



PERSONAL DATA PROCESSING AND PROTECTION POLICY

1. PURPOSE

This Personal Data Processing and Protection Policy ("**Policy**") has been prepared for the purpose of determining the procedures and principles regarding the processing of personal data and special categories of personal data as set forth in Articles 5 and 6 of the Personal Data Protection Law No. 6698 ("**Law**")

The protection of personal data is among the top priorities of SASA Polyester Sanayi Anonim Şirketi ("**Company**"), and the Company makes every effort to act in compliance with all applicable legislation in this regard. Within the framework of this Policy, the principles adopted in the conduct of personal data processing activities by the Company and the fundamental principles adopted to ensure compliance of the Company's data processing activities with the regulations set forth in the Law are explained, thereby ensuring the necessary transparency by informing personal data subjects. With full awareness of our responsibility in this context, your personal data is processed and protected within the scope of this Policy.

Within this scope, the personal and/or special categories of personal data of all real persons whose personal and/or special categories of personal data are held by the Company for any reason—including employee candidates, exam candidates, interns, employees, customers, shareholders/company partners, supplier employees and representatives, visitors, subcontractor employees, website visitors, consultants, and potential product/service buyers—are managed within the framework of this Policy. As part of its legal responsibility, the Company implements the processes of protecting, processing, and destroying personal data in accordance with the Law and the applicable legislation.

The protection of personal data and the safeguarding of the fundamental rights and freedoms of individuals whose personal data is collected constitute the core principle of our personal data processing policy. For this reason, we conduct all our activities involving the processing of personal data by respecting the protection of privacy, the confidentiality of communications, freedom of thought and belief, and the right to effective legal remedies. We take all necessary administrative and technical measures, in accordance with legislation and current technology, as required by the nature of the relevant data, to ensure the protection of personal data.

2. SCOPE

The personal and/or special categories of personal data belonging to company employee candidates, exam candidates, interns, employees, customers, shareholders/company partners, supplier employees and representatives, visitors, subcontractor employees, website visitors, consultants, potential product/service buyers, or any other individuals are covered by this Policy. This Policy applies to all records and environments in which personal and/or special categories of personal data obtained or managed by the Company are processed, as well as to all activities related to the processing of personal data by the Company.



This Policy applies to all personal data that is processed, either fully or partially by automated means, or by non-automated means provided that it is part of any data recording system

3. IMPLEMENTATION OF THE POLICY AND RELEVANT LEGISLATION

The relevant legal regulations in force regarding the processing and protection of personal data shall primarily apply. In the event of any inconsistency between the applicable legislation and the Policy, the Company acknowledges that the provisions of the applicable legislation shall prevail. The Policy concretizes and regulates the rules set forth by the relevant legislation within the scope of the Company's practices.

4. DEFINITIONS

In this Policy;

Explicit consent: Consent that is based on information provided regarding a specific subject and is declared with free will.

Network: The structure in which multiple computers are connected to each other for various reasons such as information sharing, software and hardware sharing, and ease of centralized management and support.,

Recipient group: The category of natural or legal persons to whom personal data is transferred by the data controller,

Anonymization of Personal Data: Making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data

Information Security: Preventing unauthorized or unauthorized access, use, modification, disclosure, removal, alteration and damage to information,

Data subject: The natural person whose personal data is processed,

Destruction: Deletion, destruction or anonymization of personal data,

Law: The Law on the Protection of Personal Data No. 6698 dated 24 March 2016

Board: The Personal Data Protection Board,

Authority: The Personal Data Protection Authority

Recording medium: Any medium containing personal data that is fully or partially automated or processed by non-automated means, provided that it is part of any data recording system,



Personal data: Any information relating to an identified or identifiable natural person,

Personal Data Retention and Destruction Policy: The policy on which data controllers base the process of determining the maximum period of time required for the purpose for which personal data are processed and the process of deletion, destruction and anonymization,

Processing of Personal Data: Any operation performed on personal data such as obtaining, recording, storing, retaining, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system,

Deletion of Personal Data: Making personal data inaccessible and non-reusable in any way for the relevant users,,

Destruction of Personal Data: The process of making personal data inaccessible, unrecoverable and unusable by anyone in any way,

Special Categories of Personal Data: Data relating to an individual's race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data

Policy : This Personal Data Processing and Protection Policy,

Data Recording System: The recording system in which personal data are structured and processed according to certain criteria,

Data Processor: The person who processes personal data within the organization of the data controller or in accordance with the authority and instructions received from the data controller, excluding the person or unit responsible solely for the technical retention, protection, and backup of the data

Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system,

refers to.

5. PRINCIPLES TO BE FOLLOWED IN THE PROCESSING OF PERSONAL DATA

Personal data may be processed in accordance with the procedures and principles stipulated in Article 4 of the Law titled "General Principles" and other laws, and processing activities are



carried out by the Company in accordance with the Law and other legislation. These principles are;

- Compliance with the law and good faith,
- Being accurate and up to date when necessary,
- Processing for specific, explicit and legitimate purposes,
- Being relevant, limited and proportionate to the purpose for which they are processed,
- Retention for the period stipulated in the relevant legislation or required for the purpose for which they are processed

in the form of.

6. PERSONAL DATA

Personal data is defined in Article 3/1-d of the Law as any information relating to an identified or identifiable natural person. The protection of personal data applies only to real persons; information belonging to legal entities that does not contain data relating to real person is excluded from personal data protection. Therefore, this Policy does not apply to data belonging to legal entities. This Policy applies both to data that directly identifies a person, such as the person's name, surname, or Turkish ID number, and to data through which the data subject can be identified indirectly.

7. PURPOSES OF PROCESSING PERSONAL DATA

Based on and limited to at least one of the personal data processing conditions specified in Article 5 of the Law, and primarily in accordance with the principles set forth in Article 4 regarding the processing of personal data, as well as the general principles specified in the Law, personal data is processed by the Company. The Company processes this data in line with the personal data processing purposes announced by the Board, and these purposes are as follows;

- Executing Emergency Management Processes
- Execution of Information Security Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
Execution of Employee Candidate Application Processes
- Execution of Employee Satisfaction and Loyalty Processes Execution of Employee Candidate Application Processes
- Fulfillment of Employment Contract and Regulatory Obligations for Employees
- Execution of Employee Benefits and Benefits Processes
- Conducting Audit / Ethics Activities
- Conducting Training Activities
- Execution of Access Authorizations
- Execution of Activities in Compliance with the Legislation - Execution of Access Authorizations
- Execution of Finance and Accounting Affairs



- Ensuring Physical Space Security
- Execution of Assignment Processes
- Monitoring and Execution of Legal Affairs
- Conducting Internal Audit / Investigation / Intelligence Activities
- Execution of Communication Activities
- Planning Human Resources Processes
- Execution / Supervision of Business Activities
- Execution of Occupational Health / Safety Activities
- Receiving and Evaluating Suggestions for Improvement of Business Processes
- Execution of Business Continuity Ensuring Activities
- Execution of Logistics Activities
- Execution of Goods / Service Procurement Processes
- Execution of Goods / Services After Sales Support Services
- Execution of Goods / Service Sales Processes
- Execution of Goods / Services Production and Operation Processes
- Execution of Customer Relationship Management Processes
- Execution of Activities for Customer Satisfaction
- Organization and Event Management
- Conducting Marketing Analysis Studies
- Execution of Performance Evaluation Processes
- Execution of Advertising / Campaign / Promotion Processes
- Execution of Risk Management Processes
- Execution of Storage and Archive Activities
- Implementation of Social Responsibility and Civil Society Activities
- Execution of Contract Processes
- Execution of Sponsorship Activities
- Execution of Strategic Planning Activities
- Tracking Requests / Complaints
- Ensuring the Security of Movable Property Rights and Resources
- Execution of Supply Chain Management Processes
- Execution of Wage Policy
- Execution of Marketing Processes of Products / Services
- Ensuring the Security of Data Controller Operations
- Foreign Personnel Work and Residence Permit Procedures
- Execution of Investment Processes
- Execution of Talent / Career Development Activities
- Providing Information to Authorized Persons, Institutions and Organizations
- Execution of Management Activities

Creating and Tracking Visitor Records

is in the form of

8. TRANSFER OF PERSONAL DATA



Personal data are collected by the Company in accordance with Article 8 of the Law without obtaining explicit consent in the presence of one of the conditions specified in Article 5/2 of the Law, and otherwise by obtaining the explicit consent of the data subject;

- Natural persons or private legal entities,
- Associates and subsidiaries,
- Suppliers,
- Group Companies,
- Authorized Public Institutions and Organizations

is being transferred.

9. CROSS-BORDER TRANSFER OF PERSONAL DATA

The Company may transfer personal data abroad within the scope of Article 9 of the Law if one of the following conditions is present:

- The existence of one of the data processing conditions specified in the Law and the presence of an adequacy decision regarding the country, sectors within the country, or international organizations to which the transfer will be made.
- If there is no adequacy decision, personal data may be transferred abroad provided that one of the processing conditions specified in the Law exists, and that the data subject has the opportunity to exercise their rights and to seek effective legal remedies in the country to which the data will be transferred, and provided that one of the following appropriate safeguards is in place: (i) The existence of an agreement, which is not an international treaty, between public institutions and organizations or international organizations abroad and public institutions and organizations or professional organizations with public institution status in Turkey, and the Board's permission for the transfer, (ii) The existence of binding corporate rules, containing provisions on the protection of personal data, which companies within a group of undertakings engaged in joint economic activity are obliged to comply with and which are approved by the Board, (iii) The existence of a standard contract announced by the Board, which includes matters such as data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures to be taken by the data recipient, and additional measures for special categories of personal data, (iv) The existence of a written undertaking containing provisions ensuring adequate protection and the Board's permission for the transfer.
- In the absence of an adequacy decision and if none of the appropriate safeguards stipulated in the Law can be provided, data controllers and data processors may transfer personal data abroad only on an occasional basis and only if one of the following conditions exists: (i) The data subject gives explicit consent to the transfer, provided that they are informed about the possible risks, (ii) The transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken at the request of the data subject, (iii) The transfer is necessary for the conclusion or



performance of a contract to be made in the interest of the data subject between the data controller and another real or legal person (iv) The transfer is necessary for an overriding public interest, (v) The transfer of personal data is necessary for the establishment, exercise, or protection of a right, (vi) The transfer of personal data is necessary for the protection of the life or physical integrity of the data subject or another person who is unable to express their consent due to actual impossibility or whose consent is not legally valid, (vii) The transfer is made from a register that is open to the public or to persons with a legitimate interest, provided that the conditions for accessing the register as prescribed by the relevant legislation are met and the person with a legitimate interest requests the data

10. SPECIAL CATEGORIES OF PERSONAL DATA

The Company acts with particular sensitivity in the processing and protection of special categories of personal data, which are determined as “special” by the Law and processed lawfully, and which, if learned, may cause discrimination against the data subject. In this context, the technical and administrative measures taken by the Company for the protection of personal data are meticulously applied with regard to special categories of personal data, and necessary audits are ensured within the Company.

According to Article 6 of the Law, special categories of personal data are defined as data relating to a person’s race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data.

11. PURPOSES OF PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

Based on at least one of the personal data processing conditions specified in Article 6 of the Law and in a limited manner, the Company processes special categories of personal data in accordance with the general principles set forth in the Law, particularly the principles specified in Article 4 regarding the processing of personal data. The Company processes these data in line with the purposes of personal data processing announced by the Board, and these purposes are as follows;

- Execution of Emergency Management Processes
- Execution of Information Security Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes - Execution of Information Security Processes
- Execution of Employee Candidate Application Processes
- Fulfillment of Obligations Arising from Employment Contract and Legislation for Employee- Execution of Application Processes of Employee Candidates
- Conducting Audit / Ethics Activities
- Conducting Training Activities
- Execution of Activities in Accordance with the Legislation - Execution of Training Activities



- Monitoring and Execution of Legal Affairs
- Conducting Internal Audit / Investigation / Intelligence Activities
- Planning Human Resources Processes
- Execution / Supervision of Business Activities
- Execution of Occupational Health / Safety Activities
- Execution of Contract Processes
- Tracking Requests / Complaints
- Ensuring the Security of Data Controller Operations
- Foreign Personnel Work and Residence Permit Procedures
- Providing Information to Authorized Persons, Institutions and Organizations

is in the form.

12. TRANSFER OF SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data may be processed by the Company, provided that adequate measures are taken, in the presence of one of the conditions specified in Article 6/3 of the Law, pursuant to Article 8 of the Law.

- Natural persons or private legal entities,
- Associates and subsidiaries,
- Suppliers,
- Group Companies,
- Authorized Public Institutions and Organizations - Community Companies,

is being transferred.

13. CROSS-BORDER TRANSFER OF SPECIAL CATEGORIES OF PERSONAL DATA

The Company cross-border transfers of personal data within the scope of Article 9 of the Law, provided that one of the conditions set forth below is met:

- The existence of one of the processing conditions specified in the Law and the existence of an adequacy decision on the country, sectors within the country or international organizations to which the transfer will be made.
- If there is no adequacy decision, personal data may be transferred abroad provided that one of the processing conditions specified in the Law exists, and that the data subject has the opportunity to exercise their rights and access effective legal remedies in the country to which the data is transferred, and provided that one of the following appropriate safeguards is in place:
 - (i) The existence of an agreement, which does not qualify as an international convention,



between public institutions and organizations or professional organizations with public institution status in Türkiye and public institutions, organizations, or international organizations abroad, and the transfer is approved by the Board. (ii) The existence of binding corporate rules, containing provisions on personal data protection, which companies within a group of undertakings engaged in joint economic activity are obliged to comply with, and which are approved by the Board. (iii) The existence of a standard contract announced by the Board, which includes matters such as data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures to be taken by the data recipient, and additional measures for special categories of personal data. (iv) The existence of a written undertaking containing provisions ensuring adequate protection, and the transfer is approved by the Board.

- In the absence of an adequacy decision and where none of the appropriate safeguards stipulated in the Law can be provided, data controllers and data processors may transfer personal data abroad only on an occasional basis and only if one of the following conditions exists: (i) The data subject has given explicit consent to the transfer, having been informed of the possible risks, (ii) The transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken at the request of the data subject, (iii) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person, (iv) The transfer is necessary for reasons of overriding public interest, (v) The transfer of personal data is necessary for the establishment, exercise, or protection of a right, (vi) The transfer is necessary for the protection of the life or physical integrity of the data subject or another person, who is physically or legally incapable of giving consent, (vii) The transfer is made from a register that is open to the public or to persons with a legitimate interest, provided that the conditions for accessing the register as prescribed by law are met and the person with a legitimate interest requests the data.

14. RECORDING MEDIA

As the Data Controller, the Company stores the personal and/or special categories of personal data it processes—whether wholly or partially by automated means, or by non-automated means provided that they form part of a data recording system—in compliance with the law, in the environments specified in the table below.

ELECTRONIC MEDIA	NON-ELECTRONIC MEDIA
------------------	----------------------



• Physical and Virtual Servers • Software (...) • Information Security Devices • Data Controller Computer Internal Disk • Mobile Devices • External Memory (USB, External Hard disk, etc.) • Magnetic Tape	• Printed Document / Copy / Document • Office Space • Common Archive
--	--

15. MEASURES TAKEN BY THE COMPANY TO PREVENT UNLAWFUL PROCESSING OF PERSONAL DATA

In order to prevent and protect the unlawful processing of personal data, certain technical and administrative measures are taken by the Company as the Data Controller.

15.1. Technical Measures

- Network security and application security are ensured.
- Closed system network is used for personal data transfers through the network - Network security and application security are ensured.
- Key management is in place.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- The security of personal data stored in the cloud is ensured.
- Authorization matrix has been created for employees.
- Access logs are kept regularly.
- Employees who are reassigned or leave their jobs are de-authorized in this area.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- Personal data security issues are reported quickly.
- Personal data security is monitored.
- Necessary security measures are taken regarding entry and exit to physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (fire, flood, etc.).
- Security of environments containing personal data is ensured.
- Personal data is minimized as much as possible.
- Personal data is backed up and the security of backed up personal data is also ensured.



- User account management and authorization control system are implemented and monitored.
- Log records are kept without user intervention.
- If sensitive personal data is to be sent via electronic mail, it is sent encrypted and using a KEP or corporate mail account.
- Intrusion detection and prevention systems are used.
- Penetration test is applied.
- Encryption is performed.
- Data loss prevention software is used.

15.2 Administrative Measures

- There are disciplinary regulations for employees that include data security provisions.
- Training and awareness raising activities on data security are carried out for employees at regular intervals.
- Corporate policies on access, information security, use, storage and disposal are prepared and implemented.
- Confidentiality commitments are made.
- The signed contracts contain data security provisions.
- Personal data security policies and procedures have been determined.
- Internal periodic and/or random audits are conducted and commissioned.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- Data processing service providers are periodically audited on data security.
- Awareness of data processing service providers on data security is ensured.

16. REASONS FOR RETENTION AND DESTRUCTION OF PERSONAL DATA

Personal data and/or special categories of personal data belonging to all real persons whose personal and/or special categories of personal data are held by the Company for any reason—including employee candidates, exam candidates, interns, employees, customers, shareholders/company partners, supplier employees and officials, visitors, subcontractor employees, website visitors, consultants, potential product/service buyers—are stored and destroyed in accordance with the Law. Within the scope of the Company's activities, personal data are retained for the period stipulated in the relevant legislation or for the duration required for the purposes of processing.

In this context, detailed explanations regarding retention and destruction are also addressed in the Personal Data Retention and Destruction Policy, and for matters not regulated in this Policy, the provisions of the Personal Data Retention and Destruction Policy shall apply.



17. RIGHTS OF THE DATA SUBJECT

As the Data Controller, during our activities, data subjects whose personal and/or special categories of personal data are obtained may apply to us in accordance with the procedures set forth in the Law and the Communiqué on the Procedures and Principles of Application to the Data Controller, published in the Official Gazette on March 10, 2018, by the Personal Data Protection Board. They may exercise their rights under Article 11 of the Law, which include:

- Learning whether their personal data is being processed,
- Requesting information if their personal data has been processed,
- Learning the purpose of processing personal data and whether it is used for its intended purpose,
- Knowing the third parties to whom personal data is transferred domestically or abroad,
- Requesting correction of personal data in case of incomplete or incorrect processing,
- Requesting the deletion or destruction of personal data under the conditions stipulated in Article 7,
- Requesting notification of correction, deletion, or destruction of personal data to third parties to whom the data is transferred,
- Objecting to a result arising against them by analyzing the processed data exclusively through automated systems,
- Demanding compensation for damages in case of unlawful processing of personal data.

18. PUBLICATION AND RETENTION OF THE POLICY ON PROCESSING AND PROTECTION OF PERSONAL DATA

This Policy is published and stored in electronic format.

19. PERIOD FOR UPDATING THE POLICY

This Policy shall be reviewed at least annually and updated if deemed necessary.

The Board of Directors commits to fulfilling the requirements specified in this policy and expects the same commitments from SASA employees.