SASA

Our Personal Data Retention and Destruction Policy

ERDEMOĞLU HOLDİNG

Personal Data Retention and Destruction Policy

1. INTRODUCTION

1.1 Purpose

The Personal Data Retention and Destruction Policy ("Policy") has been prepared by SASA Polyester Sanayi Anonim Şirketi ("Company") in order to determine the procedures and principles governing the retention and destruction activities carried out by the Company.

In line with its determined mission, vision and core principles, the Company has prioritized ensuring that personal data belonging to all natural persons — including job applicants, employees, interns, examination candidates, customers, shareholders/partners, business partners, supplier employees and representatives, visitors, third-party employees, website visitors, consultants, potential buyers of products/services, or any other individuals whose personal and/or special categories of personal data are processed by the Company — are processed in compliance with the Constitution of the Republic of Türkiye, international conventions, the Law No. 6698 on the Protection of Personal Data ("Law"), and other applicable legislation, and that data subjects can effectively exercise their rights.

All activities and procedures relating to the retention and destruction of personal data are carried out in accordance with this Policy prepared by the Company.

1.2 Scope

This Policy covers the personal data of all natural persons whose personal and/or special categories of personal data are processed by the Company, including job applicants, employees, interns, examination candidates, customers, shareholders/partners, business partners, supplier employees and representatives, visitors, third-party employees, website visitors, consultants, and potential product/service recipients. This Policy applies to all recording media in which personal data owned or managed by the Company are processed and to all personal data processing activities.

1.3 Abbreviations and Definitions

Recipient Group	The category of natural or legal persons to whom personal data are transferred by the data controller.
Explicit Consent	Consent that is freely given, specific, and based on adequate information.
Anonymization	Rendering personal data incapable of being associated with an identified or identifiable natural person, even when matched with other data.
Employee	Company personnel.
Electronic Media	Media in which personal data can be created, read, modified, and written using electronic devices.
Non-Electronic Media	All written, printed, visual, and other media outside electronic environments.
Service Provider	A natural or legal person providing services to the Company within the scope of a specific contract.
Data Subject	The natural person whose personal data are processed.
Relevant User	Persons who process personal data within the data controller's organization or based on authorization and instructions received from the data controller, excluding those responsible for technical storage, protection, and backup of

	data.
Destruction	Deletion, destruction, or anonymization of personal data.
Law	Law No. 6698 on the Protection of Personal Data.
Recording Media	Any environment in which personal data processed fully or partially by automatic means or by non-automatic means as part of a data recording system are stored.
Personal Data	Any information relating to an identified or identifiable natural person.
Personal Data Processing Inventory	An inventory created by data controllers by associating personal data processing activities with purposes of processing, data categories, recipient groups, and data subject groups, detailing maximum retention periods, cross-border data transfers, and data security measures.
Processing of Personal Data	Any operation performed on personal data such as collection, recording, storage, retention, modification, reorganization, disclosure, transfer, acquisition, making available, classification, or preventing use.
Board	Personal Data Protection Board.
Special Categories of Personal Data	Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.
Periodic Destruction	The deletion, destruction, or anonymization of personal data carried out ex officio at recurring intervals specified in the personal data retention and destruction policy when all conditions for processing personal data under the Law cease to exist.
Policy	Personal Data Retention and Destruction Policy.
Data Recording System	A system in which personal data are structured and processed according to specific criteria.
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.
VERBIS (Data Controllers' Registry Information System)	The information system established and managed by the Authority, accessible online, used by data controllers for registry applications and related transactions.
Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28 October 2017.
Recipient Group	The category of natural or legal persons to whom personal data are transferred by the data controller.
Data Processor	A natural or legal person who processes personal data on behalf of the data controller based on the authority granted.

2. Allocation of Responsibilities and Duties

All Company units and employees actively support the responsible units in ensuring the proper implementation of technical and administrative measures adopted under this Policy, training and raising awareness among unit employees, monitoring and continuous auditing, preventing unlawful processing and access to personal data, and ensuring lawful retention of personal data by implementing appropriate technical and administrative measures in all environments where personal data are processed.

The distribution of titles, departments, and duties of those involved in retention and destruction processes is provided in Table 1.

TITLE	DEPARTMENT	DUTY
Manager of Protection, Security and Administrative Affairs	Protection, Security and Administrative Affairs	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Manager of Management Systems and Performance Management	Management Systems and Performance Management	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of Sales and Marketing	Sales and Marketing	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of Supply Chain	Supply Chain	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Workplace Physician	Occupational Health Unit	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of Filament Strategic Business Unit	Filament SBU	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of PTA Strategic Business Unit	PTA SBU	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of Fiber Strategic Business Unit	Fiber SBU	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of Polymers and Chemicals Strategic Business Unit	Polymers and Chemicals SBU	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Manager of Machinery, Energy and Technology	Machinery, Energy and Technology	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.

Deputy General Manager of Refinery	Refinery	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Manager of Sustainability, Environment and OHS	Sustainability, Environment and OHS	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Manager of Protection, Security and Administrative Affairs	Protection, Security and Administrative Affairs	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Manager of Management Systems and Performance Management	Management Systems and Performance Management	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Deputy General Manager of Sales and Marketing	Sales and Marketing	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.
Manager of Quality and Technical Services	Quality and Technical Services	Ensuring the lawful processing, retention, protection, and destruction of personal data; implementing the technical and administrative measures falling within the scope of the relevant unit's responsibility; and ensuring compliance with the Policy.

Table 1: Distribution of Roles and Responsibilities for Data Retention and Destruction Processes.

3. Recording Media

Personal data are securely retained by the Company in compliance with the law in the environments listed in Table 2.

ELECTRONIC DATA STORAGE MEDIA	NON- ELECTRONIC DATA STORAGE MEDIA
Physical and virtual servers Software Information security devices Internal hard disks of data controller computers Mobile devices External storage devices (USB, external hard disks, etc.) Magnetic tapes	Printed documents / copies / records Office premises Central archives

Table 2: Roles and Responsibilities in Data Retention and Destruction Processes

4. Explanations Regarding Retention and Destruction

Personal data belonging to all natural persons whose personal and/or special categories of personal data are processed by the Company are retained and destroyed in compliance with the Law.

4.1 Explanations Regarding Retention

Articles 3, 4, 5, and 6 of the Law define the processing of personal data, stipulate that personal data must be processed for specific, explicit, and legitimate purposes, be limited and proportionate, and be retained only for the period required by relevant legislation or the purpose of processing.

Accordingly, personal data are retained for the period stipulated in applicable legislation or necessary for processing purposes.

4.1.1 Legal Grounds Requiring Retention

Personal data processed within the scope of Company activities are retained for the periods stipulated under applicable legislation, including but not limited to;

- Law No. 6698 on the Protection of Personal Data
- Law No. 5510 on Social Insurance and General Health Insurance
- Law No. 5651 on the Regulation of Publications on the Internet
- Law No. 5018 on Public Financial Management and Control
- Law No. 6331 on Occupational Health and Safety
- Law No. 4982 on the Right to Information
- Law No. 3071 on the Exercise of the Right to Petition
- Law No. 4857 on Labor Law
- Law No. 2547 on Higher Education
- Law No. 5434 on the Pension Fund of the Republic of Türkiye
- Law No. 2828 on Social Services
- Regulation on Health and Safety Measures in Workplace Buildings and Annexes
- Regulation on Archival Services

4.1.2 Processing Purposes Requiring Retention

The Company retains the personal data it processes within the scope of its activities for the purposes set forth below:

- Conducting Emergency Management Processes,
- Conducting Information Security Processes,
- Conducting the Selection and Placement Processes for Job Applicants / Interns / Students,
- Conducting Job Applicants' Application Processes,
- Conducting Employee Satisfaction and Engagement Processes,
- Fulfilling Obligations Arising from Employment Contracts and Applicable Legislation for Employees,
- Conducting Processes Relating to Employees' Fringe Benefits and Entitlements,
- Conducting Audit and Ethics Activities,
- Conducting Training and Development Activities,
- Managing Access Authorization Processes,

- Ensuring the Conduct of Activities in Compliance with Applicable Legislation,
- Conducting Finance and Accounting Operations,
- Ensuring Physical Premises Security,
- Conducting Assignment and Delegation Processes,
- Monitoring and Conducting Legal Affairs,
- Conducting Internal Audit, Investigation, and Intelligence Activities,
- Conducting Communication Activities,
- Planning Human Resources Processes,
- Conducting and Auditing Business Operations,
- Conducting Occupational Health and Safety Activities,
- Receiving and Evaluating Suggestions for the Improvement of Business Processes,
- Conducting Business Continuity Management Activities,
- Conducting Logistics Operations,
- Conducting Goods and Services Procurement Processes,
- Conducting After-Sales Support Services for Goods and Services,
- Conducting Goods and Services Sales Processes,
- Conducting Goods and Services Production and Operational Processes,
- Conducting Customer Relationship Management Processes,
- Conducting Activities Aimed at Ensuring Customer Satisfaction,
- Conducting Organization and Event Management Activities,
- Conducting Marketing Analysis Activities,
- Conducting Performance Evaluation Processes,
- Conducting Advertising, Campaign, and Promotion Processes,
- Conducting Risk Management Processes,
- Conducting Retention and Archiving Activities,
- Conducting Corporate Social Responsibility and Civil Society Activities,
- Conducting Contract Management Processes,
- Conducting Sponsorship Activities,
- Conducting Strategic Planning Activities,
- Monitoring and Handling Requests and Complaints,
- Ensuring the Security of Movable Assets and Resources,
- Conducting Supply Chain Management Processes,
- Conducting Remuneration and Wage Policy Processes,
- Conducting Marketing Processes for Products and Services,
- Ensuring the Security of Data Controller Operations,
- Conducting Work Permit and Employment Procedures for Foreign Personnel,
- Conducting Investment Processes,
- Conducting Talent Management and Career Development Activities,
- Providing Information to Authorized Natural Persons, Public Institutions, and Organizations,
- Conducting Corporate Governance and Management Activities,
- Creating and Monitoring Visitor Records.

4.2 Circumstances Requiring Destruction

Personal data shall be deleted, destroyed, or anonymized by the Company ex officio or upon request where;

- The relevant legislation is amended or repealed,
- The purpose requiring processing or retention ceases to exist,
- Explicit consent is withdrawn where processing is based solely on consent,
- The data subject's request for deletion or destruction is accepted,

- The Board approves the data subject's complaint, or
- The maximum retention period has expired with no legitimate grounds for further retention.

5. Technical and Administrative Measures

The Company adopts all necessary technical and administrative measures pursuant to Articles 12 and 6 of the Law to ensure data security and lawful destruction.

5.1 Technical Measures

The technical measures implemented by the Company regarding the personal data it processes are as follows.

- Network security and application security are ensured.
- Closed-system networks are used for the transmission of personal data over networks.
- Key management is applied.
- Security measures are implemented in the procurement, development, and maintenance of information technology systems.
- The security of personal data stored in the cloud is ensured.
- Access logs are maintained regularly.
- Up-to-date antivirus systems are used.
- Firewalls are employed.
- Necessary security measures are taken regarding access to physical environments containing personal data.
- Physical environments containing personal data are protected against external risks (such as fire, flood, etc.).
- The security of environments containing personal data is ensured.
- Personal data are backed up, and the security of backed-up personal data is ensured.
- User account management and authorization control systems are implemented, and monitoring of these systems is conducted.
- Log records are maintained in a manner that prevents user interference.
- If special categories of personal data are to be sent via email, they are always encrypted and sent using either a Registered Electronic Mail (KEP) or a corporate email account.
- Intrusion detection and prevention systems are used.
- Penetration testing is conducted.
- Encryption is applied.
- Data loss prevention software is used

5.2 Administrative Measures

The administrative measures implemented by the company regarding the personal data it processes are as follows:

- Disciplinary regulations containing data security provisions exist for employees.
- Employees are provided with periodic training and awareness programs on data security.
- An authorization matrix has been established for employees.
- Corporate policies have been prepared and implemented regarding access, information security, usage, storage, and disposal.

- Confidentiality agreements are executed.
- The authorizations of employees who change roles or leave the company are revoked.
- Contracts include data security provisions.
- Personal data security policies and procedures have been established.
- Personal data security issues are reported promptly.
- Monitoring of personal data security is conducted.
- Periodic and/or random internal audits are conducted and enforced.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of special categories of personal data have been established and are implemented.
- Service providers processing data are periodically audited for data security.
- Service providers processing data are provided with data security awareness.

6. Personal Data Destruction Techniques

At the end of the retention period prescribed by the applicable legislation or the period necessary for the purposes for which they were processed, personal data are destroyed by the Company ex officio or upon the request of the relevant data subject, using the techniques specified below, in accordance with the provisions of the applicable legislation.

6.1 Deletion of Personal Data

Personal data are deleted using the methods specified in Table 3.

DATA STORAGE MEDIUM	DESCRIPTION
Personal Data Stored on Servers	For personal data stored on servers whose retention period has expired, the system administrator revokes the access rights of the relevant users, after which the deletion process is carried out.
Personal Data in Electronic Media	Personal data stored in electronic media whose retention period has expired are rendered inaccessible and unusable for all employees except the database administrator.
Personal Data in Physical Media	For personal data stored in physical media whose retention period has expired, access is denied to all employees except the unit manager responsible for the document archives. In addition, data are obscured by crossing out, painting over, or erasing so as to be unreadable.

Table 3: Deletion of Personal Data

6.2 Destruction of Personal Data

Personal data are destroyed by the Company using the methods provided in Table 4.

DATA RECORD MEDIUM	DESCRIPTION
Personal Data in Physical Media	Personal data in paper form whose retention period has expired are destroyed irreversibly using paper shredders.
Personal Data in Optical / Magnetic Media	Personal data in optical and magnetic media whose retention period has expired are physically destroyed by melting, burning, or pulverizing. Additionally, data on magnetic media are rendered

	unreadable by passing the media through a special device and exposing it to a high-intensity magnetic field.

Table 4: Destruction of Personal Data

6.3 Anonymization of Personal Data

The anonymization of personal data means rendering the data in such a way that they cannot, under any circumstances, be associated with an identified or identifiable natural person, even if combined with other data.

For personal data to be considered anonymized, they must be rendered impossible to associate with an identified or identifiable natural person by using appropriate technical methods for the relevant data medium and activity area, including preventing restoration by the data controller or third parties and avoiding linkage with other data.

7. Retention and Destruction Periods

With respect to personal data processed within the scope of its activities, the Company determines;

- Retention periods for each personal data item within all activities performed in processes are recorded in the Personal Data Processing Inventory.
- Retention periods by data category are recorded in VERBIS.
- Retention periods by process are indicated in the Personal Data Retention and Destruction Policy.

The Company may update the aforementioned retention periods when necessary.

For personal data whose retention periods have expired, deletion, destruction, or anonymization is carried out ex officio by the Company.

DATA CATEGORY	RETENTION PERIOD	DESTRUCTION PERIOD
Employment	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Legal Proceedings	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Customer Transactions	5 years	Destroyed in the first periodic destruction period following the expiration of the retention period
Physical Security	6 months	Destroyed in the first periodic destruction period following the expiration of the retention period
Operational Security	3 months	Destroyed in the first periodic destruction period following the expiration of the retention period
Finance	10 years	Destroyed in the first periodic destruction period following the expiration of the retention period

Professional Experience	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Marketing	10 years	Destroyed in the first periodic destruction period following the expiration of the retention period
Audio-Visual Records	6 months	Destroyed in the first periodic destruction period following the expiration of the retention period
Race and Ethnic Origin	10 years	Destroyed in the first periodic destruction period following the expiration of the retention period
Health Information	15 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Criminal Conviction and Security Measures	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Military Service Information	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Smoking Information	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Employment	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period
Legal Proceedings	10 years from the termination of the contract	Destroyed in the first periodic destruction period following the expiration of the retention period

Table 5: Retention and Destruction Periods by Process

8. Periodic Destruction Period

Pursuant to Article 11 of the Regulation, the Company has determined the periodic destruction period as six months. Accordingly, periodic destruction procedures are conducted every year in June and December within the Company.

9. Publication and Retention of the Policy

The policy is published in two formats: printed (wet-signed) and electronic, and it is disclosed publicly on the Company's website.

10. Policy Review and Update Period

The policy is reviewed as needed, and the relevant sections are updated when necessary.