# Whistleblowing and Anti-Retaliation Policy

# Table of Contents


1. Introduction - Purpose..... 3
2. Scope of Application ..... 3
3. Definitions ..... 4
4. Responsibilities/duties of the Manager of Receipt and Monitoring of Reports..... 4, 5
5. Report submission and management procedure ..... 5
5.1. Report submission procedure ..... 5, 6
5.2. Report management procedure..... 6, 7
6. Non-satisfaction from the results of investigation of the report .....7
7. Requirements for Protection of persons submitting reports..... 7
8. Keeping of records and reports..... 8
9. Confidentiality obligation ..... 8
10. Processing of personal data..... 8, 9
11. Effects from the breach of the Policy..... 9
12. Information and Awareness raising..... 9
13. Monitoring of implementation..... 10

## 1. Introduction - Purpose

Furuno Hellas S.A. (hereinafter referred to as the "Company") is operating based on the code of ethics and the applicable legislative and regulatory framework to create a sustainable value, committed to the stricter standards of professional code of conduct, integrity, responsibility, transparency and accountability. Therefore, it has zero tolerance for actions that may disturb its healthy working environment, harm it and endanger its reputation and reliability.

This Whistleblowing and Anti-Retaliation Policy (hereinafter referred to as the "Policy") aims to the creation of an internal reporting system for breaches of the EU rules of law, the protection of persons reporting such breaches, the organization of the procedure of submission, receipt and follow-up of reports, providing guidelines for the disclosure of information relating to offenses in the workplace or in a work-related framework. The purpose of this Policy is: a) compliance of the Company with Directive (EU) 2019/1937, on the protection of persons who report breaches of EU law and Law 4990/2022 that incorporates it and b) to determine the principles and the relevant framework within the Company.

## 2. Scope of Application

### A. Material scope of application (reports object)

This policy shall apply for the protection of persons reporting or disclosing:

(a) acts of breaching the EU rules of law, according to the more specific provisions of Part I of Annex of Law 4990/2022 (Annex I to this Policy), as well as acts that may be issued subsequently as secondary acts, in the sectors:

i) of public procurements, ii) financial services, products and markets, as well as anti-money laundering and terrorist financing, iii) safety and compliance of products, iv) transport safety, v) environmental protection, vi) radiation protection and nuclear safety, vii) food and feeds safety, as well as animal health and welfare, viii) public health, ix) consumer protection and x) privacy and personal data protection as well as network system and information security,

(b) breaches affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU), i.e., cases of fraud or any other illegal activity affecting the financial interests of the EU, and as further specified in relevant Union measures,

c) breaches relating to the internal market, i.e., the EU area, in which the free movement of products, persons, services and funds 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.

### B. Scope ratione personae (persons covered by this Policy)

This Policy applies to persons reporting information on breaches acquired in the workplace, i.e., Board members, Management Executives and the personnel of the Company, regardless of the type of contract connecting them to the Company.

The protective context of this Policy, also includes third party suppliers, consultants, all types of partners of the Company under a work contract, independent services, salaried mandate, employees through third counterparties of the Company, individuals receiving training, including trainees and apprentices (paid or not), individuals whose work relationship has expired for any reason, including retirement, and individuals whose employment relationship has not yet started, in cases where information in relation to breaches has been acquired during the recruitment procedure or in any other stage of negotiation before the conclusion of a contract are also included.

The scope of application of this Policy does not include cases of violence and harassment in the workplace, which are regulated by the Policy for the handling of violence and harassment in the workplace.

## 3. Definitions

In this Policy, the following definitions shall apply:

1. “Report”: The provision of information regarding breaches hereof to the Manager of Receipt and Monitoring of Reports of the Company.

2. “Person concerned”: natural or legal person, who is referred to in the report as a person to whom the breach is attributed or with whom that person is associated, falling within the scope of application hereof.

3. “Reporting person”: The natural person who reports and provides information acquired in the workplace regarding the breaches.

4. “Retaliation”: Any direct or indirect action or omission which takes place within the workplace, causes or may cause unjustified detriment to the reporting person, or put them in a disadvantage, and is related to the report.

5. “Reasonable grounds”: The justified belief of a person, with similar knowledge, education and experience with the person reporting, that the information they have is accurate and constitutes a breach of Union law, which falls within the scope of application hereof.

6. “Feedback”: 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”: current, former or anticipated work activities within the Company, regardless of the nature of such activities, through which the persons acquire information regarding breaches and in the context of which these persons may suffer retaliation if they report them.

8. “Breaches”: acts or omissions that are illegal according to the Union law or contradict the object or the purpose of the Union law rules, which fall under the scope of application hereof.

9. “Information on breaches”: Information, including reasonable suspicion, about breaches, which occurred or are very likely to occur in the Company, and about attempts to conceal such breaches.

10. “Manager of Receipt and Monitoring of Reports” or "Manager": The legal advisor of the Company appointed as the Manager of Receipt and Monitoring of Reports, as regards breaches falling within the scope of application hereof.

## 4. Responsibilities/duties of the Manager of Receipt and Monitoring of Reports

The Manager of Receipt and Monitoring of Reports has the following responsibilities:

a) provides the relevant information regarding the possibility of reporting within the Company and makes the respective information public at a visible location in the Company;

b) receives reports related to breaches falling within the scope of application hereof;

c) acknowledges receipt of the report to the reporting person;

d) proceeds to all necessary actions in order to address the report to the competent evaluation body/committee of the Company, or completes the procedure by filing the report;

e) ensures the protection of confidentiality of the identity of the reporting person and any third party indicated in the report, by preventing access to it by non-authorized persons;

f) follows-up the reports and is in communication with the reporting person and, if required, requests further information from them;

g) provides information to the reporting person regarding the actions taken;

h) provides unambiguous and easily accessible information on the procedures under which reports may be submitted to the National Transparency Authority and, as the case may be, to public bodies or institutions, bodies, offices or agencies of the European Union; and

i) plans and coordinates training courses in relation to ethics and integrity, participates in the making of internal policies to enhance the integrity and transparency of the Company.

The Manager must: i) perform their duties with integrity, objectivity, impartiality, transparency and social responsibility; ii) respect and comply with the privacy and confidentiality rules for matters they became aware while performing of their duties and iii) refrain from the handling of specific cases, declaring an impediment, if there is a case of interest conflict.

## 5. Report submission and management procedure

### 5.1. Report submission procedure

The Company establishes easily accessible reporting channels, promotes the submission of reports for cases that fall within the scope of application of this Policy and guarantees that all reports will be handled with confidentiality. The Company protects the privacy, the identity and the confidentiality of the person reporting submitting the report and implements the applicable procedure towards the party concerned. The identity of the person reporting will not be revealed to anyone, unless revealing it is required (e.g. for the proper investigation of the report - complaint, for legal reasons, reveal to offices or law enforcement bodies or regulatory bodies, for the exercise or defense of legal claims or administrative law matters) or with the consent of the reporting person. The report may be submitted anonymously or named. By submitting a named report, the personal data of the reporting person may be communicated to the person concerned, if requested by them, subject to the terms and conditions of the applicable law on personal data (Decision of the Personal Data Protection Authority 73/2010). If the reporting person does not wish to submit the report by name, they are given the opportunity to submit the report anonymously. However, by submitting an anonymous report, the reporting person will not be able to monitor the progress of their report.

The ways to submit a report are as follows:

a) in writing, by name or anonymously by registered mail or email to the Manager of Receipt and Monitoring of Reports of the Company (Marios Spanakis son of Vasileios, Attorney in Athens, 2 Zaimi Street, P.C. 10683, Athens, Greece, email: info@mspanakis.gr) with the indication “private and confidential” or

b) orally, via phone at 210-3821057 and 6944332861 or via a personal meeting with the Manager of Receipt and Monitoring of Reports within a reasonable time following an application of the reporting person.

In the event of reporting via phone where the call is not being recorded, the Company may document the oral submission of the report with the form of accurate minutes of the call which will be drawn up by the Manager of Receipt and Monitoring of Reports, providing the reporting person with the opportunity to confirm, correct and agree with the call minutes by signing them.

When a person requests a meeting with the Manager of Receipt and Monitoring of Reports to submit a report, without prejudice to the consent of the reporting person, complete and accurate minutes of the meeting are kept in a written and recoverable format, drawn by the Manager of Receipt and Monitoring of Reports, providing the reporting person with the opportunity to confirm, correct and agree with the minutes of the meeting by signing them.

In case of refusal to sign the minutes as provided above, a relevant entry in the minutes is made by the Manager of Receipt and Monitoring of Reports.

Reports must be governed by the principle of good faith on behalf of the reporting person, who must exercise due diligence throughout the reporting procedure and the provision of the respective information. In accordance with the national law, persons who knowingly made false statements or false disclosures may be punished by imprisonment of at least two (2) years and a fine.

In order to facilitate the investigation and the proper evaluation of reports, the reports should be clear, accurate and include all available information such as e.g. the events that created the suspicion/ concern/ belief regarding the breach, with reference to names, dates, documents and places.

In the event that the reporting person, after the submission of the report, becomes aware that it was unfounded/ non-existent, they must inform the Company in the above-mentioned ways.

### 5.2. Report management procedure

As soon as any report is submitted, the following management and investigation procedure will be followed:

The Manager of Receipt and Monitoring of Reports:

- Acknowledges the receipt of the report to the reporting person immediately and in any case within seven (7) working days from the day of receipt.

- Informs the three-member Evaluation Committee of the Company about the report, which handles the report with due diligence, unbiased and with confidentiality, and which consists of the CEO, the HR Manager and the Finance Manager.

The Evaluation Committee, with the assistance of the Manager of Receipt and Monitoring of Reports, firstly investigates if the report falls within the scope of application of this Policy.

Following the above initial investigation, the Evaluation Committee proceeds to further investigation of the report. If required, further information is requested from the reporting person by the Manager of Receipt and Monitoring of Reports.

In the event that the report is made against a member of the Report Evaluation Committee or any member of the Committee has a conflict of interest, then that member is removed from the list of recipients for the specific report, they do not participate in the investigation of the report and are replaced ad hoc by the Sales Manager.

The Report Evaluation Committee shall investigate the report, conduct audits, evaluate the accuracy of the allegations included, decide on its validity or not, record the results of the investigation and, depending on them, recommend: a) the appropriate measures for handling the reported breach, such as is further training of employees, the creation of new internal controls, amendments to the existing procedures, legal actions (prosecution, action to recover funds); b) further investigation of the report or c) the termination of the procedure and filing of the report to the CEO of the Company in order to make the necessary decisions.

In the event that the report is made against the CEO or that the latter has a conflict of interest, then the decision of the Report Evaluation Committee shall be forwarded to the Chairperson of the Board of Directors of the Company or the Vice-Chairperson, if the CEO is also the Chairperson of the Board of Directors, in order to make the necessary decisions.

The Report Evaluation Committee' decisions must be reasoned and shall be made by majority vote.

The Manager of Receipt and Monitoring of Reports shall inform the reporting person for the actions taken within a reasonable period which shall not exceed three (3) months after the

acknowledgment of receipt or if an acknowledgment has not been sent to the reporting person, three (3) months after seven (7) working days have elapsed from the submission of the report.

In the event of rejection of the report by the Report Evaluation Committee, the procedure shall be terminated, the Manager of Receipt and Monitoring of Reports shall file the report and notify the reporting person in writing of the decision of the Committee, which includes the grounds for the rejection. The grounds for rejection may refer to cases where:

- The actions mentioned do not fall within the scope of application of this Policy.
- The report is incomprehensible or is submitted abusively or does not include facts that establish a breach of Union law or there are no serious indications of such breach.
- It is found that the report was not made in good faith.

## 6. Non-satisfaction from the results of investigation of the report

If the reporting person considers that their internal report was not handled effectively, they may re-submit it to the National Transparency Authority. Instructions regarding the submission procedure of a report to the National Transparency Authority are posted on its website www.aead.gr.

Especially for breaches of Articles 101 and 102 TFEU (on rules of law of free competition of the EU), the external reporting channel to which the reporting person can address is the Competition Committee.

Instructions regarding the submission procedure of a report to the Competition Committee are posted on its website www.epant.gr.

## 7. Requirements for protection of persons submitting reports

The Company protects persons reporting breaches falling within the scope of application of this Policy and ensures non-retaliation. In this context, any type of negative conduct/ retaliation against any person that submitted a report is prohibited, including threats and acts of retaliation. Similarly, the following forms of retaliation are prohibited: a) suspension, dismissal or other similar measures; b) demotion, omission or withholding of promotion; c) removal of duties, change of the place of employment, reduction of the salary, change of the working hours; d) withholding of training; e) negative performance assessment or negative employment reference; f) reprimand, imposition of a disciplinary or other measure, including a fine; g) coercion, bullying, harassment or marginalization; h) discrimination or unfair treatment; i) non-conversion of a fixed-term employment contract to a contract of indefinite term; j) non-renewal or early termination of a fixed-term employment contract; k) intentional harm, including insult of reputation, especially on social media, or financial damage, including business damage and loss of income; l) registration in a “black list”, based on a sectoral or industrial official or unofficial agreement which may entail that the person will not find a job in the sector or industry in the future; m) early termination or annulment of a products or services contract; n) refusal or deprivation of providing reasonable adjustments for people with disabilities.

Any retaliation act must be reported immediately to the Report Evaluation Committee.

Protection requirements:

a) A person making a named report on breaches that fall within the scope of application of this Policy shall be protected, provided that, at the time of the report they had good reasons to consider that the information relating to the breaches being reported were true and fall within the scope of application hereof;

b) Persons reporting anonymously who were subsequently identified and suffered retaliation, shall be protected under the condition that they meet the conditions set out in the above paragraph (par. 7.a).

Similarly, third persons connected to the reporting person who may suffer retaliation in the workplace, such as coworkers or relatives of the reporting person and the personal business or legal persons of interest of the reporting person, or to which they work or with which they are connected in any other way with an employment relationship, shall be protected where necessary.

## 8. Keeping of records and reports

The Company keeps a record for every report it receives, according to the requirements of confidentiality hereof. Reports are stored as confidential, according to the necessary safety standards of the Company, for a reasonable and necessary period, in order to be recoverable and comply with the requirements imposed by this policy, the Union or national law, and until the completion of any investigation or judicial procedure instigated as a result of a report made against the person concerned, the reporting person or third parties.

## 9. Confidentiality obligation

1) Personal data and any type of information that lead, directly or indirectly, to identification of the reporting person, shall not be disclosed to any person except authorized members of the personnel that are competent to receive or follow-up reports, unless the reporting person has given their consent. To this end, the Company shall take the necessary technical and organizational measures for the protection and security in the monitoring of the report.

2) Notwithstanding the above, the identity of the reporting person and any other information may be revealed only in cases required by the union or national law, in the context of administrative, civil or criminal investigations from the competent public authorities or in the context of judicial procedures, and provided that it is necessary to serve the purposes of union or national law or to ensure the right of defense of the person concerned.

3) Reveals under par. 2 of this part are made after the prior written information of the reporting person in relation to the reasons for the reveal of their identity and other confidential data, unless their information undermines the investigations or judicial procedures. After being informed, the reporting person shall be entitled to submit in writing remarks to the Company making the disclosure, according to par. 2, which remarks will not be disclosed. Exceptionally, in the event that the reasons provided for the remarks are not deemed efficient, the disclosure of the identity and other confidential data of the reporting person will not be prevented. The security of the identity of the reporting person and the information which it may conclude, provided for by the special provisions of Union or national law will not be further affected.

The aforementioned, as regards the protection of the identity of reporting persons, shall also apply to the protection of the identity of the persons concerned.

## 10. Processing of personal data

Any processing of personal data hereunder, shall take place in accordance with the General Data Protection Regulation (Regulation EU 2016/679 - GDPR) and Law 4624/2019, without prejudice to the more specific provisions of Law 4490/2022 and the specific arrangements concerning the processing of personal data by competent authorities.

Any processing of personal data that takes place hereunder, shall be conducted for the fulfillment of the obligation of establishing report channels and taking the necessary measures for their monitoring. In the sense of the above processing of personal data, any information related to breaches shall fall within the framework of reports. Transfer of information included in the reports, which may be used as evidence in administrative, civil and criminal investigations and procedures is allowed to the competent supervising and investigating authorities.

The Company, as the data controller, takes the necessary technical and organizational measures in order to collect the necessary and useful personal data, when submitting and

monitoring the reports, to achieve the purpose hereof. Personal data which are clearly not related to the handling of a specific report, or are unreasonable, shall not be collected or, if they were collected accidentally, shall be deleted immediately.

The Company, by way of derogation from Article 5(1)(a), Articles 12 and 13, Article 14(1-4) and Article 34 of the GDPR, does not provide the relevant information on the processing of personal data to the person concerned and any other third party in their capacity as the data subject indicated in the report or the personal data that arose from the monitoring measures and in particular about the source of origin according to Article 14(2)(f) of the GDPR, pursuant to Article 14(5) of the GDPR, in conjunction with Article 23 of the GDPR, for the time period required and provided that it is deemed necessary for the purpose of preventing and handling attempts to prevent the report, impediment, annulment or delay of the monitoring measures, especially relating to investigation, or attempts to identify the reporting persons, as well as attempts to retaliations.

The Company may not satisfy the rights provided for by Articles 15 to 22 of the GDPR when exercised by the persons and third parties indicated in the report, or arose from monitoring measures. In cases of limitation of rights of data subjects, the data controller takes all the necessary technical and organizational measures to protect their rights and freedoms. If the data controller refuses to satisfy their rights, without providing information regarding the reason for the limitation, the data subject shall be entitled to file a complaint to the Personal Data Protection Authority, which may investigate the conditions of limitation of rights and inform the data subject, provided that the information is not harmful to the fulfillment of these purposes.

In the event of personal-data breach, the company does not make any kind of announcement to the data subject according to its obligation provided for in Article 34(1) of the GDPR, if such announcement can be harmful to the purposes of this Policy. It shall inform the Personal Data Protection Authority, which may request the Company to make an announcement of the breach to the data subject if found that the conditions for omitting the announcement are not met.

## 11. Effects from the breach of the Policy

The Company reserves the right to take any appropriate measure against any employee (even dismissal), counterparty or any kind of partner, if it arises or is found in any way that: a) they prevented or attempted to prevent the submission of the report, in cases of breaches falling within the scope of application hereof; b) they have exposed any person who submitted a report based on this Policy to any kind of unfair treatment; c) retaliated or initiated malicious procedures against the person who submitted a report based on this Policy and d) they violated their obligation to respect the confidentiality of the reporting person's identity.

The same procedure may also be followed in the event that the employee, counterparty or any kind of partner intentionally misled the Company for any matter under investigation in the context of this Policy or made false claims against a coworker, counterparty or partner of the Company.

## 12. Information and Awareness raising

In order to enhance the integrity and transparency within the Company, its employees receive the appropriate information and training regarding the ethics and integrity as well as reporting breaches, ensuring that they are fully aware of their rights and obligations in the context of this Policy, as well as the procedures of the Company for the submission and investigation of a report.

The Company ensures that this Policy and any revision will be disclosed to all persons concerned and its content will be included in the Labour Regulation. Information on the Policy shall be published at a visible location in the offices of the Company as well as at the Company's website.

## 13. Monitoring of implementation

The HR Manager shall be appointed as competent for the distribution/publication of the Policy, as well as the monitoring of compliance with its requirements.