PERSONAL DATA PROTECTION POLICY

Table of contents

1. Purpose, Scope and Users

APT SA, hereinafter referred to as the “Company”, strives to comply with applicable laws and regulations related to Personal Data protection where it operates. This Policy sets forth the basic principles by which the Company processes the personal data of customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to the Company and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

All employees, permanent or temporary, and all contractors working on behalf of the Company comply with this Policy.

2. Basic Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing 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 natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An 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, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any

other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Authority: The Hellenic Personal Data Protection Authority

3. Basic Principles Regarding Personal Data Processing

The company as the controller strictly adheres to the data protection principles set out in Article 5 of the General Data Protection Regulation

3.1. Lawfulness, Fairness and Transparency

The company is processing Personal data lawfully, fairly and in a transparent manner in relation to the data subject.

3.2.Purpose Limitation

Personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.3.Data Minimization

THE COMPANY holds the accurate personal data of the subjects and ensures that their observance is limited to what is necessary in relation to the processing purposes. At the same time, it shall apply the appropriate technical measures to achieve the above objectives.

3.4.Accuracy

Personal data that the company holds are accurate and, where necessary, up to date; All the required steps are taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

3.5.Storage Period Limitation

Personal data are kept for no longer than is necessary for the purposes for which the personal data are processed.

3.6.Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Company uses

appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

3.7.Accountability

The company is responsible for and is able to demonstrate compliance with the principles outlined above.

4. Notification, Consent and Rights of Data Subjects

4.1.Notification to Data Subjects

Before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, the company is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Company's security measures to protect personal data. This information is provided through Privacy Notice.

4.2.Data Subject's Consent

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, the company is responsible for providing data subjects with options to provide the consent, with affirmative act, flatly and clearly distinguishable from the other matters and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

Where collection of personal data relates to a child under the age of 16, the company ensures that parental consent is given prior to the collection using the Parental Consent Form.

When requests to correct, amend or destroy personal data records, the company must ensure that these requests are handled within a reasonable time frame. The company must also record the requests and keep a log of these.

Personal data are processed for the purpose for which they were originally collected. In the event that the Company wants to process collected personal data for another purpose, the Company seeks the consent of its data subjects in clear and concise writing. Any such request includes the original purpose for which data was collected, and also the new, or additional, purpose(s). The request also includes the reason for the change in purpose(s).

4.3.Collection

The Company strives to collect the least amount of personal data possible. If personal data is collected from a third party, the Data Protection Officer ensures that the personal data is collected lawfully.

4.4.APT's relation to Third Parties

Whenever the Company uses a third-party supplier or business partner to process personal data on its behalf, the company ensures that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks.

The Company strives to ensure that the supplier or business partner is processing personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes. The Data Protection Officer is responsible for compliance with the obligations described in this Chapter.

4.5.Rights of Access by Data Subjects

The Company as a data controller, the Data Protection Officer is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law.

4.6.Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. The Data Protection Officer is responsible to ensure that such requests are processed within one month, provided they are not excessive. In exercising the right to data portability the data subject has the right to ask direct transfer of the personal data to another data controller in case this is technically feasible.

4.7.Right to be Forgotten

Upon request, Data Subjects have the right to obtain from the Company the erasure of its personal data. The Company as a Controller, and takes necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

5. Response to Personal Data Breach Incidents

When the Company learns of a suspected or actual personal data breach, the company performs as an internal investigation and takes appropriate remedial measures in a timely manner, according to the Data Breach Policy. Where there is any risk to the rights and freedoms of data subjects, the Company notifies the relevant data protection authorities without undue delay and, when possible, within 72 hours.

6. Audit and Accountability

The Data Protection Officer is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

7. Contact

If you have any questions or need clarification regarding the processing of your personal data by the company, please send your message to the email address gdpr@apt.gr and will be happy to serve you directly.