POLICY ON THE PERSONAL DATA PROTECTION AND PROCESSING

TABLE OF CONTENTS

1. Purpose

The main purpose of this Personal Data Protection and Processing Policy ("Policy") is to to determine the procedures and principles to be followed by data processors in accordance with their relationship with **Kimteks Poliüretan Sanayi ve Ticaret A.Ş.** ("Company"), by making explanations about the personal data processing activity carried out by the Company in accordance with the law and the systems adopted for the protection of personal data, and to ensure transparency towards the persons whose data is processed.

The company shall perform its activities in accordance with the provisions of the Turkish Constitution and the international conventions to which we are a party, as well as Personal Data Protection Law ("PDPL") and relevant legislation on the protection and privacy of personal data. The company is sensitive to the protection of personal data, fundamental rights and freedoms, and focuses on fundamental human rights such as right of privacy and freedom of thought in all its activities.

2. Scope and Implementation

This Policy has been prepared in accordance with applicable regulations and international standards. The Company shall primarily implement this Policy in all data processing activities such as data processing, transfer, modification.

The Company also has different policies on the protection of personal data and the information security

in relation to certain business activities and processes. This Policy does not invalidate the data protection terms stipulated in different policies of the Company, unless it contains additional terms or demands a higher standard for the protection of personal data. This Policy is implemented in conjunction with such other policies and procedures as appropriate.

In case of conflict between the provisions of the current legislation on the protection and processing of personal data and the provisions of this Policy, the current legislation shall prevail.

3. Definitions

***PDPL*:** Personal Data Protection Law No. 6698

***GDPR*:** European Union General Data Protection Regulation

***Data Processor*:** The natural or legal person who processes personal data on behalf of the data controller based on the authority given.

***Data Controller*:** The person who determines the purposes and means of processing personal data and manages the facility where the data is systematically kept (data recording system)

***Data Owner/Respective Person*:** Natural persons whose personal data are processed, including, but not limited to, employees, customers, business partners, shareholders, officials, potential customers, candidate employees, interns, visitors, suppliers, and employees of partner institutions, third parties and those listed here, who have commercial relations with the Company and its subsidiaries.

***Explicit Consent*:** Consent on a specific subject, based on information and expressed with free will,

***Personal Data*:** All kinds of information related to an identified or identifiable natural person.

***Sensitive Personal Data*:** Data on the race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, dresses, their association, foundation or union membership, health, sexual life, criminal conviction and security measures and their biometric and genetic data.

***Personal Data Processing*:** All kinds of actions performed on the data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data through fully or partially automated means (or through non-automated means provided that it is a part of any data recording system).

***Anonymization of Personal Data*:** The procedure of making personal data unrelated to a certain or identifiable natural person under any circumstances, even by matching other data.

***Deletion of Personal Data*:** The procedure of making personal data inaccessible and unusable for the relevant users in any way

Destruction of Personal Data: The procedure of making personal data inaccessible, irretrievable and reusable by anyone in any way

***PDP Board/Board*:** Personal Data Protection Board,

***PDP Authority/Authority*:** Personal Data Protection Authority,

4. Personal Data Processing

a. Principles of Personal Data Processing

The Company's policies and procedures are implemented in accordance with the processing principles stipulated in the PDPL and relevant legislation. We are aware that these principles are of vital importance in the execution of the rights of the data owner and in their control over the data, and we are extremely sensitive to focus on these principles in all our processing activities. The principles in our personal data processing activities are as follows:

- Personal data are processed in a transparent and lawful manner.

The Company's data processing activities are based on the legal processing reasons included in the PDPL. In addition, it takes into account the reasonable expectations of the data owners due to the good faith. The Company shall use a clear and understandable language in its communication with the data owner and is always easily accessible.

- Personal data are only processed for specific, explicit and legitimate purposes.

Prior to the implementation of the data processing activities, the Company determines the purpose of the processing activities. The data are processed only for additional purposes that are compatible with the primary processing purpose. For each additional purpose, the compliance with the primary purpose is determined based on the internationally accepted criteria. The Company shall inform the data owners about the purposes of data processing in accordance with the principle of transparency.

- Personal data are associated, limited and restrained for the purpose for which they are processed.

The Company processes the necessary amount of data. The data are obtained using the most appropriate method for the data privacy and security. In the processing activities, the Company shall refrain from disproportionate interference with the rights, interests and freedoms of the data owners.

- The personal data are accurate and updated, where necessary.

The Company shall that the data are up-to-date in all processing activities. The Company shall destroy or correct missing, erroneous or incorrect data as soon as possible. The Company shall regularly check the up-to-dateness of the data.

- The personal data are retained for as long as required by the relevant legislation or for the purpose for which they are processed.

Upon the annulment of processing purposes, the data are deleted, destroyed or anonymized as soon as possible.

- The Company ensures appropriate security while processing the personal data.

The company considers the data security as the main principle. It follows the best practices in this direction and takes the necessary administrative and technical measures.

- The Company demonstrates that it complies with other principles of PDPL and/or GDPR.

The Company complies with the principle of accountability in all processing activities.

b. Purpose of Personal Data Processing

The purposes of processing personal data are as follows:

- To Execute Emergency Management Processes
- To Execute Employee Candidate/Intern/Student Selection and Placement Processes
- To Execute Application Processes of Employee Candidates
- To Fulfill Employment and Legislation Obligations for Employees
- To Execute Benefits and Vested Benefits Processes for Employees
- To Conduct Audit/Ethical Activities
- To Conduct Educational Activities
- To Execute Access Authorizations
- To Execute Activities in Compliance with the Legislation
- To Execute Finance and Accounting Affairs
- To Ensure Physical Space Security
- To Execute Assignment Processes
- To Conduct Internal Audit/Investigation/Intelligence Activities
- To Conduct Communication Activities
- To Plan Human Resources Processes
- To Execute/Supervise Business Activities
- To Execute Occupational Health/Safety Activities
- To Receive and Evaluate Suggestions for Improvement of Business Processes
- To Conduct Logistics Activities
- To Execute Goods/Service Procurement Processes
- To Execute Goods/Service Post-Sales Support Services
- To Execute Goods/Service Sales Processes
- To Execute Goods/Service Production and Operation Processes
- To Execute Activities for Customer Satisfaction
- To Manage Organizations and Events
- To Execute Storage and Archive Activities
- To Execute Contract Processes
- To Follow-up Requests/Complaints
- To Ensure the Security of Movable Property and Resources
- To Execute Supply Chain Management Processes
- To Execute Wage Policy
- To Execute Marketing Processes for Products/Services
- To Ensure the Security of Data Controller Operations
- To Execute Talent/Career Development Activities
- To Provide Information to Authorized Persons, Institutions and Organizations
- To Create and Track Visitor Records

c. Legal Reasons for Processing Personal Data:

When processing personal data, the Company relies on one of the legal processing conditions stipulated in Article 5 of the PDPL. The conditions and terms of processing personal data - the compliance with the law - are listed in a limited number in the Law and these conditions cannot be extended. When processing personal data, the Company relies on the following legal grounds:

- The explicit consent of the data owner,
- It is necessary to process the personal data of the contractual parties, provided that it is directly related to the establishment or execution of an agreement,
- It is mandatory for the data controller to fulfill its legal obligation,
- It is mandatory to process data for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data owner.

The company does not rely on a legal reason for explicit consent in the presence of another legal reason.

d. Legal Reasons for Sensitive Personal Data Processing

Sensitive data are those that will expose the person to discrimination in case of disclosure such as religion, race, belief, health or sexual life. Sensitive personal data may not be processed without the existence of limited legal grounds stipulated in the PDPL, Article 6.

In this context, the Company processes sensitive personal data other than health or sexual life based on;

- The explicit consent of the data owner and legal reasons.

. Health data are processed based on;

- The explicit consent of the data owner,
- The protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing by persons under the confidentiality obligation,

.

5. Disclosure Requirement

The company is obliged to inform the data owners in accordance with the KVKK and the Communiqué on the Procedures and Principles in Fulfilling the Clarification Obligation. If the personal data are obtained from the data owner, the Company shall inform the data owners personally or by authorized persons at the time of obtaining the data. If the personal data are not obtained from the data owner, the Company is obliged to inform within a reasonable time, and if the data are to be used or transferred for communication with the data owner, the Company shall fulfill the disclosure requirement at the first communication or transfer.

The Company shall inform the data owners about the legal entity and address information of the Company, the purpose of processing personal data, to whom and for what purposes the processed data will be transferred, the method of collecting personal data and the legal reason and the rights stipulated in the PDPL, Article 11.

When the purpose of processing personal data is changed, the Company shall inform the data owner prior to the data processing activity.

The Company shall process the data of the following persons and publish the clarification texts at a defined place:

- **Employees**

It refers to the employees employed by the Company. The Employee Clarification Text has been delivered to them by hand/e-mail.

- **Employee Candidates**

It refers to the employee candidates who apply to the Company physically or using various portals. The Employee Candidate Clarification Texts are delivered by hand or submitted by e-mail.

- **Supplier Employee**

It refers to the employees of the parties from which the Company purchases goods, products or services for the production and operations of the Company's goods, products and services. In accordance with the agreements between the parties, the disclosure to the supplier employees shall be performed by the supplier company.

- **Supplier Official**

It refers to the officials of the parties from which the Company purchases goods, products or services for the production and operations of the Company's goods, products and services. In accordance with the agreements between the parties, the disclosure to the supplier officials shall be performed by the supplier company.

- **Potential Product or Service Buyer**

Refers to the people to whom the company wants to sell products or services. Potential Customer Clarification Texts shall be submitted by e-mail.

- **Product or Service Buyer**

Refers to the people to whom the company sells products or services. In accordance with the agreements between the parties, the disclosure to the product or service buyers shall be performed by the company to which the said employees are affiliated. In necessary cases, which are not for the execution of the contract, the Data Controller shall perform the disclosure.

- **Intern**

It refers to the interns employed by the Company. The Intern Clarification Text shall be delivered to them by hand/e-mail.

- **Intern Candidate**

Refers to the intern candidates who apply to the Company physically, through the website or various portals. The Intern Candidate Clarification Text shall be submitted by hand/e-mail.

- **Online Visitors**

Refers to online visitors who access the company's websites. Online Visitor Clarification Texts are published at www.kimpur.com.

- **Visitor**

Refers to the visitors who visit the company's offices and facilities. Visitor Clarification Text shall be provided at the office entrances. They shall be delivered by hand.

- **Reference Person**

Refers to the reference persons who share the information of employee candidates and intern candidates who apply to the Company physically, through the website or various portals. Reference Person Clarification Texts shall be submitted by e-mail.

6. Data Security

As the data controller in the processing of personal data, we are obliged to prevent the unlawful processing and access of personal data and to ensure its protection. Therefore, the Company has taken all technical and administrative measures regarding data security, including additional measures required for the protection of sensitive personal data. In this context, the measures taken by our company are listed below.

- **Technical Measures**

- We ensure network and application security.
- We use a closed system network for personal data transfers via the network.

- We implement a key management.
- We take security measures within the scope of procurement, development and maintenance of information technology systems.
- We ensure the security of personal data stored in the cloud.
- We implement data masking, when required.
- We cancel the authorizations of employees whose duty changes or who quit their job in this field.
- We use up-to-date anti-virus systems.
- We use firewalls.
- We ensure the security of environments containing personal data.
- We back-up personal data and ensure the security of the backed up personal data.
- We implement and follow-up the user account management and authorization control system.
- We have identified current risks and threats.
- If sensitive personal data is to be delivered by e-mail, we deliver them in encrypted form and using a KEP or corporate mail account.
- We utilize intrusion detection and prevention systems.
- We have taken cyber security measures and constantly monitor their implementation.
- We implement encryption.
- We utilize data loss prevention software.

- **Administrative Measures**

- We possess disciplinary regulations including data security provisions for employees.
- We periodically carry out training and awareness activities on data security for employees.
- We perform confidentiality commitments.
- The signed agreements contain data security provisions.
- We take additional security measures for personal data transferred via paper and deliver the relevant document in a confidential document format.
- We take necessary security measures regarding entry and exit to physical environments containing personal data.
- We ensure the security of physical environments containing personal data against external risks (fire, flood, etc.).
- We reduce personal data as much as possible.
- We conduct in-house periodic and/or random audits.
- Data processing service providers are periodically audited on data security.
- Data processing service providers are periodically audited on data security awareness.
-

7. Transfer of Personal Data

a. Domestic Transfer

Our company transfers personal data to third parties based on the data processing conditions stipulated in the PDPL, Articles 5 and 6. The Company takes all necessary security measures in data transfer activities. In this context, the recipients to which our Company transfers data are as follows:

- **Suppliers,** for the purposes of execution of Training Activities, Execution of Talent/Career Development Activities, Execution of Goods/Services Procurement Processes, Execution of Communication Activities, Execution of Benefits and Vested Benefits Processes for Employees, Planning of Human Resources Processes, Execution of Finance and Accounting Affairs , Execution/Supervision of Business Activities, Organization and Event Management;
- **Authorized Institutions and Organizations,** for the purposes of Fulfillment of Employment and Legislation Obligations for Employees, Planning of Human Resources Processes, Execution/Supervision of Business Activities, Providing Information to Authorized Persons, Institutions and Organizations,

- **Associations**, for the purposes of Execution/Inspection of Business Activities, Execution of Goods/Services Post-Sales Support Services, Execution of Logistics Activities, Ensuring the Security of Movable Goods and Resources.

b. International Transfer

The company shall transfer data abroad by providing one of the following conditions stipulated in the PDPL, Article 9.

- The explicit consent of the data owner,
- The country to which personal data will be transferred has the status of "safe country" and ensures adequate protection,
- The rights and obligations of the Company and the receiving party regarding data transfer are regulated to ensure protection, and the Board has authorization to do so.

In this context, the recipients to which our Company transfers data are as follows:

- **Suppliers**, Execution of Activities for Customer Satisfaction, Receiving and Evaluation of Suggestions for Improvement of Business Processes, Follow-up of Requests/Complaints, Execution of Customer Relationship Management Processes, Execution of Company/Product/Services Loyalty Processes

8. Personal Data Inventory

The Company has created a data inventory with the details stipulated by the Law regarding the personal data processed within the scope of PDPL. The Company's data inventory includes the following details:

- Business processes where personal data are used,
- Category of personal data,
- Processed personal data,
- Processed sensitive personal data,
- Purpose and legal reason of processing data,
- Domestic recipients of personal data,
- Whether personal data is transferred abroad,
- Personal data retention periods

In case of a change in the processing activities, the Personal Data Inventory shall be updated. The Company notifies the Data Controller Registry of the information and updates, if any, contained in the Personal Data Inventory. The information that the Company will provide to the data owner under the disclosure requirement mentioned in this Policy, Article 5, are consistent with the information disclosed in the Registry.

9. Roles and Responsibilities

The roles and responsibilities of our company for the processing of personal data are as follows:

- The relevant department is responsible for informing the data owners, such as customers, subcontractors, suppliers, whose data is processed, about this Policy.
- The relevant department is responsible for informing the parties, which process data on behalf

of the Company, such as employees and suppliers, about the Policy, and for performing regular controls and ensuring the implementation of the Policy by the data processors.

- The relevant department is responsible for updating this Policy. The relevant department shall make the necessary improvements by considering the needs of the company's information processing systems, and carry out the policy updating processes, when required.
- The relevant department is authorized to approve the updates to this Policy.
- In case of violation of the Policy, the relevant department is responsible for the determination and implementation of sanctions.

10. Deletion, Destruction and Anonymization of Personal Data

- In case the legal grounds requiring data processing are eliminated, the personal data shall be deleted, destroyed or anonymized upon the decision of the Company, for periodic control and/or upon the request of the data owner, in accordance with the PDPL, Article 7 and the provisions of other relevant legislation.
- The company shall not keep personal data longer than necessary in association with the reason for obtaining the personal data. The Company shall delete, destroy or anonymize personal data in the first periodical destruction process following the date on which the obligation to delete, destroy or anonymize personal data emerges.
- The Company has prepared a *Retention and Destruction Policy* in order to determine the relevant procedures and principles. This Retention and Destruction Policy stipulates the criteria to be used in the retention and destruction periods, including the retention period for each category of personal data and the legal obligations of the Company to retain the data. This Retention and Destruction Policy has been prepared in accordance with the Personal Data Inventory specified in this Policy, Article 8.
- In the deletion, destruction and anonymization of personal data, the Company shall comply with the principles stipulated in this Policy, Section 4/a, the technical and administrative measures stipulated in Article 6, the Retention and Destruction Policy and the relevant legislation provisions and Board decisions.
- The personal data shall be destroyed safely in accordance with the provisions of the PDPL, the relevant legislation and the *Retention and Destruction Policy* of the Company. The company shall choose the appropriate method upon the request of the data owner, and explain its reason.

11. Rights of Data Owner and Execution of Rights

a. Rights of Data Owner

The Data Owners have the following rights regarding their processed personal data in accordance with the PDPL, Article 11:

- To learn whether your personal data is processed or not,
- If personal data has been processed, to request information as to personal and learn to whom it has been disclosed,
- To learn the purpose of processing and whether the data is used in accordance with its purpose,
- To learn the third parties to whom personal data are transferred in the country or abroad and to

request the notification of the transaction made in this direction to the third parties,

- To request rectification if the data have been processed incompletely or inaccurately, and to request the notification of this to the third parties,
- To request the deletion or destruction of personal data upon the annulment of processing purposes, although it has been processed in accordance with the provisions of the relevant law,
- To object to the emergence of any consequence against the herself/himself,
- To request compensation for the damages due to unlawful processing of personal data.

b. Execution of Rights

You may submit your applications and requests regarding your personal data to the Company using the Data Owner Application Form,

1. By sending them to the address of Emniyet Evleri Mah. Eski Büyükdere Cad. Sapphire Plaza No:1/4 Kat:19 Daire:1 34415 Kağıthane/Istanbul along with your wet signature and a copy of your identity card,
2. By signing with secure electronic signature or mobile signature and sending it to the Company's PDPL mail address (ik@kimpur.com) or,
3. By sending them to the address of kimtekspu@hs01.kep.tr by signing with a secure electronic signature or mobile signature, via registered electronic mail (KEP),
4. By applying personally to Kimteks Poliüretan San. Ve Tic. A.Ş with a valid identity document.

.

In your application, you must include your name, surname, signature, your ID number (Turkish Citizens), nationality (Foreign Citizens), passport (or ID if applicable) number, residential area and business address, e-mail address, fax number, if any, and finally the subject of the request in accordance with the legal obligations regarding the procedures and principles of application to the data controller. In addition, you must include documents confirming the identity and information and documents related to the subject of your request with your application.

You must clearly state which of your rights you want to exercise in your request and the details of the transactions you request.

The subject of the request shall be related to the data owner. In case of an application on behalf of someone else, the requester must rely on a specially documented authorization (power of attorney) for the requested transaction. Unauthorized applications shall not be considered.

c. Evaluation of Application

We shall evaluate your applications and get back to you as soon as possible and at the latest

within 30 days from the date of receipt of your application.

If required, additional information and documents may be requested during the evaluation process. In cases where it complies with the relevant legislation, a fee may be charged for fulfilling the request.

The Company shall take all necessary administrative and technical measures to conclude the applications to be made by the data owner, in accordance with the law and the rule of good faith.

d. Rejection of Application

The application shall be rejected;

- If the application is not made in accordance with the above-mentioned procedures,
- If the application contains a request contrary to the current legislation,
- If the application is not based on a legitimate cause or is considered as an abuse of right,
- If the personal data subject to the application are processed for purposes such as research, planning and statistics to be anonymized with official statistics,
- If the personal data are made public by the data owner.
- In the presence of one of the other conditions stipulated in the PDPL, Article 28.

. In case that the application is rejected, the Company shall notifiy the data owner of the rejection and the reason for rejection.

e. Right to Complaint

The data owner has the right to complain to the Board when the application is rejected or

if the answer given by the Company is insufficient or the Company does not respond within 30 days.

.

The owner may exercise his/her right to complain within 30 days from the date of the Company's response and in any case within 60 days from the date of application

.

12. Publication and Enforcement of the Policy

This Policy enters into force on 30.07.2021.
The current version of this Policy shall be published in the company documentation system.

13. Policy Update

This Policy shall be updated in accordance with the quality document procedure within the legal period stipulated in the legislation.
The repealed old copies of this Policy shall be withdrawn with the approval of the data controller and shall be kept by the archive officer during the legal process stipulated in the legislation. Policies with retention period expired shall be destroyed by our relevant unit officer and issue a report about it.