faith submits a Report. More specifically, the Company commits that employees who have submitted a Report will not suffer retaliation,

harassment or marginalization, intimidation or threats and unfair treatment because of their Report.

Also, unjustified changes in the employment relationship because of the Report (e.g. dismissal, suspension, degradation or deprivation of promotion, reduction of salary, change of place of work, transfer, change of duties, change of working hours, etc.) are not permitted. In case of malicious Reporting, the above protection does not exist.

The same level of protection applies to third parties associated with reporting persons who could suffer retaliation in a work-related context, such as colleagues or relatives of reporting persons.

In case the Reporting person is an external partner, premature termination or cancellation of a contract for goods or services as a result of the Reporting is not permitted.

Any act of retaliation should be immediately reported to the EDA, investigated, and resolved. If the investigation reveals that there has indeed been retaliation, disciplinary action will be imposed against the perpetrator. The person accused of committing the retaliation has the burden of proving that his actions are not related to the Report made by the employee.

In the event that an employee decides to Report an incident covered by this policy and in which they were previously involved, the fact that they ultimately reported it will be considered in their favor in any other subsequent proceeding.

In case the Report is made confidentially and after investigation it is proven that thanks to it the Company protected its vital financial or other interests, the person who made the Report will be rewarded in the most appropriate way.

13 Investigation of a report

The Company undertakes to treat with due care any Report, whether confidential or anonymous. The EDA investigates the incidents contained in the Report as soon as possible. Where necessary and depending on the Report, additional professional

support may be received from other company executives as well as external specialized consultants.

14 Confidentiality - Anonymity

The Company encourages employees and contractors to raise concerns about potential misconduct through existing Reporting channels. It also undertakes to make every effort and take all appropriate measures to protect the identity of both the Reporting person and the persons included in the Reports and to handle the case in full secrecy and confidentiality.

In any case, during the investigation of an incident, the identity of the Reporting Person shall not be disclosed to anyone other than the authorized persons competent to receive, monitor and investigate the reports, unless the Reporting person has given explicit consent or the Report proves malicious.

Anonymity is achieved using appropriate technical and organizational measures and mainly through the reporting platform where it is possible to submit either a confidential or anonymous Report. The Platform supports anonymous reporting, two-way communication and meets high security standards.

15 Personal Data

Any processing of personal data under this policy is conducted in accordance with the national and European legislation applicable to personal data as well as the Company's personal data protection policy. The data of all parties involved are protected and processed solely in relation to each Report and for the sole purpose of verifying the validity or otherwise of the Report and investigating the specific incident.

The Company takes all necessary technical and organizational measures to protect personal data, in accordance with the Company's privacy policy.

Sensitive personal data and other data not directly related to the Report are not taken into account and deleted.

Access to the data contained in the reports can only be granted to those involved in the management and investigation of the incident.

Personal data and material obtained during the handling of the Report shall be deleted within a reasonable time from the completion of the investigation initiated based on the Report.

16 Corrective actions and disciplinary actions

Depending on the results of the investigation, the Reports Management Committee proposes corrective and/or disciplinary/legal actions. These actions may include (but are not limited to): (a) additional employee training, (b) establishment of new internal control points, (c) amendments to existing policies and/or procedures, (d) disciplinary sanctions including permanent removal/dismissal, or (e) legal action.

17 Information and education

The Company ensures that all employees will be informed and trained on the content of this Policy and on any new revision.

External partners are committed to informing their staff accordingly. This will be done by highlighting this reporting policy and in addition to providing them with material that the Company will provide them with.

Information and awareness actions will be continuous both internally and externally to establish a positive corporate reporting culture that will support the principles of integrity, honesty, and transparency.