PRIVACY POLICY

The present Privacy Policy (hereinafter referred to as «**the Policy**») has the purpose of ensuring an adequate level of protection to personal data within Up Hellas (hereinafter referred to as «**Up Hellas**» or «**the Company**»), based on the principles and obligations imposed by applicable data protection legislation.Up Hellas is part of «Up Group», a multinational cooperative group of companies based in France which operates more than 60 years.

The Policy is applicable to all the processing activities within Up Hellas and provides the general conditions regarding collection, use, transfer and storage of personal data, imposing obligations to all employees, as well as any other persons carrying out activities for the Company based on collaboration (hereinafter referred to as «**collaborators**»).

While carrying out its business and administrative activity, Up Hellas is collecting personal data regarding its employees, candidates for vacant positions within the Company, clients, beneficiaries of Up Hellas' products and/or solutions including cardholders', representatives and other contact persons of its contractual partners (businesses), visitors, as well as any other persons which may have a contact with the Company. The personal data are processed within Up Hellas exclusively in the limits and conditions imposed by the present Policy and in accordance with the applicable legislation.

1. Definitions:

Supervisory authority	means an independent public authority which is established by a Member State, for the purpose of monitoring the compliance and protection to the rights and freedoms of natural persons as to what concerns the processing of personal data and the free movement of such data within the European Union, pursuant to Article 51 of the GDPR; in Greece, this is *Hellenic Data Protection Authority* ("**HDPA**);
Personal data	means any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one 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	Means the following categories of personal data: data relating to criminal convictions, data revealing racial or ethnic origin, politic opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning a natural person's sex life or sexual orientation;

Recipient	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Applicable legislation	Means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as any national implementation laws or any other law or legal provisions governing the field of data protection;
Controller	means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Processor	means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller;
Processing	means 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, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Registry of processing activities	means the registry kept in accordance with Article 30 of the GDPR which includes, by others, the name and contact data of the controller, the processing activities identified within the Company, including, for each processing activity, the purpose, categories of personal data being processed, categories of data subjects, retention periods, categories of

	recipients;
Data protection officer (DPO)	means the person named by Up Hellas, whose activity observes the provisions of Article 38 and the following of the GDPR.

2. Principles of processing personal data

Personal data collected by Up Hellas are being processed in accordance with the principles provided by Article 5 of the GDPR. The responsibility for observing these principles belongs to each employee within Up Hellas.

2.1. Legality, equity, and transparency

Processing personal data within Up Hellas shall be made, in accordance with the applicable legal provisions, in a transparent and equitable manner towards the data subjects. In this regard, Up Hellas is preparing, where necessary, privacy notices to be displayed, communicated, or sent to the data subjects at the latest at the time of collecting their personal data. When an employee collects the data straight from the data subject, they have the obligation to ensure that the respective data subject has been properly informed regarding the processing of their personal data by the Company.

2.2. Purpose limitations

Personal data are being collected by the Company for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes. Therefore, any employee shall ensure that the purpose of the processing is the same as the one being communicated to the data subject via applicable privacy notice(s). No employee can extend the purpose of processing without previous consulting the DPO.

2.3. Data minimization

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Every employee has the obligation to verify that, in their activity, they do not request, store, transmit, access or process in any other way, personal data not necessary. Otherwise, the employee has the obligation to inform the DPO on the situation, offering details about the circumstances.

2.4. Accuracy

Personal data shall be exact and, where necessary, updated. Up Hellas takes all necessary measures to ensure that inexact personal data, given the purposes of their processing, are deleted or rectified, without undue delay.

2.5. Storage limitations

Up Hellas ensures that personal data being processed are stored in a form that permits the identification of natural persons only for the period necessary for meeting the purposes of their processing. The storage period or the criteria to determine such period shall be found in the registry of processing activities.

2.6. Integrity and confidentiality

Up Hellas ensures the security of personal data against any unauthorised or illegal processing and/or against any loss, destruction or accidental deterioration; the Company takes all necessary technical and organizational measures, taking into consideration the categories of personal data being processed, the state of the art, as well as the likelihood of producing the risks and their consequences.

3. Legality of processing activities

3.1. The purposes and legal grounds

Any employee only processes the personal data strictly necessary for him to fulfil his duties, as they are provided in the individual employment contract or in any other contract concluded with the Company, in the job description or in other applicable mandatory internal documents. Throughout the performance of its duties, they have an obligation to ensure that the processing activities they carry out are not excessive in relation to the original purpose for which the personal data were collected. To the extent that the processing is carried out with a view to achieving a subsequent purpose, the person is obliged to take all necessary measures, in accordance with this Policy, as well as with the internal regulations and procedures, to fulfil the obligations of Up Hellas pursuant to GDPR (*e.g.,* obtaining consent for further processing activity, informing the data subject), in consultation with the Data Protection Officer.

The employee is also obliged to ensure that any processing activity that they carry out is carried out based on a legal ground for processing and has been previously approved within the Company. Any new processing activity carried out may be done only with the approval from the Company's management, with the mandatory participation of the Data Protection Officer.

a. Processing personal data based on consent

When the processing activity is based on the data subject’s consent, the employee collecting the explicit consent of the data subject has the obligation to ensure, before processing the personal data of the respective data subject, that it has been informed via a privacy notice and that it has explicitly and validly given its consent for the processing. The consent shall be documented appropriately by the employee in accordance with the applicable forms, policies and/or internal procedures, as the case may be.

b. Processing personal data based on a legitimate interest

Personal data may be processed based on a legitimate interest of the Company if such interest prevails over the rights and freedoms of the data subjects. The Company’s legitimate interest has, in principle, a legal or commercial nature and it is established at Up Hellas level, in the relevant documents.

c. Processing personal data based on a legal obligation

The processing activity is legal when applicable legal provisions impose or authorize such processing. In this regard, any employee is obliged to ensure that the processing activities they carry out does not exceed the legal framework.

d. Processing personal data based on contract performance

The processing is carried out based on contract performance when it is necessary for the performance of a contract with the data subject or to make steps for such a contract at the request of the data subject. The collaborators are obliged to ensure that all the personal data collected at the moment of concluding the contract are necessary for the conclusion and/or for the performance of the contract. Such assessment is not necessary for activities where draft contracts are used. Although, if there are any suspicions or hints that the respective contract is not compliant with the applicable legislation, the DPO shall be notified without undue delay.

3.2. Retention and deletion

Personal data shall not be kept more than it is necessary for achieving the purposes for which they were collected. The maximum retention period is provided in the registry of processing activities at the Company level, as well as in the privacy notices. In this regard, the persons designated responsible by Up Hellas have the obligation to erase or delete, in accordance with the procedures implemented at the Company level, all the personal data whose retention period have expired and that do not fall under a legal or contractual retention obligation. The same procedure also applies for the erasure of personal data following a right to be forgotten request by the data subject.

It is forbidden for the collaborators to destroy or alter, in any manner, personal data processed by the Company, other than by observing the legal framework, the provisions of the present Policy, the registry of processing activities or any other mandatory internal provisions. Also, it is forbidden for the collaborators to access, sell, transfer, offer or allow access in any other manner to the personal data processed by the Company to any third-party in an illegal way and without an express authorisation from the Company.

3.3. Personal data by Up Hellas's Subcontractors

When any employee concludes, on behalf of the Company, any contract with a service supplier or another business partner which implies processing of personal data in the Company's name, they must ensure that the supplier, when acts as a Data processor, offers a similar level of protection as the one offered within the Company as to what concerns the integrity, security and confidentiality of personal data. Disclosure of personal data to third-parties other than the ones in the present section is strictly forbidden.

In this regard, the employee shall use the draft data processing agreement adopted at the Company level. When the supplier imposes their own draft agreement, the legal department of Up Hellas shall ensure that this contains all the mandatory clauses pursuant of the GDPR. To the extent there are any hints of non-compliance of the proposed agreement with the provisions of the GDPR, the DPO shall be consulted. The service supplier or the business partner

shall process only those personal data being strictly necessary for complying with their contractual obligations and/or solely under the instructions issued by the Company and solely for the agreed purposes.

4. Transfer and/or communication of personal data

The Company may transfer personal data to other subsidiaries of the Up Group, provided that such subsidiaries are located within the European Union (EU) or the European Economic Area. All data transfers shall comply with the requirements set forth by the General Data Protection Regulation (GDPR). The Company shall ensure that all subsidiaries receiving the personal data adhere to the same data protection standards and safeguards as those implemented by the Company. This includes but is not limited to maintaining data confidentiality, integrity, and availability.

Personal data may exceptionally be transferred outside the European Union. Such transfers are subject to appropriate safeguards within the meaning of Article 46 of the RGPD.

The transfer of personal data shall be carried out for legitimate business purposes, such as improving customer service, facilitating internal administration, and ensuring efficient operation of the Up Group's activities.

Personal data may be communicated as well to any authorized administrative or judicial authority or, more generally, to any authorized third party, in order Up Hellas to satisfy its legal or regulatory obligations (on the legal basis of compliance with an obligation or on the legal basis of prevailing interest of Up Hellas in the defense of its legitimate rights).

Data subjects shall retain all their rights under the GDPR, including but not limited to the right to access, rectification, erasure, and objection. The Company shall facilitate the exercise of these rights with respect to the data transferred to subsidiaries.

5. Observing the data subject’s rights

The data subjects have the following rights, according to the GDPR provisions:

(i) Right of access their personal data;
(ii) Right to rectification of inaccurate personal data;
(iii) Right to erasure (”Right to be forgotten”);
(iv) Right to restriction of processing personal data;
(v) Right to data portability;
(vi) Right to object to the processing of personal data;
(vii) Right not to be subject to a decision based solely on automated processing, including profiling.

Up Hellas shall address any data subjects' rights request, if the request had been received at any of the contact data provided by the Company.

Any employee receiving such request shall immediately communicate the request to the DPO, who decides on how to address it.

Any data subjects' rights request shall be addressed by the DPO in maximum one month from the receipt of the request by Up Hellas. To the extent that, in view of the nature, complexity and number of requests received, the DPO is unable to address the request within the legal timeframe, the DPO shall inform the person concerned within 1 (one) month of receipt of the request. In any case, the settlement period cannot be extended by more than 2 (two) months.

The DPO, in collaboration with persons within the Company, verifies the identity of the person submitting the request. Personal data which are not necessary for the registration of the request, collected for the purpose and at the time of confirmation of the identity of the data subject shall be deleted as soon as his identity has been validated.

The DPO shall provide the data subject with the response to their request and shall complete the registry of data subjects' rights requests.

When the DPO considers that the request is manifestly unfounded, the DPO shall register the request alongside the arguments based on which the request had not been addressed.

6. Confidentiality and security

6.1. Confidentiality of personal data

Personal data are subject to confidentiality, as provided in the individual working agreement or any other binding document concluded with the clients and collaborators. In this regard, it is strictly forbidden any processing of personal data by employees for any other purpose than the ones included in their job description. Personal data shall be processed exclusively in the name of and according to the Company's interests. Any processing for private purposes by the collaborators is strictly forbidden. The publication or disclosure of personal data by collaborators, in conditions other than those established by legal provisions, as well as by internal regulations and procedures, is strictly forbidden and may attract disciplinary, civil or criminal liability of these persons.

Also, the access of collaborators is restricted to the categories of personal data that are strictly necessary in order to perform their job duties. Proper implementation of this measure requires a prudent separation and division of roles and responsibilities within the Company. In this regard, each employee must contribute to maintaining the confidentiality of personal data, so that any disclosure or access, either to persons outside the Company or to other collaborators, in an unauthorized manner, is prevented. It is forbidden to communicate access passwords to applications, programs, folders and to any kind of equipment used for the processing of personal data to any unauthorized person.

6.2. Security of personal data

Up Hellas makes every effort to ensure the security and confidentiality of the personal data, by implementing adequate technical and organizational measures. Such measures include:

- Implementation of appropriate technical and organizational measures regarding the identification, prevention, detection, response and recovery of data in case of security incidents regarding data protection;

- Development and implementation of a system to control access to personal data for collaborators (both regarding personal data stored digitally and on paper);

- Development and implementation of a system to control access to personal data for collaborators (both regarding personal data stored digitally and on paper);

- Encrypted VPN connections for the transfer of personal data between production systems;

- Use of appropriate means and procedures for the destruction or deletion of personal data, in accordance with the legal provisions and registers for the processing of personal data.

All collaborators are obliged to comply with the technical and organizational measures implemented by the Company and not to process personal data in a way that cannot ensure their confidentiality and security, in accordance with internal information security policies and procedures.

Personal data must be kept in a way that ensures its integrity, confidentiality, and security. The persons within Up Hellas remain responsible for the disclosure of personal data to unauthorized persons.

When personal data is stored in electronic format, the persons within Up Romania are obliged to ensure that this data is protected against unauthorized access. In this sense, the people within Up Romania will use complex passwords and will save any documents exclusively on the storage devices authorized by the Company through internal procedures (*e.g.* saving documents on personal devices belonging to these persons or in personal e-mail boxes is prohibited). All copies executed for achieving a purpose shall be destroyed as soon as the respective purpose is achieved. The collaborators shall remain liable for disclosure of personal data to unauthorized persons.

When personal data are electronically stored, the collaborators shall ensure that these data are protected against unauthorized access. Thus, the collaborators shall use complex passwords and shall save any documents solely on storage devices authorized by the Company via internal procedures (*i.e.,* saving documents on personal devices or in personal mailboxes is strictly forbidden).

6.3. Security and confidentiality of personal data in the context of using mailboxes and internet in general

The telephonic equipment, e-mail addresses, intranet and internet are exclusively offered to the collaborators by the Company to be used for professional purposes, in accordance with applicable legal provisions and with internal regulations and procedures within Up Hellas.

6.4. Ensuring the privacy of data by design and by default

The Company is liable to take into consideration the collection of the minimum amount of personal data necessary for carrying out the processing activity. This shall be assessed both at the moment of establishing the means of processing, the design of the activity or of the solution, as well as on the period of carrying out the respective activity or, as the case may be, of functioning of the solution.

When designing such activity or solution, it shall also be taken into consideration how the obligation to inform the data subject is done, which are the risks, in order to establish the adequate measures for diminishing the consequences of such, as well as to establish proper technical and organizational measures, as to carry out the activity in safe conditions.

Moreover, the Company is liable for applying technical and organizational measures to ensure that, implicitely, only the necessary data for each of the purposes of the processing shall be processed. This obligation refers to the volume of personal data being collected, the degree of their processing, their retention period and their accessibility.

In this regard, the DPO shall be involved in designing any new activity or technical solution, when such implies the processing of personal data.

7. Roles and responsibilities

All collaborators processing personal data shall comply with the provisions of this Policy, as well as to the applicable data protection legislation.

Revised on January 2025