



Policy on the Management of Reports/Complaints & Protection of Persons Reporting Violations of Union Law (Whistleblowing Policy)

Purpose

This Policy sets out the Company's framework for the protection of individuals who report breaches of Union law, in accordance with Law 4990/2022, which incorporates Directive (EU) 2019/1937 into Greek law.

This Policy aims, on the basis of the legislative provisions as well as the Company's business ethics and commitment to transparency - principles that are inextricably linked to the Company - to establish the framework for the protection of individuals who submit reports, to clarify the operation of the reporting system, and to set out the procedure for investigating such reports. The Company seeks to ensure full compliance with the spirit of the law, while reinforcing transparency in economic and social life.

Definitions

"Report": oral or written provision of information on breaches of this Policy and of Law 4990/2022.

"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 is attributed or with whom that person is associated.

"Reporting Person" or "Whistleblower": Any natural person of any gender who submits a report within the framework of this Policy.

"Retaliation:" Any direct or indirect act or omission, which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person

"Reasonable Grounds": A justified belief of a person with similar knowledge, training, and experience to the reporting person, that the information they possess is true and constitutes a breach of Union law, falling within the scope of this Policy.

"Public Disclosure": the making of information on breaches available in the public domain.

"Facilitator": Any natural person of any gender who assists a Reporting Person in the reporting process within the work-related context, whose assistance must remain confidential.

"Follow-up Actions": Any measures undertaken by the report recipient, or by any authority or body to which the report is referred due to competence, for the purpose of assessing the accuracy of the allegations contained in the report and addressing the reported breach, including internal inquiry, investigation, prosecution, action for the recovery of funds , or closure of the procedure.



Policy on the Management of Reports/Complaints & Protection of Persons Reporting Violations of Union Law (Whistleblowing Policy)

“Feedback”: Information provided to the reporting person on measures that have been taken or are envisaged as part of the follow-up actions, and the reasons therefor.

“External Report”: Any oral or written provision of information regarding breaches to the National Transparency Authority (NTA).

“Supervisory Authority”: The National Transparency Authority (NTA), established by law as the single external reporting channel for all categories of reports, regardless of type or sector.

“Work-Related Context”: Current, past, or anticipated work-related activities in the public or private sector, irrespective of their nature, through which individuals acquire information on breaches and may suffer retaliation for reporting them.

“Internal Report”: Any oral or written provision of information on breaches to the Report Reception and Monitoring Officer (“R.R.M.O.”).

“Breaches”: Any acts or omissions that are unlawful under Union law, or that defeat the object or purpose of Union law, falling within the material scope of this Law and this Policy.

“Information on Breaches”: Information, including reasonable suspicions, concerning breaches that have been committed or are likely to be committed in the organization where the reporting person works, has worked, is seeking to work, or is in negotiations to work, or in other entities with which the reporting person had contact through or on the occasion of work, as well as information on attempts to conceal breaches.

“Report Reception and Monitoring Officer (R.R.M.O.)”: The natural person designated by public and private sector entities employing 50 or more employees, responsible for receiving reports concerning breaches.

“Applicable Legislation”: All provisions of Greek, European Union, or other legislation to which ELPEN Pharmaceutical Co. Inc. is subject, governing issues of breaches and protection of individuals, as further described below.

Application

This Policy applies to all Company staff, including members of the Management, employees, executives, and external partners, across all Company Divisions and Departments.

Frequency

As described in the relevant procedures.



Policy on the Management of Reports/Complaints & Protection of Persons Reporting Violations of Union Law (Whistleblowing Policy)

Responsibilities

All Company Divisions and Departments, and their respective managers, are responsible for ensuring compliance with this Policy by the employees of their respective Divisions and Departments as described in the procedure.

References

- Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law, and any implementing legislation.
- Law 4990/2022 on the protection of people reporting breaches of Union law, as incorporated into the Greek law, and any implementing legislation.
- Law 4624/2019 on the protection of personal data
- Company's specific Protection Policies and Privacy Statements

PROCEDURE

1. Report Reception and Monitoring Officer (R.R.M.O.)

Appointment of the R.R.M.O.

The Company has appointed specific natural persons as Report Reception and Monitoring Officers, on the basis of their professional qualifications and expertise.

These individuals are duly authorized by the Company to receive, investigate and generally manage all reports of breaches.

All handling of reports is strictly confidential, and their position within the Company does not conflict with the responsibilities assigned to them under this Policy.

The tenure of the Report Reception and Monitoring Officer shall be for a minimum period of two (2) calendar years but may be terminated earlier for good cause.

In the event of a conflict of interest between a Report Reception and Monitoring Officer and a particular Report or Reporting Person, the individual concerned must notify the other R.R.M.O.s accordingly and recuse themselves from the investigation of that specific Report.



Policy on the Management of Reports/Complaints & Protection of Persons Reporting Violations of Union Law (Whistleblowing Policy)

Duties and Responsibilities of the Report Reception and Monitoring Officers

The RRMOs shall:

- a) provide appropriate information on the possibility of submitting a report within the Company and display the relevant information in a visible place in the premises of the Company;
- b) receive reports concerning Breaches falling within the scope of this Policy;
- c) confirm receipt of the report to the Reporting Person within seven (7) working days from the date of receipt;
- d) forward the report for investigation in a pseudonymized manner, ensuring compliance with the confidentiality and data protection requirements of Chapter VI of Law 4990/2022. Where the report is incomprehensible, submitted abusively, or fails to describe facts that may constitute a Breach of Union law, or where there are no serious indications of such a Breach, the process shall be terminated by archiving the Report and notifying the Reporting Person. Should the Reporting Person consider that the matter has not been effectively addressed, they may re-submit the Report to the National Transparency Authority (NTA). The investigation process is further detailed in Article 4 of this Policy;
- e) ensure the protection of the confidentiality of the Reporting Person's identity, as well as any third party named in the report, preventing access by unauthorized persons;
- f) monitor reports and maintain communication with the reporting person, and, where necessary, request further information;
- g) provide feedback to the Reporting Person on the actions taken within a reasonable time, not exceeding three (3) months from the confirmation of receipt or, if no confirmation has been sent, within three (3) months from the expiry of the seven (7) working days following the submission of the Report;
- h) provide clear and easily accessible information regarding the procedures under which Reports can be submitted to the National Transparency Authority (NTA) and, where applicable, to public authorities or EU institutions and bodies,
- i) design and coordinate training activities on ethics and integrity, and participate in the development of internal policies aimed at enhancing integrity and transparency within the Company.



2. Categories of Reports

2.1 Reporting Persons may submit a Report concerning Breaches relating to the following irregularities and/or dysfunctions within the Company. These categories derive from Law 4990/2022.

The following list is not exhaustive but sets a general framework defining the legislative scope. Accordingly, the provisions of the Law and of this Policy apply for the protection of persons who report or disclose Breaches in the following areas:

- public procurement,
- financial services, marketed products, as well as the prevention of money laundering and terrorist financing,
- product safety and compliance,
- transport safety,
- environmental protection,
- public health,
- consumer protection,
- protection of privacy and personal data, as well as the security of network and information systems,
- European Union rules on competition and state aid,
- Breaches relating to the internal market concerning acts that contravene corporate taxation rules.

As noted above, the categorisation of potential reports is indicative and not exhaustive. The scope of potential Breaches cannot be fully predicted or limited.

2.2 It is presumed, both by Law 4990/2022 and by the professional ethics upheld by the Company, that anyone may submit a Report if they become aware of Breaches occurring within the corporate framework. Furthermore, the Reporting Person is not required to provide strong evidence; it is sufficient that there are Reasonable Grounds or adequate indications that a Breach is taking place. However, if the reporting system is misused, criminal sanctions are provided for under the applicable legislation.

3. Named or Anonymous Reports

3.1 The Company guarantees that all reports are recorded, stored, and investigated in strict confidentiality, fully complying with the protection of personal data as required by Law 4624/2019, the Company's Privacy Policy, and Article 14 of Law 4990/2022. The Company is committed to keeping the



Policy on the Management of Reports/Complaints & Protection of Persons Reporting Violations of Union Law (Whistleblowing Policy)

Reporting Person's identity confidential throughout the process. The Reporting Person's identity and any other information may only be disclosed where required by Union or national law, within the context of investigations by competent authorities, or during court proceedings, and only where such disclosure is deemed necessary for the clarification of the Report.

3.2 The Company has established the following communication channels with the Report Reception and Monitoring Officers (RRMOs) for the submission of Reports and complaints:

- i) by email at: **whistleblowing@elpen.gr**
- ii) orally, through a personal meeting with one or more of the Report Reception and Monitoring Officers (RRMOs)
- iii) by an anonymous or named letter

4. Investigation Procedure

4.1 Submission of a Report

- The Company encourages the submission of named Reports and complaints and guarantees that all received messages will be treated with absolute confidentiality. However, if the reporting person does not wish to submit a report under their name, they may do so anonymously, and their anonymity will be safeguarded throughout the process.
- The Report Reception and Monitoring Officers (RRMOs) decide, after consultation, whether to accept or reject the Report/complaint. Grounds for rejection may include:
 - insufficient information and/or evidence,
 - The Report has been made with malicious intent and is not based on factual events.
 - the Report does not constitute a Breach under this Policy and applicable law.
- If a Report is deemed unfounded, it will be archived.
- In the case of archiving, the RRMOs shall inform the Reporting Person about the progress of their Report, and if the Reporting Person persists in their initial claim despite the archiving decision, they may address the matter to the National Transparency Authority (NTA).
- In all cases, acknowledgement of receipt must be provided within seven (7) days from the date of receipt of the report.



4.2 Investigation

4.2.1 If the Report is accepted, the RRMOs must act immediately and initiate the investigation process according to the following methodology and standards of accuracy:

- The investigation of the reporting person's allegations shall commence without delay, with the confidentiality, objectivity, and integrity required.
- If deemed necessary, the RRMOs may invite the complainant to provide supplementary questions, information or clarifications.
- In the event of a conflict of interest between any RRMOs and the complainant or the reported person, or due to the nature of the reported incident, the Officer concerned shall be excluded from the process.
- After gathering all relevant information, the RRMOs shall determine the course of action to clarify the reporting person and address the parties involved.
- Throughout the investigation, the identities of the parties involved, and any developments shall remain strictly confidential, except in the cases noted above and under Law 4990/2022, regarding compliance with judicial proceedings or matters of public interest.
- If the evidence provided by the complainant indicates the commission of a criminal offense prosecutable ex officio, the Report Reception and Monitoring Officers (RRMOs) must immediately forward a copy of the report to the competent local Prosecutor.

4.2.2 The procedure shall be completed within three (3) months from the date of acknowledgement of receipt.

5. Protection from Retaliation

The Company is committed to protecting all persons falling within the scope of this Policy who, in good faith, have made a report, against any form of retaliation with regard to their current position and their future professional development.

Any form of retaliation against persons covered by this Policy is strictly prohibited, including threats and acts of reprisal. In this respect, reporting persons must notify the RRMOs if they are subject to, or threatened with, retaliatory acts.

6. External Reporting to the National Transparency Authority (NTA)

In accordance with the provisions of Law 4990/2022, the Reporting Person may submit an External Report directly to the National Transparency Authority (NTA) through the following means:



- i) **Electronically:** via email to kataggelies@aead.gr
- ii) **By post:** to the postal address of the NTA – Lenorman 195 & Amphiaraou, 104 42 Athens
- iii) **In person:** at the premises of the NTA – Lenorman 195 & Amphiaraou, 104 42 Athens

7. Storage of Reports

7.1 Record-Keeping and Data Management

In accordance with the Company's Written Records Policy, it is necessary to maintain files of all documents and data through which the entirety of the Company's operations and processes is recorded and documented, in either paper or electronic form. These documents may, though not necessarily, contain personal data of natural persons.

7.2 Storage of Personal Data

The Company stores and retains both Reports and personal data contained in written or electronic form. Under the responsibility of Report Reception and Monitoring Officers, all files are stored securely, in line with the provisions below regarding data security.

Paper records are stored in the offices of the Report Reception and Monitoring Officers (RRMOs). All Company offices are locked, with keys held exclusively by authorised persons. Within the offices, the files are stored in cabinets or bookcases, preferably lockable, and not in open desk areas. Archiving is detailed, with categorisation by chronology, type of document, or purpose of processing.

For Reports filed electronically, and the retention period, the provisions outlined in the Company's Privacy Policy apply accordingly.

7.3 General Security Measures

Security measures include, but are not limited to, the following:

- Monitoring compliance with the fundamental security principles, as described above;
- Identification of files that contain or do not contain personal data;
- Compliance with the Company's Internal Audit Procedure, as established in the Company's relevant policy;
- Clear definition of responsibilities and powers of the Report Reception and Monitoring Officers (RRMOs);



Policy on the Management of Reports/Complaints & Protection of Persons Reporting Violations of Union Law (Whistleblowing Policy)

- Implementation of measures for the secure keeping and storage of files in appropriate locations and for the appropriate retention period, as described above;
- Compliance with the Company's Policy on Secure Destruction/Deletion of Personal Data;
- Protection, safe use and storage of data storage devices, particularly portable ones (e.g. external drives, USB sticks);
- Maintenance of backup copies at regular intervals using encryption;
- Compliance with the Policy for the Proper Use of IT Equipment and Services, including policies on the use of portable/removable devices and related technical measures for their proper use;
- Ongoing consultation with the Company's Data Protection Officer on data protection and processing security matters.

8. Records – Personal Data

The Report Reception and Monitoring Officers (RRMOs) maintain a Register of Reports in electronic form, in accordance with applicable national and European legislation on the protection of personal data, including the General Data Protection Regulation (GDPR) 679/2016, Law 4624/2019, and decisions of the Hellenic Data Protection Authority. The Register also includes the outcome of the investigation as well as all data substantiating that outcome.

Any processing of personal data under this Policy is carried out in accordance with the applicable national and European legislation on personal data, as well as the Company's Personal Data Protection Policy. The data of all parties involved are protected and processed solely in relation to the specific report, exclusively for the purpose of verifying its validity and investigating the specific incident.

The Company takes all necessary technical and organisational measures to protect personal data, in line with its applicable Personal Data Protection Policy.

Sensitive information not related to the report is disregarded and deleted.

Access to the data contained in reports is restricted to those involved in the management and investigation of the report, i.e. the Report Reception and Monitoring Officers (RRMOs), including specialised external advisers and/or other Company staff specifically engaged in investigating a particular incident.

Personal data is deleted within a reasonable period following completion of the investigation initiated on the basis of the report, or, in the event of judicial dispute, following the issuance of a final and irrevocable court decision. It is noted that the Company is obliged to provide any information requested by



judicial authorities in connection with a reported incident.

9. Monitoring and Review of this Policy

The Company's Management shall monitor the compliance with and implementation of this Policy, and, where necessary, proceed with its review or amendment, in consultation with the Report Reception and Monitoring Officers (RRMOs).

In addition to regular reviews, the Policy may be amended where significant changes occur in at least one of the following: a) the organisational structure of the Report Reception and Monitoring Officers (RRMOs), b) information systems, c) security requirements, d) technological developments, e) the type and/or processing of personal data, f) findings of internal or external audits demonstrating insufficient and/or ineffective measures with regard to protection and security, or following a personal data processing security breach incident.

10. Contact

For any questions regarding the provisions of this Policy, or if you require further information about your rights and how to exercise them, you may contact the Report Reception and Monitoring Officers (RRMOs) at:
whistleblowing@elpen.gr