

## Privacy Notice in Whistleblowing Procedures

ELLAKTOR Group ensures compliance with applicable laws and regulations by establishing and implementing a Whistleblowing Policy, which includes procedures for submitting, managing, evaluating, resolving and monitoring complaints and other prevention and response measures to potential violations of the law. Employees of the Group (i.e. ELLAKTOR S.A. and its subsidiaries), as well as Third Parties can use all the reporting channels which the Group has established to express concerns, but also to report incidents of any kind of irregularities, omissions or criminal acts (already committed or about to be committed) which concern the Group.

### Who is responsible for the processing of your data

The Controller according to Article 4 (7) GDPR is ELLAKTOR SA (hereinafter "Company"), based in Nea Kifisia, on Ermou St. 25.

The Group may receive Reports from employees of its subsidiaries, or / about incidents concerning its subsidiaries, while making clear that the reporting channel is at group level. Whistleblowers may also request that the investigation be conducted at the subsidiary level. In such case, the Joint Data Controllers in accordance with Article 4 (7) GDPR are the Company and the its respective subsidiary company.

### Data sources and categories of personal data we process

The Report submitted through the confidential reporting channels may contain simple, but also special categories ("sensitive") personal data about the whistleblower, the person(s) concerned, as well as third parties. The data collected could be the name, surname, current job title, company name, e-mail address, and any other information related to the above persons. A Report usually contains information about the specific allegation and how the person concerned, if any, is alleged to be involved in the alleged unlawful or improper conduct. Furthermore, a submitted Report may include documents in the broad sense, i.e., text, photographs, and/or videos.

In principle, we do not request or process special categories of personal data. However, such special categories of personal data may be collected through the Report you submit.

Only the data strictly necessary for the submission of the Report shall be collected. Personal data which are obviously not relevant to the handling of a specific Report, and/or are sensitive data, are not collected, or if collected accidentally, are deleted without delay.

If you submit a Report, we will process the personal data that you choose to share with us. You can submit your Report either with your identity disclosed or anonymously. If you are a person concerned, we will process that personal data contained in the Report submitted against or about you. If we consider that a Report is required to be investigated further, other data may be collected at the stage of the investigation (e.g. from witnesses).

### Purpose and legal basis of the processing

The Group processes the personal data of the data subjects (the whistleblower's, the person's concerned and the third parties' who may be mentioned in the Report) within the frame of reporting channels - including the reporting application (platform) - for the sole purpose of disclosing the commission, or reporting suspicion

of commission, of serious illegal, unethical or generally unlawful conduct, as well as the prevention, restriction and monitoring of such unlawful conduct throughout the Group.

The legal basis for the processing of personal data included in Reports related to violations of Law 4990/2022 is the Group's obligation to comply with a legal obligation (Article 6(1)(c) GDPR).

Furthermore, your personal data will be processed if it is necessary to safeguard the legitimate interests of the Group or the third party (Article 6(1)(e) GDPR). Such legitimate interests of the Group are the prevention and detection of violations within the Group, the verification of the legality of internal procedures and the safeguarding of the integrity of the Group.

Special categories of data are processed only if, in addition to pursuing a legitimate interest and complying with a legal obligation as described above, the processing is lawful and in accordance with Article 9 (2) GDPR.

### **Recipients of personal data**

Access to personal data contained in the Reports is granted to the Person Responsible for the Receipt and Monitoring Reports of each subsidiary of the Group, who are responsible to receive, monitor and manage Reports / complaints as well as other competent executives of the Group or specially authorized persons from the subsidiaries, to the extent necessary to fulfill the aforementioned purposes. In particular, the Person Responsible for the Receipt and Monitoring Reports ensures the confidentiality and protection of the personal data of the whistleblower, unless the whistleblower has given his/her explicit consent to the disclosure of his/her identity or the Report proves to be malicious.

Transfers may take place, where appropriate, to the competent supervisory and investigative authorities, legal representatives and auditors in the context of administrative, civil and criminal investigations and proceedings. The Group shall take appropriate technical and organisational measures when monitoring the Report and communicating with other executives or with the authorities responsible for dealing with it, in case the incident also constitutes an illegal act and is subject to criminal or administrative sanctions.

All persons who are authorised recipients of the data are expressly bound to maintain the confidentiality of the data. The data processors acting on our behalf, such as the company providing the reporting application (platform) , are contractually bound to process data only in accordance with our instructions and to fully comply with this privacy notice, data protection laws and any other appropriate confidentiality and security measures.

### **Retention period**

Your personal data will be retained:

(a) for the purposes of receiving and management of Reports, for a period not exceeding the period necessary for their management, normally not exceeding five years after their filing date, as defined in the Group's Whistleblowing Policy.

(b) for as long as necessary to complete any investigation or judicial proceedings initiated as a consequence of the Report against the person concerned, the reporting person or third parties,

(c) for the purpose of reporting anonymised statistical data to the higher Management until such data are anonymised, which shall in any case be done before the expiry of the retention period set for the handling of Reports.

## Your rights regarding the protection of your personal data

Whether you are the person submitting the Report, or the person concerned or another third party, you can contact our Company or/and the Group's Data Protection Officer (dpo@ellaktor.com) in order to be informed of your rights to information, access, rectification, erasure, restriction and opposition to processing, in accordance with Articles 15 et seq. of the GDPR.

However, you should be aware that we are obliged, pursuant to Article 15 of Law 4990/2022, Article 23 of the General Data Protection Regulation and national legislation (Law 4624/2019), to withhold relevant information on the processing of personal data to the data subject, and to any third person - as data subject - named in the Report, in particular on the source of origin, for as long as necessary and if deemed necessary for the purposes of preventing and countering attempts to obstruct the Report, or delaying or aborting the monitoring measures or any attempts to identify the whistleblower as well as for the their protection against retaliation..

In this context, the rights of access, rectification, erasure, restriction and opposition to processing, when exercised by the persons concerned or third parties named in the Report or resulting from monitoring measures, may also be restricted, as is the right to information.

In case you are not satisfied with our response to your requests/questions, you have the right to address/submit a complaint to the competent supervisory authority which is the Hellenic Data Protection Authority, Kifissia 1-3, 115 23, Athens, Greece, <https://www.dpa.gr/>, tel. 2106475600 via its web portal <https://eservices.dpa.gr/>.