PERSONAL DATA PROTECTION POLICY

This Personal Data Protection Policy (hereafter **"Policy"**) refers to the personal information collected, processed and used by **"Flexopack S.A.",** with registered offices at Koropi Attica, 37 Ifestou str., tel: (+30) 210 6680000 (hereafter **"Company"** or **"We"**).

Introduction – Our Company as Data Controller

Our Company processes personal data as an employer, prospective employer, supplier of products and services, for marketing related purposes and in the course of its operations and its standard business as flexible packaging manufacturer.

It also processes personal information when co-operating with third parties / business partners and with respect to the visits to its website.

Being member of the Flexopack Group, the Company obviously also processes personal data when interacting with other Flexopack Group companies, whereas - as its shares are trading in the Athens Stock Exchange - it also processes information with regard to its investors and their relationship with the Company.

What kind of data we process

We process personal data which include but are not limited to:

- Information referring to a subject's name, contact details (full address, email address, phone number), birth date and place, gender, bank details, marital and family status, passport, visas and ID numbers, tax and social security numbers, as well as information on previous experience, references and professional certificates, correspondence with or about the data subject, the contract of employment and any amendments to it and all information needed for the execution of a contract of employment, as is the case with our employees;
- Information referring to a subject's name, gender, identity card number or passport number, birth date and place, mailing address, telephone numbers, email address and other contact details, resume, educational qualifications, professional qualifications and certifications and employment references, as well as employment and training history or pictures/photographs maybe included in an application, as is the case with job applicants;
- Information referring to a subject's name, contact details (mailing address, email address, phone numbers), tax ID, payment details, job title and role/function; scanned version of invoices, billing and similar documents, as is the case with our suppliers, including trainers, technicians, lawyers, accountants, auditors and other service providers, and their personnel and representatives;
- Information referring to a subject's name, contact details (mailing address, email address, phone numbers), tax ID, payment details, job title and role/function, delivery information, as is the case with our clients and our clients' personnel and representatives; etc.

- Information about a subject's IP address, browser type and Internet Service Provider, visited websites, referred URL, date-time-duration of the visit, extracted data and downloaded files etc., as is the case with our website visitors.
- Information referring to a subject's name, identity card or passport, citizenship, contact details (mailing addresses, phone numbers, email addresses), tax ID etc., as is the case with our shareholders, co-beneficiaries of the shares etc.

Special categories of data

Where necessary, we may keep information relating to a subject's health, which could include reasons for absence and /or accident reports and notes, as well as medical records, as is the case with our employees and staff.

This information is used in order to comply with our health and safety and occupational health obligations, including in order to consider how a subject's health affects the ability to work and fulfil the respective employment obligations, as well as to comply with our statutory obligations and applicable legislation with regard to recruitment, employment and other industrial or professional legal requirements with respect to occupational medicine.

All above data and any other data that constitutes special category of data, including references to a subject's ethnic origin /nationality etc. are lawfully collected and processed by the Company and, unless this is not authorized or required by law or such information is required to protect the subject in an emergency, we obtain the subject's explicit consent.

Where we collect personal data from

The Company collects personal information:

- Directly from the data subject, as is the case with job applicants, employees, clients' representatives and suppliers' contact persons etc.;
- From internal sources, i.e. from the several Departments of the Company or from other Group entities and/or entities otherwise affiliated with the Company, as is the case with the contact details of another Group company's supplier or client etc. within the Group's supplier relationship management;
- From external third parties, including agents, intermediaries, suppliers, business partners, advisors etc.;
- Through the electronic information system of the Athens Stock Exchange Group, in the context of our communication with it, when, for example, we receive the necessary records for updating our shareholders' registers;
- From publicly accessible sources, i.e. from trade and business registers, industry networking and exhibitions, internet sources, directories or newspapers etc.

Why we process personal data

Personal data is processed by our Company as necessary for the performance of our core business. In particular and as the case may be:

- We process our employees' personal data in order to fulfil our contractual obligations towards them within the framework of the employment agreement executed between

us (for reasons of payment etc.), as well as to comply with legal requirements (announcement to the authorities, social security payments etc.);

- We process job applicants' personal data in order to assess their application and eva;uate their overall qualifications and ability to work for us, having eventually prompt consent thereof, in which case they – either directly or through an agency or otherwise in question – have delivered their resume to our Company;
- We process our suppliers' personal data in order to meet our contractual and legal obligations towards them within the framework of the supply or services or other commercial or other agreement executed between us (for reasons of payment, receipt of services or products etc.);
- We process our clients' personal data in order to comply with our obligations arising by law or the business relationship therewith (for reasons of delivery of products, credit management, invoicing processing, contact arrangements etc.);
- We process our shareholders' data in order to comply with our legal obligations and regulatory requirements as a listed company.

In the cases where the processing is made for contract fulfillment reasons, the purpose of personal data processing is determined by the contract in place with the data subject, whereas in the case where the processing is dictated by law or regulation, the purpose thereof is usually related to provisions of commercial, industrial, trade or tax authorities and bodies or to serve control purposes from authorities.

In certain cases, we need to process personal data to pursue our legitimate business interests, for example to prevent fraud or potential crimes, for administrative purposes or to protect the Company's assets and to improve our efficiency, as is the case with our CCTV systems recordings, personal data required for clients' complaints handling, transfer of data within the Group etc..

Where this is the case, we try to never process a subject's data where these interests are overridden by the subject's own interests and we only use methods and technologies which are necessary, proportionate and implemented in the least intrusive manner, by appropriate means that ensure a balance with the subject's fundamental rights and freedoms.

Without such data, the Company may not be in the position to conclude contracts with suppliers and customers, continue the employee-employer relationship and/or provider-receiver arrangements etc., as the case may be.

We also sometimes process personal data upon the subject's consent (as is the case with those of our employees who consent to the processing of their personal data when voluntarily entering a group insurance policy etc.).

In such cases the data subject may withdraw consent at any time, such withdrawal not affecting, though, the data processing up to the date of the withdrawal.

Monitoring / CCTV surveillance / E-mail correspondence

While on the premises of our Company, a data subject is in certain cases monitored through the use of CCTV system, recording persons' images.

Outside the Company's premises it may be that corporate equipment, including laptops or tablets etc. and telephone/mobile telephone use, may also be monitored.

All for reasons relating to the subject's personal safety and integrity and as precautionary/preventive measures against crimes or other possible dangers to the subject; and to protect our Company's assets and resources.
Any personal data (name, address, title/position, contact details) we send and/or receive in our e-mail or other electronic correspondence is processed in compliance with the GDPR and any other applicable law or regulation.
Our Company uses the personal data contained therein and any attachments thereto lawfully, fairly and in a transparent manner; for specified, explicit and legitimate purposes.
Our correspondence recipients are duly informed that they have all rights provided for by respective legislation regarding their personal data.

How we use and protect personal data

We do not collect more information than we need to fulfil the purposes for which we process personal data.
We hold accurate and up to date data in manners that reasonably ensure appropriate security thereof, protection against unauthorized or unlawful processing, accidental loss, destruction or damage.
We restrict physical access to authorized persons and maintain and use appropriate technical and organizational measures and specified technological solutions and IT systems to protect the integrity, safety, security and availability of the personal data we process.

Automated decision making and profiling

The Company does not use automated decision making for procedures that have legal implications or similarly significant impact on the data subjects and our decisions are made upon human reviewing.
We do not proceed to profiling within the meaning of the applicable personal data legislation.

For how long we retain personal data

Personal data is retained for no more than it is necessary for the purposes for which it is processed for.
For so long as personal data is retained by the Company, we implement and at all times have in place appropriate technical and organizational measures as required by law, in order to safeguard the rights of the data subjects and to ensure the safety and confidentiality of the personal data processed, including restricting unlawful or unauthorized access to such data and limiting to the best possible extent accidental loss, destruction or damage thereto.
When we process personal data based on the data subject's consent, the processing s made for as long as the consent remains valid and until such time it is withdrawn thereby.

Who receives personal data

A subject's information is disclosed to appropriate Company's personnel. We may also disclose personal data to competent authorities if and insofar this disclosure is mandatory under applicable law (disclosure to tax authorities and to internal or external auditors evidently included).

We also disclose personal data to service providers, as well as to external consultants, training providers, business associates and professional advisors, including lawyers and accountants, as well as to other third parties, if we are legally compelled to do so (industry requirements included) or where we need to comply with our contractual duties to the data subject, for instance where we may need to pass on certain information to our insurance associates in case of an accident, to our IT structure providers, banks or other financial institutions for credit and account handling etc., as well as for logistics and products delivery matters.
In all such cases, we do so where appropriate and only in accordance with local laws and requirements and we try to at all times ensure that such third parties have undertaken appropriate data processing obligations to ensure the security and confidentiality of the subject's data.
Due to our global activities and our Group structure, personal information may be transferred outside of the E.E.A. when and to the extent we need to comply with our legal or contractual requirements and/or for purposes connected with the management of the Group's business (for example, for reasons of centralized supplier and customer services, centralized IT services and/or internal shared service center in finance and accounting).
We do so only where an adequate level of protection is ensured or where we have in place safeguards including the use of standard contractual terms, to ensure the security of a subject's data in case of these transfers or upon explicit consent of the data subject.
In view of continuous development and expanding our business, we may be involved in mergers and/or acquisitions with other entities, in which cases it is typical to have personal data entailed in the transaction or potential transaction. The Company ensures the confidentiality and security of personal data processed with respect to such transactions by accordingly implementing, in all such cases, personal data protective provisions and/or other safeguards (non-disclosure and data protection obligations imposed on the potential subsidiary etc).

When we assign data processing

Where the Company relies on a third-party data processor, to execute personal data processing on its behalf, we choose one who provides adequate security level and measures and undertake reasonable steps to ensure compliance of the data processor with such measures, binding ourselves with it with respective data processing agreements.

Future use and update

If in the future we intend to process personal data for a purpose other than that which it has been collected for, we will inform the subject of that purpose and any other relevant information if such purpose is not compatible with the initial, to the extent permitted by law.

Data subject's rights

If and to the extent we process a subject's personal data based on his/her consent, the subject may withdraw consent and request us to stop using and/or disclosing such personal data for any or all of the purposes for which consent has been granted to the Company.
A data subject is also entitled to request access to his/her personal data, i.e. provision of a copy thereof and/or respective information on his/her personal data processed by the Company, as

well as rectification of any inaccurate personal data or supplementation thereof, erasure or restriction of processing, as the case may be and under the legal prerequisites thereof.
He/she also has the right to object to our Company's processing, if and as the case may be, as well as to receive the data in machine-readable format.
To proceed to submitting the respective applications, as well as for any further query or clarification needed by the data subjects, they may address the Company directly as follows:

Postal address: 37 Ifestou str, Koropi 19400, Attica Greece.
Telephone: (+30) 210 6680000
e-mail: gdpr@flexopack.com

Exercise of above rights is made by the data subjects through specific forms submitted to the Company, which are available for free.
The Company acts on such requests free of charge, without undue delay and in any event within one (1) month from receipt of the request. If, however, the request is complicated or there is a large number of requests, the Company will inform the applicants for extension thereof and, in the event that any requests are manifestly unfounded or excessive, for example because of their repetitive character, the Company may either charge a reasonable fee, considering its administrative costs for taking the action requested or refuse to act on the request.
In the case where any data subject believes his/her personal data protection is breached by the Company, he/she may file a respective complaint before the competent Data Protection Authority (ΑΠΔΠΧ / www.dpa.gr / 1-3 Kifissias Avenue, P.C. 115 23, Athens / tel.: +30 210 6475600 / fax: + 30 210 6475628 / e-mail: contact@dpa.gr).

Changes to this Policy

We reserve the right to make changes to this Policy from time to time.
Regularly reviewing our website ensures that a data subject is always aware of the updated version.
If we make material changes to this Policy, we will promptly provide notification via prominent notice on our website or to the relevant data subjects' category.