



Whistleblowing Policy

Regulatory Compliance | Business Ethics

Approval	Board of Directors
Entered into effect	June 2025
Issue	Whistleblowing policy v.2 (June 2025)
Issued by	Regulatory Compliance Department
Previous versions	Whistleblowing policy v.1 (August 2022)

TABLE OF CONTENTS

1. Purpose - Zero tolerance statement	4
3. Definitions	4
4. Scope	5
5. Object of reports	6
6. Internal reporting channels	7
7. Report content	8
8. Roles and responsibilities	8
8.1. RRMR	8
8.2. Deputy RRMR	10
9. Report management	10
9.1. Growthfund	10
9.2. Growthfund Subsidiaries	12
10. Whistleblower protection measures	12
10.1. General protection measures	12
10.2. Special protection measures	13
11. External reports	15
12. Public disclosure	16
13. Personal data protection	16
14. Measures in the event of a confirmed breach	18
15. Remedial measures in the event of breaches	19
16. False Report and Protection Against False Reports	19
17. Policy Management and resolution of questions	20

1. Purpose - Zero tolerance statement

The Hellenic Corporation of Assets and Participations S.A. (**Growthfund** or the **Company**) is committed to ensuring the highest level of ethical and professional conduct and to demonstrating zero tolerance for illegal or improper actions that may affect its compliance with legal and regulatory obligations and/or its reputation and credibility.

The Growthfund's Whistleblowing Policy (Policy) aims at the prevention and combating of any illegal or improper action. Specifically, the Policy's purpose is:

- ✓ to define the principles, the protection measures, and the general operational framework under which the Company receives, investigates, and manages reports of any improper, illegal, unethical, unprofessional, or criminal acts or omissions that have been brought to its attention;
- ✓ to encourage individuals to make reports through the designated internal communication channels, in the event that they become aware of any illegal or unfair conduct within the workplace, without fear of retaliation;
- ✓ to ensure the Company's compliance with Law 4990/2022, as in force (**Whistleblowing Law**), which incorporates Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons reporting breaches of Union law into Greek legislation.

The Policy also sets out the guidelines for Growthfund's portfolio companies, which establish and implement similar policies and procedures, depending on the legal framework governing them.

The Company assures that it takes all reports seriously and investigates them with full confidentiality and discretion, ensuring that the personal data of the parties involved are protected, in accordance with the applicable legislative and regulatory framework on personal data protection. Depending on the findings that result from the investigation of each report, the Company takes, as appropriate, the necessary and suitable measures in order to address and prevent the recurrence of any similar incident or behavior in the future.

3. Definitions

Report	The provision of information, orally or in writing, regarding actual or suspected improper, illegal, unfair, unethical, or criminal acts or omissions that fall within the scope of this Policy.
Breaches	Actual or suspected improper, illegal, unfair, unethical, or criminal acts or omissions that fall within the scope of this Policy.
Whistleblower	The natural person who makes a Report.

Reported Person	The natural or legal person named in the Report as the person who committed the Breach or who is associated with the person to whom the above conduct is attributed.
Reporting Channel(s)	The channels designated in this Policy through which Reports are submitted.
Good Faith	The reasonable belief of the Whistleblower that their Report is true, based on objective facts and circumstances.
Malicious Report	The Report made by the Whistleblower with the knowledge that it is not true.
Retaliation	Any direct or indirect act or omission that takes place within the work environment and causes or may cause unjustified harm to the Whistleblower or to persons connected with them, or places the Whistleblower or persons connected with them at a disadvantage, and is related to the Report.
RRMR	Responsible for Receiving and Monitoring Reports
Deputy RRMR	Responsible for Receiving and Monitoring Reports, in the event that the RRMR is unable to handle the case (e.g., due to conflict of interest)
NTA	National Transparency Authority
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation or GDPR)

4. Scope

This Policy applies to:

- a) Persons who obtained information on Breaches falling within the scope of the Whistleblowing Law in the context of their work, including the following:
 - All employees of the Company, such as its executives or staff, regardless of the type of their employment contract (e.g., contract of dependent employment or independent services, full-time or part-time employment, secondment);
 - members of the Corporate Governance Council and Growthfund's Board of Directors;
 - the volunteers and paid or unpaid trainees;

- persons working under the supervision and instructions of partners, suppliers, and subcontractors.
- b) persons (with any of the capacities referred to in category (i)) who obtained information on Breaches in the context of an employment relationship that has ended for any reason.
- c) persons (with any of the capacities referred to in category (i)) whose employment relationship has not yet commenced, in the event that information on Breaches has been obtained during the recruitment process or at another stage of negotiation prior to the conclusion of the contract.
- d) mediators or third parties (natural or legal persons) connected with the Whistleblowers or their Report (e.g., colleagues or relatives of the Whistleblower, legal entities of the Whistleblowers' interests or for which they work or with which they are otherwise connected through an employment relationship).

5. Object of reports

In the event that any person subject to this Policy becomes aware that any of the following misconducts is being committed, they must immediately make a Report through the designated Reporting Channels. Specifically, a Report may be submitted for the following Breaches, which fall within the material scope of application of the Whistleblowing Law as follows:

- a) breaches of EU law in the following areas:
- public contracts;
 - financial services, products and markets, as well as the prevention of money laundering and terrorist financing;
 - product safety and compliance;
 - transport safety;
 - environmental protection;
 - protection against radiation and nuclear safety;
 - safety of food and animal feed, as well as animal health and welfare;
 - public health;
 - consumer protection;
 - 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 under Article 325 of the Treaty on the Functioning of the European Union (TFEU) and as specifically defined in the relevant Union measures;

- c) Breaches related 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 relating to practices that infringe corporate tax rules or arrangements intended to secure a tax advantage that defeats the object or purpose of the applicable corporate tax legislation;
- d) Breaches of domestic law relating to offences of bribery and trading in influence, as codified in Articles 159, 159A, 235, 236, 237, 237A, and 396 of the Penal Code and in Article 134 of Law 5090/2024.

It is noted that the Company encourages the submission of Reports concerning the above Breaches, as well as irregular behaviors which, although not covered by the Whistleblowing Law, constitute cases of serious misconduct. Indicatively, such misconducts, insofar as they are not directly or indirectly connected with the above cases, may concern Breaches of any other law, rule, or regulation, such as disputed accounting practices, breaches of internal accounting controls, irregularities in financial reporting or any other financial matters (e.g., fraud or deliberate error in the preparation, evaluation, or revision of any financial statement), any conduct that may be defined as a criminal offence or an attempt thereof (e.g., fraud, embezzlement, corruption, forgery or alteration of documents), or other unethical behavior.

It is specifically noted that Reports concerning incidents of violence and harassment under the provisions of Law 4808/2021 are not examined within the framework of this Policy, but the Company's Policy on Combating Violence and Harassment at Work, as in force from time to time, as well as the Company's Reporting Management Procedure, shall apply.

6. Internal reporting channels

The Company, in order to encourage the submission of Reports, has created special internal communication channels which Whistleblowers may use to submit their Reports, either with their name or anonymously. Specifically, Reports may be submitted in the following manners:

- **Through the "Safevoice" Reporting platform**, which can be accessed at <https://safevoice.growthfund.gr>,
- **by e-mail:** safevoice@growthfund.gr,
- **by letter** submitted either in person or by post to the Company's offices, at 4 Karagiorgi Servias Street, Postal Code 10562, Athens, Attica, bearing the indications "Whistleblowing Report" or "Report under Law 4990/2022" and "For the attention of the Responsible Officer for Receiving and Monitoring Reports (YPPA) – Growthfund/4th floor";

- **by meeting with the Responsible Officer for Receiving and Monitoring Reports (YPPA)** following the submission of a relevant request to the following email address: safevoice@growthfund.gr.

Whistleblowers are encouraged to submit their Report under their name for better communication with the RRMR, both for the provision of any supplementary information or further clarifications and to facilitate the monitoring of the Report. It is specifically clarified that, in the event the Report is submitted through the "Safevoice" Reporting platform or via the email address safevoice@growthfund.gr, the members of the Evaluation Committee, as designated in section 9.1, simultaneously receive the Report.

Otherwise, if the Report is submitted through any other communication channel, the RRMR receives the Report and forwards it, provided that the corresponding conditions set out in section 9.1 are met, to the Evaluation Committee for Reports. For more information, instructions, or clarifications regarding the possibility of submitting a Report through the above channels, you may contact the RRMR directly at the following email address: safevoice@growthfund.gr.

In the event that any third party, other than the RRMR, becomes the recipient of a Report, they shall forward it without delay to the RRMR, without any modification of its content or disclosure of information that could lead to the identification of the Whistleblower or of any third party named in the Report.

7. Report content

Each Report shall include at least the following: The main reason for submitting the Report (i.e., an act or omission that could potentially cause or has already caused an incident worthy of reporting), the date, time, and location of the event, the frequency of the incident, the names of the persons/parties involved, the names of any witnesses (if any), related monetary amounts or assets, and any details or relevant records. It is not necessary to include evidence when submitting the Report, but any relevant information that may facilitate its evaluation will be taken into account.

As stated above in section 6, the Company allows the submission of a Report through the designated Reporting Channels, either under name or anonymously. It is clarified that the platform also provides the possibility of submitting an anonymous Report. The Whistleblowers are nevertheless encouraged to submit their Report under their name through the above channels for better communication with the RRMR.

8. Roles and responsibilities

8.1. RRMR

The RRMR plays a central role in the proper implementation of this Policy, as he is responsible for receiving and monitoring the internal Reports submitted through the designated Reporting

Channels. However, in the event that a conflict of interest arises in the handling of a specific Report or an impediment is identified in the person of the RRMR that prevents the proper execution of his duties, he shall be replaced by the Deputy RRMR.

Specifically, the impeded RRMR must immediately refrain from the process of monitoring and handling the relevant Report, declaring his impediment, and the Deputy RRMR fully assumes his duties and informs, as appropriate, the Board of Directors and/or the Growthfund's Corporate Governance Council. Specifically, in the event that the Report contains allegations against the RRMR regarding a possible Breach of provisions of Union law, he is limited to recording the Report in the special register he maintains and forwarding the Report to the National Transparency Authority as an external reporting channel, while informing the Whistleblower.

The RRMR (and, in case of replacement, the Deputy RRMR) performs his duties with integrity, objectivity, impartiality, transparency, and social responsibility, and fully respects the rules of secrecy and confidentiality regarding matters of which he became aware in the course of performing his duties. In any case, he must ensure that any parallel engagement, duty, position, or capacity does not affect his independence and impartiality.

The RRMR (and, in case of replacement, the Deputy RRMR) has the duty to:

- ✓ To provide the appropriate information regarding the possibility of submitting a Report and to post the relevant information in a prominent place within the Company.
- ✓ To receive Reports that fall within the scope of this Policy.
- ✓ To acknowledge receipt of the Report to the Whistleblower within seven (7) working days from the date of receipt, regardless of the method of submission, unless such notification to the Whistleblower is rendered impossible due to the absence of necessary contact details.
- ✓ For Reports submitted through the above electronic platform, notification is carried out by means of an automated message. For Reports submitted orally, namely in the case of a personal meeting between the Whistleblower and the RRMR, the minutes prepared by the RRMR serve as acknowledgment of receipt of the Report. In the event that the Whistleblower refuses to sign the minutes, a relevant note is made by their drafter.
- ✓ To keep records for each Report received through the designated Reporting Channels, including complete and accurate minutes of meetings between him and the person submitting the Report, provided the Report is submitted to him orally. In this latter case, to provide the Whistleblower with the opportunity to verify, correct, and approve the content of the minutes by signing them.
- ✓ To conduct an initial assessment of the Report and lay the groundwork for its handling by the competent employees and executives, or to terminate the process by filing the Report when:
 - It is manifestly unreasonable, vague, unintelligible, or

- is submitted or repeated abusively, or
 - it does not contain elements that substantiate a Breach, or
 - there are no serious indications of a Breach.
- ✓ To forward the Report for investigation in a pseudonymized form either to the competent bodies of the Company or to the competent authorities, as the case may be.
 - ✓ To ensure the protection of the confidentiality of the identity of the Whistleblower and any person named in the Report, in accordance with applicable legislation.
 - ✓ To monitor the progress of the Report, maintain contact with the Whistleblower, and, if necessary, request additional information from him.
 - ✓ To inform the Whistleblower of the actions taken within a reasonable period, not exceeding three (3) months from the acknowledgment of receipt, or, if no acknowledgment has been sent to the Whistleblower, within three (3) months from the end of the seven (7) working days following the submission of the Report.
 - ✓ To retrieve any previously filed Report for reassessment, in the event that new information is submitted.
 - ✓ To provide clear and easily accessible information regarding the procedures for submitting Reports to the NTA and, where applicable, to public authorities or institutions or other EU bodies/services.
 - ✓ To design and coordinate training activities on ethics and integrity, and to participate in the development of internal policies aimed at strengthening integrity and transparency within the Company.
 - ✓ To inform, as appropriate, the Company's Management, the Board of Directors and/or the Corporate Governance Council regarding Reports received and their progress.

8.2. Deputy RRMR

The Deputy RRMR is responsible for receiving and monitoring internal Reports submitted through the designated Reporting Channels, in cases where the RRMR is unable to handle the matter and must be replaced (e.g. due to a conflict of interest or an exceptional impediment). The Deputy RRMR, when acting in place of the RRMR, shall assume the same responsibilities as the RRMR, as detailed in Section 8.1. The role of Deputy RRMR has been assigned to the Director of Human Resources.

9. Report management

9.1. Growthfund

The RRMR plays a central role in the proper implementation of this Policy, as he is responsible for receiving and monitoring the Reports submitted through the designated Reporting Channels. The role of Deputy RRMR has been assigned to the Director of Human Resources. However, in the event of a conflict of interest arising in the handling of a specific Report or if an impediment is identified concerning the RRMR, the latter shall immediately recuse himself from the process of monitoring and managing the relevant Report, declaring the impediment to the Board of Directors or the Corporate Governance Council, depending on the person against whom the Report is directed (as defined below), and the Deputy RRMR (or an external advisor) shall fully assume his responsibilities. Regardless of the Reporting Channel used by the Whistleblower, the RRMR shall record the Report in a dedicated file maintained for this purpose.

The handling of submitted Reports is assigned to the Report Evaluation Committee (**Evaluation Committee**) and is carried out in accordance with this Policy and the Company's Report Management Procedure. The members of the Evaluation Committee handling the Report must ensure the preservation of confidentiality and discretion, and perform their duties with integrity, objectivity, and impartiality. The Evaluation Committee is composed of: (i) the Director of Regulatory Compliance of the Growthfund, who serves as the head of the Committee and is responsible for the overall process, (ii) the Growthfund's Director of Internal Audit, and (iii) the Director of Human Resources. In the event of a conflict of interest or an impediment concerning the other members (excluding the RRMR), Growthfund has designated alternate members to replace the primary ones, namely the Director of the Legal Department and the Director of Financial Services. In the event that a conflict of interest is identified involving more than one of the aforementioned individuals, or any insurmountable impediment arises that prevents their proper participation in the Evaluation Committee, rendering its formation impossible, it is noted that the Committee's responsibilities may be assigned to an external advisor. By way of exception, if the Complaint concerns a member of the Board of Directors, it shall be handled exclusively by the RRMR (or, if replaced, by an external advisor), who shall inform only the Corporate Governance Council about the Report and its progress.

Specifically, to the extent that the Report is directed against a member of the Board of Directors, the RRMR shall assess the Report independently or in cooperation with an external advisor. It is at the discretion of the RRMR whether to appoint an external advisor, taking into account in particular the reported incident and the information contained in the Report. If the Report does not concern a member of the Board of Directors, the RRMR shall forward the Report to the Evaluation Committee, which is responsible for assessing the Report either independently or in cooperation with an external advisor.

If the Report requires investigation, the Evaluation Committee (or the RRMR, provided the aforementioned specific conditions apply) may assign part or all of the investigation to designated authorized individuals deemed suitable for each case. Specifically, depending on the nature of the reported Breach and the individuals mentioned in the Report, the Evaluation Committee (or the RRMR, provided the aforementioned specific conditions apply) shall decide on a case-by-case basis with whom to collaborate, whether within or outside the Company, all of whom shall be bound by strict obligations of confidentiality and discretion.

Upon completion of the investigation and the collection of all necessary information, the Evaluation Committee shall inform the Company's Management and submit a relevant report

containing anonymized and aggregated data, unless the identification of the individuals involved is deemed necessary and is in accordance with the applicable framework. Based on the findings of the submitted report, the Company's Management shall decide on the appropriate course of action, taking the necessary and suitable measures to resolve and address any incident. It is specifically clarified that if the Report concerns a member of the Board of Directors, the RRMR shall carry out the aforementioned actions and inform exclusively the Corporate Governance Council, which is responsible for overseeing the Board of Directors and taking the necessary measures to address the reported incident.

The RRMR has the authority to refer the Report for investigation to the competent authorities, as applicable, including indicatively the National Transparency Authority, the Hellenic Competition Commission, the Bank of Greece, the Hellenic Data Protection Authority, the Single Public Procurement Authority, the Greek Atomic Energy Commission, the Hellenic Food Authority, the Consumer Ombudsman, the National Cybersecurity Authority, the Authority for Combating Money Laundering and Terrorism Financing and for Monitoring Asset Declarations, the Independent Authority for Public Revenue, and the General Directorate for Financial Crime Prosecution.

In all of the above cases of referral, the RRMR shall pseudonymize the Report under investigation, namely the details of the Reporting Person and/or any information that may reveal their identity, in accordance with the specific provisions and restrictions of the applicable legal framework. Notwithstanding the above, if the RRMR identifies indications of a criminal offence subject to ex officio prosecution based on the submitted evidence, they shall promptly forward a copy of the Report to the competent Prosecutorial Authority and inform the Whistleblower.

9.2. Growthfund Subsidiaries

Growthfund's subsidiaries establish internal reporting channels and assign the aforementioned responsibilities to appropriate individuals or bodies, in accordance with the provisions set out in Section 9.1 of this Policy. The above composition, as described in the preceding section, is recommended for adoption by Growthfund's subsidiaries to the extent that the corresponding roles exist; otherwise, it may be substituted by other executives, provided that the applicable legal framework is duly taken into account.

10. Whistleblower protection measures

10.1. General protection measures

The Company takes all Reports into consideration. All Reports are assessed and investigated promptly and thoroughly, where required. In any case:

- ✓ All Reports are treated confidentially, unless disclosure is required under applicable law.
- ✓ All personal data are processed in accordance with the GDPR and any other applicable national data protection legislation.

- ✓ The Company shall neither impose nor tolerate any form of retaliation against individuals who submit a Report in good faith or against persons associated with them.
- ✓ The Company informs the Whistleblower of the progress and actions undertaken, to the extent possible, so as not to jeopardize the ongoing investigation.
- ✓ Corrective measures are taken depending on the nature and severity of the Breach or the circumstances reported, in accordance with applicable legislation and the Company's policies and procedures.

10.2. Special protection measures

Special protection measures are provided to the Whistleblower, provided that the Report was submitted either under their name or anonymously and subsequently identified.

a) Confidentiality

A fundamental and inviolable principle of the Policy is the confidentiality of the Whistleblower's identity, as well as the safeguarding of their position and/or professional development. In this context, the Company guarantees the protection of the Whistleblower's identity confidentiality. The identity of the Whistleblower may be disclosed only in the context of a legal obligation, as specified below.

All information related to a Report is treated confidentially, with specific technical and organizational measures applied (e.g. Pseudonymization). Such information and/or the identity of the Whistleblower (directly or indirectly) shall not be disclosed to any unauthorized person or entity, except in cases where the Whistleblower has provided explicit consent for the disclosure.

The confidentiality obligation extends to the RRMR, the Deputy RRMR, the Evaluation Committee, and any other individual involved in the investigation of the Report. Accordingly, the Company guarantees the confidentiality of the Whistleblower's identity and of the information contained in their Report. The confidentiality obligation also applies to the Reported Persons, as well as to any other individual named in the Report. The identity of the Reported Person is likewise protected throughout the entire course of the Report's examination.

By way of derogation, information related to a Report, including the identity of the Whistleblower, may be disclosed exceptionally, without the Whistleblower's consent, but subject to prior written notification, in the following cases:

- a) when required by national and/or European legislation, or
- b) in the context of an investigation by the competent authorities, or
- c) in the context of judicial proceedings,

and provided that this is necessary for the handling of the Report or for safeguarding the rights of defence of the Reported Person, subject to prior written notification regarding the reasons

for the disclosure of their identity and under the conditions set out in paragraph 3 of Article 14 of Law 4990/2022.

b) Prevention of retaliation

The Company is committed to protecting every Whistleblower, provided that the Report has been submitted in good faith and the Whistleblower has reasonable grounds to believe that the Report is true and falls within the scope of the Policy. The same protection is also afforded to intermediaries or third parties (natural or legal persons) who are connected to the Whistleblowers or their Report.

The Company shall neither impose nor tolerate the imposition of any form of retaliation, nor threats or attempts thereof, as a consequence of the Report, including the following:

- ✓ termination, dismissal, or equivalent measures;
- ✓ demotion or denial of promotion;
- ✓ reassignment of duties, change of workplace, reduction of salary, modification of working hours;
- ✓ denial of training opportunities;
- ✓ negative performance evaluation or adverse professional reference;
- ✓ imposition or enforcement of any disciplinary measure, reprimand, or other penalty, including financial penalties, where applicable and enforceable;
- ✓ coercion, intimidation, harassment, or marginalization;
- ✓ discrimination, unfavourable or unfair treatment;
- ✓ deliberate harm, including damage to the person's reputation, especially on social media, or financial loss, including loss of employment and/or income;
- ✓ blacklisting through sectoral or industry-wide formal or informal agreements, which may result in the person being unable to secure employment in the sector or industry in the future;
- ✓ premature termination or cancellation of a contract for goods or services;
- ✓ revocation of a licence or approval;
- ✓ referral for psychiatric or medical evaluation, and
- ✓ denial or deprivation of reasonable accommodations for persons with disabilities.

Any such form of retaliation, which causes or may cause unjustified harm or place the aforementioned persons at a disadvantage, shall be considered a serious Breach of applicable

legislation and this Policy, and must be reported immediately to the RRMR through any available Reporting Channel.

In the event that retaliation is imposed due to the submission of a Report, the following remedial measures shall apply, in accordance with applicable legislation, and specifically:

- ✓ The Whistleblower shall be entitled to full compensation for any form of damage resulting from retaliation.
- ✓ In the event of proceedings before a Court or other Authority concerning harm suffered by the Whistleblower, and provided that the Whistleblower demonstrates that they made a Report and suffered harm, it shall be presumed that the harm was caused as retaliation for the Report.
- ✓ any measures imposed as retaliation shall be null and void.
- ✓ The Whistleblower shall be entitled to request the restoration of the situation to what it was prior to the imposition of the retaliatory measures, provided that this is objectively possible and does not impose a disproportionate burden on the obligated party.
- ✓ Termination of an employment contract in the form of retaliation shall in all cases be null and void.

c) Support measures against retaliation

In the event that a Report is submitted, the persons referred to in point no. 4 of this Policy shall be entitled to support against retaliation; more specifically:

- ✓ free provision of legal advice regarding procedures and legal remedies against retaliation before any Authority, as well as free legal assistance from a list of lawyers designated by the competent bar association, and
- ✓ free provision of psychological support from a list of psychiatrists and psychologists compiled by the Ministry of Health.

11. External reports

Whistleblowers are encouraged to submit their Report concerning any Breaches of Union law through the aforementioned Reporting Channels (internal Report), rather than directly to the competent authority (external Report), without prejudice to their right to submit a Report directly to the competent bodies they deem appropriate in each case. The competent authority for receiving and monitoring external Reports, pursuant to the Whistleblowing Law, shall be the National Transparency Authority ("NTA"). Reports to the NTA must be submitted through the means prescribed by law.

In any case, Whistleblowers may report information through external channels when they reasonably believe that submitting an internal Report would not be handled effectively or that there is a risk of retaliation.

12. Public disclosure

A person who makes a public disclosure concerning Breaches shall not be entitled to protection, unless one of the following conditions is met:

- i. the Whistleblower has previously made both an internal Report and an external Report to the NTA, or has submitted an external Report directly to the NTA, and no appropriate action has been taken in response to the Report within the prescribed time limits;
- ii. the Whistleblower has reasonable grounds to believe that the Breach may constitute an imminent or immediate danger to the public interest, or that there is an emergency situation or a risk of irreversible harm;
- iii. the Whistleblower has reasonable grounds to believe that submitting an external Report to the NTA may pose a risk of retaliation or may not be handled effectively due to the specific circumstances of the case, such as when evidence may be concealed or destroyed, or when the recipient of the Report may be colluding with the perpetrator of the Breach or may be involved in the Breach.

13. Personal data protection

The processing of personal data included in a Report shall be carried out in accordance with national and European data protection legislation, as well as the relevant Company policies. The data subject to processing include the data contained in the Report, as well as any data processed during the submission, handling, and follow-up of a Report. Specifically, the personal data of all parties involved shall be protected and processed solely for the purposes of preventing, detecting, or investigating any Breach.

Sources of the data include the Whistleblowers, the Reported Persons, any intermediaries, witnesses and/or other third parties involved, from whom data are collected during the investigation and follow-up of Reports.

The personal data of all individuals involved in the Report shall be protected and processed exclusively for the following purposes: (a) fulfilment of the Company's legal obligation to establish and operate the reporting channels,

(b) submission, monitoring, management, and archiving of Reports, (c) execution of follow-up actions and, more generally, adoption of necessary measures for the follow-up of submitted Reports,

(d) protection of Whistleblowers, particularly against retaliation,

(e) adoption of measures or legal actions against reported persons who commit Breaches, and

(f) provision of information on any criminal offences to the competent prosecutorial, judicial and/or administrative authorities.

For the reported offences falling within the material scope of Law 4990/2022, the processing of personal data constitutes a legal obligation of the Company (Article 6(1)(c) of the GDPR in conjunction with Article 15(2) of Law 4990/2022). For other reported offences that do not fall within the material scope of the Law, it is in the Company's legitimate interest to disclose potential unlawful acts or abusive practices that expose it to financial and legal risks, harm its reputation and corporate culture, and generally contribute to an adverse working environment (Article 6(1)(f) of the GDPR).

Access to the data included in a Report shall be granted only to authorised individuals involved in the receipt, handling, and investigation of the specific incident, and only to the extent necessary, all of whom are bound to the Company by strict confidentiality and non-disclosure obligations. Specifically, recipients of the personal data included in the Report may, as the case may be, include the Report Reception and Monitoring Officer (RRMO), the Deputy RRMO, the members of the Report Evaluation Committee of the Growthfund, the Data Protection Officer, the Audit Committee, the Board of Directors, other companies within the same portfolio, external advisors bound by confidentiality clauses, legal counsel, the provider of the electronic reporting platform, as well as judicial, prosecutorial, and administrative authorities. In all cases, the RRMO shall disclose only the strictly necessary information required for the thorough investigation of the matters included in the Report.

Personal data shall be retained for a reasonable and necessary period to fulfil the purposes of this Policy, in order to ensure the retrievability of Reports and compliance with the applicable legislation, and in any case until the completion of any investigation or legal proceedings initiated as a result of the Report. Specifically, following the completion of the investigation of the Report, the Company shall retain the personal data for a defined period, which varies depending on the outcome of the investigation, as follows:

- ✓ If the Report is deemed unfounded, the personal data shall be deleted within two (2) months from the date it is filed. However, the retention period may be extended for a maximum of six (6) months, if deemed necessary by the Company's Report Evaluation Committee (or by the RRMO, in cases where the Report is submitted against a member of the Board of Directors).
- ✓ If the Report yields substantiated findings against an employee or executive of the Company, the personal data shall be retained throughout the duration of their employment or relationship with the Company and shall be deleted twenty (20) years after the termination or cessation of the collaboration, regardless of the manner in which it occurs.
- ✓ If the Report yields substantiated findings against an external partner or supplier of the Company, the personal data shall be retained throughout the duration of the collaboration and shall be deleted five (5) years after the termination or cessation of the collaboration, regardless of the manner in which it occurs.

Personal data that are clearly unrelated to the handling of a specific Report, or are excessive, shall not be collected, or if collected inadvertently, shall be promptly deleted to the extent

possible. Moreover, the Company implements the necessary technical and organisational measures to ensure a high level of data security.

Without prejudice to any other provisions of this Policy, the Company shall take appropriate measures to ensure the timely information of data subjects regarding the processing of their personal data in a concise, transparent, and easily accessible format, using clear and plain language, namely prior to the processing of their personal data.

However, the Reported Persons and any other individual named in the Report, in their capacity as data subjects, shall not be informed of the processing of their personal data, by way of derogation from the applicable data protection legislation, for as long as necessary. The provision of information shall be assessed on a case-by-case basis, as there may be instances where such notification may, indicatively: (a) hinder the investigation of the case and obstruct the assessment of the Report, as well as the collection of necessary information and evidence, (b) lead directly or indirectly to the identification of the Whistleblowers, (c) result in the disclosure of confidential information which, due to its nature and especially the overriding legitimate interests of the Company, must remain confidential, (d) impede the establishment, exercise, or defence of the Company's legal claims and/or any criminal proceedings, (e) lead to any form of retaliation, including threats and acts of retribution. In such cases, the Company shall not be obliged to provide information regarding the processing of personal data to the Reported Person or to any third party named in the Report, for as long as necessary. In all cases, the Company undertakes to assess each matter individually, taking into account, for the purpose of notification, the nature of the information and the risks associated with its disclosure. Moreover, the reasons for delaying or refusing to provide notification shall be documented in writing.

Likewise, pursuant to the applicable provisions of Law 4990/2022, the Company may refrain from satisfying the rights granted to data subjects under Articles 15–22 of the GDPR, when exercised by the Reported Person or any other individual named in the Report, to the extent and for as long as deemed necessary for the purposes of preventing and addressing attempts to obstruct the submission of Reports or to hinder, frustrate, or delay the monitoring and management process of the Report, particularly investigations or efforts to ascertain the identity of the person who submitted the Report, as well as for their protection against retaliation. In such cases, the Company may reject the relevant requests of the data subjects in writing and with justification, within the timeframes stipulated by the applicable legislation, for the period deemed necessary.

In cases where the rights of data subjects are restricted, the Company shall take all necessary technical and organisational measures to safeguard the rights and freedoms of the individuals concerned. In the event of refusal to satisfy the rights, the data subjects shall be informed of the reason for the restriction. Alternatively, data subjects may lodge a complaint with the Hellenic Data Protection Authority (HDPA).

14. Measures in the event of a confirmed breach

In the event of a confirmed Breach, the Company may take any necessary and appropriate measures, as applicable, against the Reported Person, following a decision by the competent

corporate body (as specified in section 9.1 of this Policy), in order to effectively address the Breach and prevent the occurrence or recurrence of similar incidents or conduct in the future.

If the individual found to have committed the Breach is an employee of the Company, the latter shall take the appropriate measures, insofar as such measures may be taken in view of the circumstances, and may, depending on the case, terminate the employment contract in accordance with the procedures provided for in the applicable legislation, expressly reserving the right to pursue any other lawful claims, whether judicially or extrajudicially.

Likewise, the Company may take action against any of its employees who is found to have:

- ✓ concealed, covered up, or attempted to cover up the reported Breach;
- ✓ obstructed or attempted to obstruct the submission of the Report;
- ✓ retaliated against or initiated malicious proceedings against the Whistleblower;
- ✓ knowingly submitted a false Report;
- ✓ violated the confidentiality of the Whistleblower's identity;
- ✓ violated this Policy in any other manner.

With respect to individuals not directly controlled by the Company who are found to have committed the reported Breach, the Company shall take all appropriate and legally permissible measures required to address the Breach, including, indicatively, termination of the relevant contract and/or services of such individuals and the exercise of any other lawful rights available to it.

15. Remedial measures in the event of breaches

The Company guarantees that it will actively support the Whistleblower and provide the necessary assistance through all appropriate means and reasonable accommodations, in order to protect them from retaliation and, to the extent possible, restore their working conditions to the state they were in prior to the reported incident, if such conditions have been adversely affected.

In the event that further legal actions have been initiated against the Reported Person in the context and as a result of the Report, the RRMO shall remain in contact with the Whistleblower, where required, throughout the course of the legal proceedings.

16. False Report and Protection Against False Reports

The Company protects individuals who submit Reports in good faith and have reasonable grounds to believe that the information concerning the reported Breaches is true and falls within the scope of this Policy. However, the Company reserves all lawful rights against any individual who knowingly submits false Reports or makes false public disclosures.

In any case, any Reported Person who suffers harm, whether directly or indirectly, as a result of a Report submitted in bad faith retains the protection and remedial measures available to them under the applicable legislation. Reports shall be deemed to have been submitted in bad faith if they are made maliciously, with culpable ignorance as to the truth or falsity of the allegations in question, and/or with the sole intent to harm the Company, the Reported Persons, or other individuals. Employees who submit a Report in bad faith may be subject to sanctions or other lawful measures, at the Company's discretion.

17. Policy Management and resolution of questions

The Policy is managed by the Regulatory Compliance Department, which works closely with the Company's other departments, as deemed appropriate, to jointly address any issues that may arise. The Policy is reviewed periodically with regard to the need for its revision.

This Policy is communicated to all personnel and is available on the Company's website, as well as on its internal network (intranet), which is accessible to all employees.

For any questions, concerns, or clarifications regarding this Policy, you may contact the RRMO directly.