DATA PROTECTION POLICY

GROUP COMPLIANCE DIVISION

ENTRY INTO FORCE: 03/2024

DOCUMENT CODE: GR.ELL.CMP.PL.DPPL.v2-2024/03

Legal framework for personal data protection

The General Data Protection Regulation (EU) 2016/679 (GDPR) and Law 4624/2019 constitute the legal framework, which in general governs the management of personal data and ensures the protection of the rights and freedoms of natural persons when their data is processed. The purpose, inter alia, is to ensure that any processing of personal data takes place in full awareness of the natural persons concerned and that all the principles and conditions of legality laid down by the GDPR and applicable national law are met.

Definitions

Personal data: Any piece of information by which a specific natural person can be identified directly or indirectly (data subject). Such information is a name, an ID number, a tax registration number, a social security registration number, a postal address, a telephone number or an e-mail address, a car registration number, location data, a face image that is received through a closed-circuit television or online identifiers. In addition, personal data can be one or more factors that are specific to the physical, physiological, genetic, psychological, economic, cultural, or social identity of a natural person if through them the natural person can be identified. The data of legal entities are not personal data and are not protected by the relevant legislation.

Special categories of personal data: Personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a specific natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing of personal data: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, registering, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Group Data Protection Officer (DPO): The person appointed by ELLAKTOR Group to exercise independent supervision over any matter relating to the processing of personal data. In particular, the DPO informs and advises the Group, its executives and personnel, monitors compliance with the GDPR and the current national legal framework for data protection, assists in the formulation of relevant policies and procedures and monitors their implementation, and is also the point of contact of the Group for the Hellenic Data Protection Authority.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Company: Company shall mean the company "ELLAKTOR S.A."

Group: Group shall mean the company "ELLAKTOR S.A." and the companies it controls.

General Principles of personal data protection observed by the Group

The companies of the ELLAKTOR Group are bound to fully comply with the obligations and other provisions of the GDPR and applicable national law during the processing of the personal data of the executives, the staff, the associates, the suppliers, the shareholders, the bondholders or the customers of the Group as well as every third natural person, in the exercise of their legal activities and the provision of their services. Compliance with the current legal framework for data protection is a key priority of the Group. For this purpose, the Group implements all appropriate organizational and technical measures and procedures for data protection and respect for the rights of natural persons to which they refer.

The Group is bound not to process special categories of personal data, except health data, provided there is a relevant legal obligation, and is always taking the appropriate technical and organizational measures for the security of this data and for the access to them only by specifically authorized competent persons bound by duty of confidentiality.

The executives, the staff as well as all external associates or any third parties that cooperate or perform works on behalf of the Group, who, within the framework of their legal responsibilities and duties, have access to personal data that are processed in the framework of the Group's legal activities, are obliged to have read, understood, and complied with this Policy.

Violation of the principles set forth in this Policy as well as the provisions of the GDPR and the applicable national legal framework will be dealt with in accordance with the Group's Code of Ethics in addition to any other legal sanctions that violation of the law may result in.

No third party may have access to personal data belonging to the Group without having first concluded a data confidentiality agreement, which imposes on the third party no less burdensome obligations than those to which the Group is already bound to comply with and entitles the Group to monitor third parties for their compliance.

The Company keeps a register of the processing activities in which the processing activities appear with their specific characteristics that refer to the purpose, the legal basis, the categories of data subjects and the categories of personal data that are subject to processing, the potential recipients of this data, the data retention time, possible data transfers outside the European Economic Area and the technical and organizational measures applied for the security of personal data. This file is drawn up and updated by the companies of the Group and is retained collectively by Compliance under the supervision of the DPO and is made available to the Hellenic Data Protection Authority upon its request.

Responsibilities and roles

ELLAKTOR Group is designated as Controller for the processing of personal data in accordance with the GDPR, Law 4624/2019 (articles 60-62) and this Policy.

The DPO carries out their duties with complete independence, does not receive any mandates for the exercise of their duties and refers to the CEO for any matter concerning the management of personal data and ensuring compliance with personal data protection legislation. The DPO constantly advises,

supervises and monitors all activities of the Group and provides relevant information to the Compliance, as a guarantee of compliance with the requirements of the legal framework.

According to the article 39 of the GDPR, DPO's duties are the following:

- Informs and consults the controller or processor for the Company's Management and its employees regarding their obligations arising from the GDPR and the relevant Greek Legislation, in relation to the protection of personal data.
- Monitors compliance with the European GDPR Regulation and the relevant Greek Legislation, as well as with this Policy and Procedure, the Company's policies in relation to the protection of personal data, including the awareness of employees who process personal data and controls that must be carried out. Oversees the process of a security risk impact assessment (DPIA).
- Provides advice, when requested, regarding the impact assessment, related to the protection of personal data in accordance with what is defined by the European GDPR Regulation (article 35).
- Cooperates with the supervisory authority [Hellenic Data Protection Authority (HDPA)] and acts as a point of contact for it on issues related to the processing of personal data, as well as for the cases of consultation defined in article 36 of the European Regulation.
- Receives, in conjunction with Compliance, the requests pertaining to the exercise of rights of the subjects and participates in their management, while the DPO has the authority and responsibility for the communication with the subjects in the context of the management of the requests as the aforementioned process.
- Recommends the implementation of training programs and/or personnel's informing on personal data management issues.
- Participates in all matters related to the protection of personal data.
- Participates properly and in a timely manner in the decision-making process for all matters related to the protection of personal data.
- The DPO is appointed on the basis of professional qualifications and in particular, on the basis of his expertise in the field of data protection law and practice, as well as on the basis of his ability to fulfill the relevant duties. DPO may be a member of the Group's personnel or to perform their duties under a service contract. The contact details of the DPO are published and communicated to the supervisory authority.
- He reports directly to the CEO of the Company.
- He is bound by the observance of confidentiality regarding the exercise of his duties, in accordance with the applicable legislation.

The Management of the Group ensures that the DPO is duly informed of and participates in all issues related to the protection of personal data, supports the DPO for the effective performance of their duties by providing resources necessary to carry out those tasks and to maintain their expert knowledge, and ensures that they can access the personal data and the relevant processing operations of the Group.

The DPO is assisted by Compliance, which is responsible for coordinating the actions required in relation to the Group's compliance with the requirements of the GDPR and the current national legal framework, and in general is obliged to assist the DPO in the exercise of his duties.

Compliance is responsible for maintaining the aforementioned Register of Processing Activities of the Group as well as all relevant policies, procedures, contract texts, information texts, impact assessments (DPIA etc.) and any other evidence that demonstrates the Group's compliance with the GDPR and the national legislation on the protection of personal data. In addition, it is also responsible for maintaining the register of requests for the exercise of the data subjects' rights and the register of notifications of personal data breaches.

The DPO and the Compliance jointly constitute the points of contact with the employees and other data subjects for the exercise of their rights in relation to the processing of their personal data, and for the provision of clarifications on any issue concerning the protection of the relevant personal data within the Group.

All executives and employees of the Group who process or participate in the processing of personal data are responsible for compliance with the legislation on the protection of personal data and are bound by a duty of confidentiality.

Principles related to processing of personal data

The processing of the personal data is carried out by the Group in accordance with the principles as defined in article 5 of the GDPR and are described in the register of processing activities of the Group, and are the following:

(a) Personal data shall be processed lawfully, fairly, and transparently (principle of lawfulness, fairness, and transparency).

(b) Personal data shall be collected only for specified, explicit, clear, and legitimate purposes and shall not be processed in a manner that is incompatible with or in excess of these purposes (principle of purpose limitation).

(c) The personal data collected shall be adequate, relevant, and limited to what is strictly necessary, for the purposes for which they are collected, retained, and processed (principle of data minimization).

(d) Personal data shall be accurate and up-to-date and efforts shall be made to erase or rectify it without delay (principle of accuracy).

(e) Personal data shall be retained in such a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (principle of storage limitation).

(f) Personal data shall be processed in a manner that ensures necessary security and protection against unauthorized or unlawful access, disclosure, loss, destruction, or damage (principle of integrity and confidentiality).

(g) The controller must always be able to demonstrate compliance with the requirements of the GDPR (principle of accountability).

Rights of data subjects

The data subjects have the following rights regarding the processing of personal data maintained and processed by the Group:

a. The right to be informed of the categories of personal data that are being processed as well as of the purposes, the legal basis, the potential recipients, and the general conditions for the processing of their personal data.
b. The right of access to their personal data that are being processed and the conditions of such processing.
c. The right to rectify inaccurate data concerning them or to have incomplete data completed.
d. The right to erasure their data (right to be forgotten), provided that the terms and conditions of Article 17 of the GDPR are met.
e. The right to restriction of processing of data for the reasons and under the conditions of Article 18 of the GDPR, particularly where:
    i. The accuracy of the personal data is contested by the data subject and until the Group verifies the accuracy of that data.
    ii. The processing is unlawful, but the data subjects oppose the erasure of the data and request the restriction of their use instead.
    iii. The Group no longer needs the data, but this data is required by the data subjects for the establishment, exercise, or defense of legal claims.
    iv. The data subjects have objections to the processing during the period that elapses until it is verified whether the legitimate grounds presented by the Group override those of the data subject.
f. The right to data portability. In particular, the data subjects have a) the right to receive the personal data concerning them and which they provided to the Group, in a structured, commonly used and machine-readable format, as well as b) the right to transmit those data to another controller without the Group having the right to hinder, when the processing is based on the consent of the subjects or on a contract and is carried out by automated means.
g. The right to object to the processing of their data on grounds relating to their particular situation, including profiling, under the conditions of Article 21 of the GDRP. If personal data is processed by the Group for the promotion of corporate - commercial purposes (marketing), the data subjects shall have the right to object to the processing of their data for the above purposes, which includes profiling that is related to direct marketing.
h. The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them in a similar way. The exercise of the above right is not allowed (i) if the corporate decision is necessary for entering into, or performance of, a contract between the data subject and the Group, (ii)if this is allowed by law or (iii)if it is based on the data subjects' prior explicit consent.

Data subjects may exercise the above rights by submitting a request as described in the Procedure for the Exercise and Management of the Rights (Annex I). The Group shall be bound to respond to the relevant requests of the subjects in accordance with the provisions of the GDPR, the applicable national legislation and the aforementioned internal procedure.

Data security

All executives and employees of the Group are responsible for ensuring that the personal data retained and processed by the Group are retained secure and are not disclosed or transferred to any third party, unless the third party is authorized by the Group to receive and process such information in the context of (a) the legal activities of the Group and provided that it has entered into a corresponding confidentiality agreement or (b) there is a relevant legal obligation by law or by a court decision.

Executives and employees of the Group have access to personal data based on the needs of their duties and responsibilities and the access rights that have been given to them.

The Group takes all appropriate technical and organizational steps for the security of personal data that it keeps and processes. In particular, inter alia, personal data must be retained in an access-controlled environment that meets the required security measures, in accordance with the requirements of the relevant policies and procedures of the Group.

The Group implements, both at the time of determination of the means for processing and at the time of the processing itself, appropriate technical and organizational measures, which are designed to implement data-protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects (data protection by design).

The Group implements appropriate technical and organizational measures for ensuring that, by default, only personal data, which are necessary for each specific purpose of the processing, are processed.

In case of a personal data breach, the Group without delay and, if possible, within 72 hours from the moment it becomes aware of the fact, informs the Hellenic Data Protection Authority, unless the personal data breach is not estimated likely to result in a risk for the rights and freedoms of natural persons, providing all necessary information and the relevant documentation. When the personal data breach is estimated likely to result in a risk to the rights and freedoms of natural persons, the Group shall communicate the personal data breach to the data subjects, unless such communication requires a disproportionate effort, or in the meantime the Group has applied appropriate technical and organizational protection measures to the personal data affected by the breach and rendered them unintelligible to any unauthorized person, or in the meantime the Group has taken measures which ensure that the risk to the rights and freedoms of data subjects is no longer likely to materialize.

Storage period and destruction of personal data

The Group does not keep personal data in a form that allows the identification of data subjects for a period longer than is necessary in relation to the purposes for which the relevant data were collected, unless there is a legal obligation.

Personal data, whether retained in electronic form or in a physical file, are erased after the expiration of their storage period, which has been determined depending on the category of data and the purpose of processing in the context of the respective activity, according to the Data Retention and Destruction Procedure (Annex II).

The Group could store personal data for a longer period than the specified storage period, if the personal data is to be processed solely for archiving purposes, for scientific or historical research purposes or for statistical purposes, without prejudice to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of data subjects.

Transfer of data outside the European Union

The Group does not transfer any personal data, which retains and processes, to countries outside the European Union (EU) unless there is an appropriate level for the protection of the data subjects based on a relevant European Commission decision or one or more of the safeguards or exceptions set out in Chapter V of the GDPR are valid.

If, in the context of its legal activities, there is a need to transfer personal data outside the EU, the Group selects the appropriate mechanisms for the lawful transfer fully complying with the GDPR and informs accordingly the data subjects.

The DPO checks whether the legal conditions for the transfer of data exist in all the above situations.

Final provisions - approval and revision of the Policy

The Data Protection Policy and Procedure is approved by the CEO and is reviewed whenever necessary. The DPO is responsible for preparing and proposing revisions to this Policy in cooperation with Compliance, and a revision is materialized if deemed necessary.

Under the care of Compliance, the Data Protection Policy and Procedure is posted updated on the Group's website www.ellaktor.com.