Table of Contents

1. Introduction

Iknowhow SA operates in accordance with ethical rules and the applicable legal and regulatory framework in order to create sustainable value, committed to the highest standards of professional ethics, integrity, transparency and accountability. For this reason, the Company has zero tolerance for actions that may disrupt its healthy working environment, cause harm and jeopardize its reputation and credibility. This Reporting Policy (hereinafter the 'Policy') aims to establish an internal system for reporting breaches of EU law, to protect the persons reporting such breaches, to organize the procedure for submitting, receiving and following up reports.

2. Purpose

The purpose of this Policy is (a) to ensure that the Company complies with Directive (EU) 2019/1937, concerning the protection of persons who report breaches of EU law, and Law 4990/2022 which incorporates this Directive, (b) to define the principles and framework for reporting within the Company, (c) to encourage all those referred to in paragraph 3.2 of this Policy to report in case they become aware of any illegal or unethical behavior within the Company(d) to ensure that reports are handled and the incidents are investigated in complete confidentiality, that the personal data of the parties involved are protected and that those who report will be protected from retaliation.

This Policy sets out the general principles and operating framework under which the Company receives, processes and investigates reports of irregularities, omissions or other criminal acts brought to the attention of staff, customers, suppliers or other stakeholders. The Company adopts and applies this Policy, respecting the principle of proportionality and taking into account the size, legal form, nature and complexity of the activities, ensuring appropriate governance arrangements at all times.

This Policy and any amendments thereto are approved by the Board of Directors of the Company.

3. Scope of application

3.1. Material Scope (Subject-matter of reports)

This Policy is applicable for the protection of persons who report or disclose:

(a) breaches falling within the scope of the Union acts set out in the Annex I of the L.4990/2022 that concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and security of network and information systems;

(b) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU, such as cases of fraud or any other illegal activity against the financial interests of the EU, and in particular as set out in the relevant EU measures;

(c) breaches relating to the internal market, i.e. the area of the EU in which the free movement of goods, persons, services and capital is ensured, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

3.2. Personal Scope (persons to whom this Policy applies)

This Policy applies to persons who report information about breaches obtained in the course of their work, and in particular:

-to workers, regardless of whether their employment is full or part-time, permanent or seasonal, or whether they are seconded from another institution.

- to persons with self-employed status or counselors or domestic workers,

- to shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees

- to any persons working under the supervision and direction of contractors, subcontractors and suppliers

- to persons who report or publicly disclose information on breaches acquired in a work-based relationship which has since ended for any reason, including retirement, as well as to reporting persons whose employment relationship has not yet started, in cases where information on breaches has been obtained during the recruitment process or at another stage of negotiation prior to the conclusion of a contract

-facilitators

-third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons

and

- legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

4. Definitions

For the purposes of this Policy, the following definitions apply:

1. 'Report' means the oral or written communication of information on breaches concerning this Policy
2. 'Person Concerned' means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach (which falls within the scope of this Policy) is attributed or with whom that person is associated
3. 'Reporting Person' means a natural person who reports information on breaches acquired in the context of his or her work-related activities
4. 'Retaliation' means any direct or indirect act or omission which occurs in a work-related context which causes or may cause unjustified detriment to the reporting person and which is linked to the report
5. 'Reasonable ground' means a reasonable belief on the part of a person with similar knowledge, training and experience to the reporting party that the information provided is true and constitutes a breach of Union law falling within the scope of this Policy
6. 'Feedback' means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up

7. ‘Work-related context’ means current or past work activities in Company through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information
8. ‘Breaches’ means acts or omissions that are unlawful and relate to the Union acts and areas or defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope of this Policy.
9. ‘Information on breaches’ means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the Company in which the reporting person works or has worked or in another organization with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches
10. ‘Competent Person to Receive and Monitor Reports’ means the Competent Person to Receive and Monitor Reports concerning breaches which fall within the scope of application of this Policy.

5. Duties/Responsibilities of the Competent person to Receive and Monitor the Reports

The Competent person to receive and monitor the reports has the following duties/responsibilities:

a) provides appropriate information regarding the possibility of submitting a report within the Company and communicates the relevant information in a prominent place within the Company
b) receives reports concerning breaches falling within the scope of this Policy
c) confirms the receipt of the report to the reporting person
d) takes the necessary actions, in order that the Competent Evaluation Committee within the Company deal with the report, or closes the procedure by archiving the report
e) ensures the protection of the confidentiality of the reporting person’s identity and any third party’s named in the report, in order to prevent access by unauthorized persons
f) monitors the reports and maintains contact with the reporting person and, if necessary, requests further information
g) provides information to the reporting person on the actions taken

h) provides clear and easily accessible information on the procedures under which reports may be submitted to the National Transparency Authority (NTA) and, where appropriate, to public entities or institutions, bodies, offices or agencies of the European Union; and

i) plans and coordinates training activities related to ethics and integrity and participates in the development of internal policies to strengthen the integrity and transparency of the Company.

The Competent Person to Receive and Monitor the Reports shall: i) perform his/her duties with integrity, objectivity, impartiality, transparency and social responsibility; ii) respect and observe the rules of confidentiality and secrecy on matters of which he/she has become aware in the performance of his/her duties; iii) refrain from managing specific cases, declaring an impediment where there is a conflict of interest.

6. Procedure of submitting and handling reports

6.1. Procedure of submitting reports

The Company establishes easily accessible reporting channels, encourages the reporting of incidents falling within the scope of this Policy and ensure that all reports received are investigated with confidentiality. The report can be submitted by disclosing the identity of the reporting person or anonymously, in writing or orally or through an electronic platform. Upon submission of a non-anonymous report, the personal data of the reporting person may be disclosed to the person concerned, if requested, under the terms and conditions of the applicable personal data legislation. If the reporting person does not wish to submit a report by disclosing his identity, he/she has the option to submit the report anonymously. However, by submitting an anonymous report, the reporting person will not be able to track the progress of their report.

The ways of submitting a report are as follows:

1. The written report shall be submitted in person or by post to the headquarters of the Company. (340 Kifisias Avenue-15451, Athens, Greece) in an envelope marked "For the attention of the Competent Person to Receive and Monitor Reports " or 'Report of the Law. 4990/2022" or any other indication that the report falls under the provisions of the Law

4990/2022. The written report is also submitted by e-mail to the e-mail address of the person to Receive and Monitor Reports**(**whistleblowing@iknowhow.com).

2. The oral report shall be submitted: a) by telephone with a recording of the conversation, provided that the reporting person has duly consented. The content of the report submitted by telephone shall be documented either by a recording of the conversation in a stable and retrievable form or by a complete and accurate transcript of the conversation in a record prepared by the Competent Person to Receive and Monitor Reports, giving the reporting person the opportunity to verify, correct and agree to the final transcript of the conversation by signing the record. In the case of an oral report, where no recording of the conversation takes place, the content of the report shall be documented in the form of an accurate record, which shall be drawn up by the Competent Person to Receive and Monitor Reports, giving the reporting person the opportunity to verify, correct and agree to it by signing it
   b) by a personal meeting of the reporting person with the Competent Person to Receive and Monitor Reports, which shall be held within a reasonable period of time from the date of the reporting person's request, which may be submitted in writing or orally or by email to the Competent Person to Receive and Monitor Reports . In this case, the Competent Person to Receive and Monitor Reports shall keep a complete and accurate record of the meeting in a fixed and retrievable form, either by recording the conversation, if the reporting person has duly consented, or in writing, which the reporting party may verify, correct, agree to by signing
3. The report via an online platform is submitted online on the specially designed online platform: https://iknowhow.talknow.gr.
4. Reports must be governed by the principle of good faith on the part of the Reporting Person, who must exercise due diligence throughout the process of submitting the report and providing the relevant information. In order to facilitate the investigation and proper assessment of reports, reports are encouraged to be clear, concise and contain all available information, e.g. the events that gave rise to the suspicion/concern/conviction of the breach, with reference to names, dates, documents and locations. If the reporting person, after submitting the report, realizes that it was unfounded/unsubstantiated, he/she must inform the Company in the above-mentioned ways.

6.2. Procedure of handling reports

As soon as a report is submitted, the below handling and investigation procedure will be followed:

The Competent Person to Receive and Monitor the reports:

Confirms the receipt of the report to the reporting person, immediately and, in any case, within seven (7) working days from the date of receipt.

Informs the Group's three-member Report Evaluation Committee, which handles the report with due diligence, impartially and confidentially, and which consists of one executive member of the Company's Board of Directors, one non-executive member of the Company's Board of Directors and one lawyer from the Company's Legal Support Team..

In the event that the Competent Person to Receive and Monitor Reports receives a report in which allegations are made against himself/herself or against the Report Evaluation Committee, he/she is limited to registering it in its register of reports and forwarding it to the National Transparency Authority(NTA) as an external reporting channel, informing the reporting person.

The Report Evaluation Committee:

First of all, investigates whether the report falls within the scope of this Policy.

After the initial evaluation, the Committee then proceeds to further investigation of the report.

If necessary, further information shall be requested from the reporting person, through the Competent Person to Receive and Monitor Reports. The Report Evaluation Committee investigates the report, assesses the accuracy of the allegations contained therein, decides on the merits or otherwise of the report under investigation, records the results of the investigation and, accordingly, recommends (a) the appropriate measures to address the reported breach, such as additional training of employees, creation of new internal controls, modifications to existing procedures, legal action (prosecution, action to recover funds), b) the further investigation of the report, or c) the closing of the procedure and the archiving of the report, to the CEO of the Company, to make the necessary decisions. In case that the report is directed against the Managing Director or the latter finds himself/herself in a conflict of interest situation, then the decision of the Report Evaluation Committee is forwarded to the Chairman of the Company's Board of

Directors, so that he/she can take the necessary decisions. Decisions of the Reports Evaluation Committee shall be reasoned and taken by majority vote.

The above-mentioned Competent Person to Receive and Monitor the reports, informs the reporting person of the actions taken within a reasonable period of time, which shall not exceed three (3) months from the acknowledgment of the receipt, or if no confirmation has been sent to the reporting person, three (3) months at the end of seven (7) working days from the submission of the report. In case of rejection of the report by the Report Evaluation Committee, the procedure is terminated, the above-mentioned Competent Person archives the report and notifies the reporting person, in writing, of the Commission's decision, including the reasons for rejection. Reasons for rejection of the report may relate to cases where:

- The reported acts do not fall within the scope of this Policy.

- The report is incomprehensible or improperly submitted, or does not contain facts which constitute a breach of Union law or there are no serious indications of such breach.

- The report is found not to have been made under the terms of good faith.

7. Non-satisfaction from the final outcome of investigations triggered by the report

If the reporting person considers that his/her internal report has not been addressed effectively, he/she resubmits it to the National Transparency Authority (NTA). Instructions regarding the procedure of reporting to the NTA are available on its website, www.aead.gr.

In particular, concerning breaches of Articles 101 and 102 of TFEU (the EU's free competition rules), the external reporting channel to which the reporting person may address is the Hellenic Competition Commission. Instructions on how to report to the Hellenic Competition Commission can be found on its website, www.epant.gr.

8. Conditions for the protection of reporting persons

The Company protects persons who report breaches that fall within the scope of this Policy and ensures that there is no retaliation. In this context, any form of negative behavior/retaliation against anyone who has submitted a report is prohibited, including threats and retaliatory actions. More specifically, the Company undertakes that employees who have submitted a

Report will not suffer retaliation, harassment or marginalization, intimidation or threats and unfair treatment as a result of their Report, (e.g. dismissal, unfounded negative evaluation, non-provision of leave, exclusion from educational seminars, non-approval of expenses, etc.). Also, unjustified changes to the employment relationship as a result of the Report (e.g. dismissal, suspension, demotion or deprivation of promotion, reduction of salary, change of workplace, relocation, differentiation of duties, change of working hours, etc.) are not allowed. In case of malicious Reporting the above-mentioned protection does not exist. The same level of protection applies to third parties connected to the reporting persons who could be retaliated against in a work context, such as colleagues or relatives of the reporting persons.

If the reporting person is an external partner, early termination or cancellation of a contract for goods or services is not allowed as a result of the Report. Any act of retaliation should be immediately reported to, investigated and resolved by the Report Evaluation Committee. If the investigation reveals that there was indeed retaliation, disciplinary action will be taken against the perpetrator. The person accused of committing the retaliation has the burden of proving that his/her actions are not related to the Report made by the employee (reversal of the burden of proof). In the event that an employee decides to report an incident covered by this policy in which he/she was previously involved, the fact that he/she eventually reported it will be taken into account in his/her favour in any other subsequent proceedings (e.g. disciplinary proceedings). In the event that the reporting employee expresses the desire to be provided with special protection against any retaliation (e.g. transfer to another department of the Company), the Company will consider the possibility of satisfying the relevant request within the existing possibilities.

9. Record and report keeping

A Central Register of Reports shall be maintained. The means of record keeping are specified in the Reports Handling Procedure.

10. Confidentiality – Anonymity

The Company encourages employees and external partners to express their concerns about potential misconduct through the existing reporting channels. The Company also undertakes to make every effort and take every reasonable measure to protect the identity of both the

Reporting Person and the individuals included in the reports and to handle the case with complete confidentiality and discretion. In any case, during the investigation of an incident, the identity of the Reporting Person shall not be disclosed to anyone other than the authorised persons who are competent to receive, monitor and investigate reports, including any qualified external consultants specifically called in to investigate the incident, unless the Reporting Person has given express consent or the Report is found to be malicious. Anonymity is achieved through the use of appropriate technical and organizational measures and in particular through the on-line reporting platform where the possibility of submitting either an anonymous or non -anonymous Report is provided. The Platform, besides being anonymous, supports two-way communication and meets high security standards.

11. Processing of personal data

Any processing of personal data under this Policy is carried out in accordance with the national and European legislation applicable to personal data and the Company's privacy policy. The data of all parties involved are protected and processed exclusively and only in relation to the respective Report and for the sole purpose of verifying the merits 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 will not be taken into account and will be deleted. Only those involved in the management and investigation of the incident can have access to the data contained in the reports. The manner of exercising and the conditions for limiting the rights of the data subjects in the reports, i.e. the reporting persons and the persons concerned, are described in the Complaints Handling Procedure. Personal data are deleted within a reasonable period of time from the completion of the investigation initiated on the basis of the Report. Personal data is deleted from the Reporting Register, the material resulting from the investigation and the reporting platform, in accordance with the timeframes set out in the Reporting Handling Procedure and the Internal Investigation Procedure.

12. Consequences of the breach of the policy

The Company reserves the right to take any appropriate measure against any of its employees, contractors or partners of any kind, if it is found or established in any way that a) they have prevented or attempted to prevent the submission of a report in cases of breaches falling within the scope of this Policy, b) subjected any person who submitted a report under this Policy to any form of adverse treatment; c) retaliated or initiated malicious proceedings against a person who submitted a report under this Policy; d) breached the confidentiality of the identity of a reporting person. The same procedure may also be followed if an employee, contractor or any of its associates intentionally misled the Company about any matter under investigation in the context of this Policy or made false allegations against a colleague, contractor or associate of the Company.

13. Information and awareness-raising

In order to enhance integrity and transparency within the Company, its employees receive appropriate information and training on ethics and integrity and on reporting breaches, ensuring that they are fully aware of their rights and obligations under this Policy, as well as the Company's procedures for reporting and investigating breaches. The Company will ensure that this Policy and any revision thereof will be communicated to all persons concerned. An update on the Policy is published in a prominent place on the Company's website.

14. Approval, Implementation Monitoring and Revision of the Reporting and Protection Policy

This Policy has been developed in consultation with all stakeholders, has been approved by the Company's Board of Directors and fully complies with the provisions of Law 4990/2022, as applicable. It is also subject to regular review to ensure compliance with the current legislation on Protected Reports and the legislation on Privacy and Personal Data Protection.

The Human Resources Department of the Company is responsible for the distribution/publication of the Policy, as well as for monitoring compliance with its requirements.