ERDEMOĞLU
HOLDİNG

Our Personal Data Retention and Destruction Policy

Erdemoğlu Holding A.Ş.
Personal Data Retention and Destruction Policy

1. INTRODUCTION

1.1 PURPOSE

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

In line with its determined mission, vision and fundamental principles, the Company prioritizes processing the personal and/or special categories of personal data of all , including job applicants, employees, interns, shareholders/partners, business partners, supplier employees and officials, visitors, third-party employees, website visitors, consultants, or any other real persons whose personal data are processed by the Company, in accordance with the Constitution of the Republic of Türkiye, international agreements, the Personal Data Protection Law No. 6698 ("Law") and other relevant legislation, and ensuring that data subjects can effectively exercise their rights.

Personal data retention and destruction activities are carried out in accordance with this Policy prepared by the Company in this regard.

1.2 SCOPE

This Policy covers the personal and/or special categories of personal data belonging to all real persons, including job applicants, employees, interns, shareholders/partners, business partners, supplier employees and officials, visitors, third-party employees, website visitors, consultants, or any other real persons whose personal data are processed by the Company. This Policy applies to all recording environments owned or managed by the Company in which personal data 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.
Data Processor	A natural or legal person who processes personal data on behalf of the data controller based on the authority granted.
Recipient Group	The category of natural or legal persons to whom personal data are transferred by the data controller.

2. RESPONSIBILITIES AND DUTY DISTRIBUTION

All units and employees of the Company actively support the responsible units in ensuring the proper implementation of technical and administrative measures taken within the scope of

this Policy, training and raising awareness of unit employees, monitoring and continuous auditing, preventing unlawful processing of personal data, preventing unlawful access to personal data, and ensuring lawful retention of personal data by taking technical and administrative measures for data security in all environments where personal data are processed.

The titles, units and duty descriptions of those involved in personal data retention and destruction processes are set out in Table 1.

TITLE	UNIT	DUTY
IT Support Officer	Information Technologies	Ensuring lawful processing, retention, protection and destruction of personal data; implementation of technical and administrative measures within the unit's responsibility; compliance with the Policy
Human Resources Manager	Human Resources	Ensuring lawful processing, retention, protection and destruction of personal data; implementation of technical and administrative measures within the unit's responsibility; compliance with the Policy
Protection, Security and Administrative Affairs Manager	Protection, Security and Administrative Affairs	Ensuring lawful processing, retention, protection and destruction of personal data; implementation of technical and administrative measures within the unit's responsibility; compliance with the Policy

Table 1: Duty Distribution for Retention and Destruction Processes

3. RECORDING ENVIRONMENTS

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: Personal Data Retention Environments

4. EXPLANATIONS REGARDING RETENTION AND DESTRUCTION

The Company retains and destroys personal data of all real persons in accordance with the Law.

4.1 EXPLANATIONS REGARDING RETENTION

Articles 3, 4, 5 and 6 of the Law regulate personal data processing principles and conditions. Accordingly, personal data are retained for the period stipulated in the relevant legislation or required by the processing purpose.

4.1.1 LEGAL GROUNDS REQUIRING RETENTION

Personal data are retained for the periods stipulated under the following legislation, including but not limited to:

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

and other secondary legislation in force.

4.1.2 PROCESSING PURPOSES REQUIRING RETENTION

The Company retains personal data for purposes including but not limited to:

- Execution of Emergency Management Processes
- Execution of Information Security Processes
- Conducting Recruitment and Placement Processes
- Execution of Job Application Processes
- Employee Satisfaction and Engagement Processes
- Fulfillment of Employment Contract and Legal Obligations
- Execution of Fringe Benefits Processes
- Conducting Audit and Ethics Activities
- Execution of Training Activities
- Execution of Access Authorization Processes
- Ensuring Compliance with Legislation
- Execution of Finance and Accounting Affairs
- Ensuring Physical Space Security
- Execution of Assignment Processes
- Follow-up and Execution of Legal Affairs
- Internal Audit / Investigation Activities

- Execution of Communication Activities
- Planning of Human Resources Processes
- Execution and Supervision of Business Activities
- Execution of Occupational Health and Safety Activities
- Business Continuity Activities
- Execution of Procurement Processes
- Advertising / Campaign / Promotion Processes
- Risk Management Processes
- Archiving Activities
- Corporate Social Responsibility Activities
- Execution of Contract Processes
- Sponsorship Activities
- Strategic Planning Activities
- Follow-up of Requests and Complaints
- Ensuring Security of Movable Assets
- Execution of Wage Policy
- Ensuring Operational Security
- Execution of Investment Processes
- Providing Information to Authorized Institutions
- Execution of Management Activities
- Creation and Monitoring of Visitor Records

4.2 GROUNDS REQUIRING DESTRUCTION

Personal data shall be deleted, destroyed or anonymized in cases where:

- Relevant legislation is amended or repealed,
- The processing purpose ceases to exist,
- Explicit consent is withdrawn,
- The data subject's request is accepted,
- The Board deems the request appropriate,
- The maximum retention period expires without a lawful basis for further retention.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

In order to ensure the secure retention of personal data, to prevent their unlawful processing and access, and to ensure the lawful destruction of personal data, the Company implements technical and administrative measures in accordance with Article 12 of the Law and the fourth paragraph of Article 6 of the Law, within the framework of the adequate measures determined and announced by the Board for special categories of personal data.

5.1 TECHNICAL MEASURES

The technical measures adopted by the Company with respect to the personal data it processes are set forth below:

►Network security and application security are ensured.
►A closed system network is used for the transfer of personal data via networks.
►Key management practices are implemented.
►Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
►The security of personal data stored in cloud environments is ensured.
►Regular maintenance and updates are carried out.
►Access logs are regularly maintained.
►Data masking measures are implemented where necessary.
►Up-to-date antivirus systems are used.
►Firewalls are utilized.
►Security cameras operate on a separate WLAN.
►Additional security measures are taken for personal data transferred via paper, and relevant documents are sent in the format of confidential documents.
►Necessary security measures are taken regarding entry to and exit from 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 also ensured.
►User account management and authorization control systems are implemented and monitored.
►Log records are maintained in a manner that prevents user intervention.
►Where special categories of personal data are transmitted via electronic mail, they are sent in encrypted form and exclusively through Registered Electronic Mail (KEP) or corporate email accounts.
►Secure encryption and cryptographic keys are used for special categories of personal data and are managed by different units.
►Intrusion detection and prevention systems are utilized.
►Penetration testing is conducted.
►Cybersecurity measures have been implemented and their application is continuously monitored.
►Encryption is applied.
►Special categories of personal data transferred via portable storage devices, CDs or DVDs are transmitted in encrypted form.
►Data loss prevention software is utilized.
►Physical backup is performed within the backup system.
►High-level antivirus protection is used.

5.2 ADMINISTRATIVE MEASURES

The administrative measures adopted by the Company with respect to the personal data it processes are set forth below:

►Disciplinary regulations containing data security provisions for employees are in place.
►Training and awareness activities on data security are conducted for employees at regular intervals.
►An authorization matrix has been established for employees.
►Corporate policies regarding access, information security, use, retention and destruction have been prepared and are implemented.
►Confidentiality undertakings are executed.
►Authorizations of employees whose duties change or who leave employment are revoked.
►Executed contracts include data security provisions.
►Personal data security policies and procedures have been established.
►Personal data security incidents are promptly reported.
►Personal data security is continuously monitored.
►Personal data are minimized to the extent possible.
►Internal periodic and/or random audits are conducted and commissioned.
►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.
►Data processors and service providers are periodically audited with respect to data security.
►Awareness regarding data security is ensured among data processors and service providers.

6. PERSONAL DATA DESTRUCTION TECHNIQUES

Upon the expiry of the retention period stipulated in the relevant legislation or required for the purposes for which they are processed, personal data shall be destroyed by the Company, either ex officio or upon the request of the data subject, in accordance with the relevant legislation and by using the techniques specified below.

6.1 DELETION OF PERSONAL DATA

Personal data are deleted using the methods set forth in Table 3 below.

DATA RECORDING ENVIRONMENT	DESCRIPTION
Personal Data Stored on Servers	For personal data stored on servers whose retention period has expired, access authorizations of the relevant users are revoked by the system administrator, and subsequently the deletion process is carried out.
Personal Data Stored in Electronic Environments	Personal data stored in electronic environments whose retention period has expired are rendered completely inaccessible and unusable for all employees (relevant users), except for the database administrator.
Personal Data Stored in Physical Environments	For personal data stored in physical environments whose retention period has expired, such data are rendered completely inaccessible and unusable for all employees except the unit manager responsible for the document archive. In addition, a masking process is applied by crossing out, painting over, or erasing the data so that they become unreadable.

Table 3: Deletion of Personal Data

6.2 DESTRUCTION OF PERSONAL DATA

Personal data are destroyed by the Company using the methods set forth in Table-4.

DATA RECORDING	DESCRIPTION
Personal Data in Physical Environment	The personal data in paper environment that needs to be kept confidential is destroyed at the end of the required period, in a way that it cannot be reversed in paper shredding machines.
Personal Data in Optical / Magnetic Media	The process of physically destroying personal data in optical and magnetic media by melting, burning, or pulverizing at the end of the required period is applied. Additionally, the magnetic media is passed through a special device to expose it to a high level of magnetic field, making the data unreadable.

Table 4: Destruction of Personal Data

6.3 ANONYMIZATION OF PERSONAL DATA

Personal data anonymization is the process of rendering personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even if matched with other data.

For personal data to be considered anonymized, it must be rendered impossible to associate with an identified or identifiable natural person, even through the use of appropriate techniques by the data controller or third parties, including reversing the process and/or matching the data with other data, taking into account the recording medium and the relevant field of activity.

7. RETENTION AND DESTRUCTION PERIODS

With respect to the personal data processed by the Company within the scope of its activities:

► Personal data retention periods determined on a personal data basis for all activities carried out depending on the relevant processes are set out in the Personal Data Processing Inventory,
► Retention periods determined on a data category basis are specified in the registration with VERBİS,
► Retention periods determined on a process basis are regulated under the Personal Data Retention and Destruction Policy.

The Company may update such retention periods where necessary.

Upon the expiration of the applicable retention periods, the Company shall ex officio delete, destroy, or anonymize the relevant personal data.

DATA CATEGORY	RETENTION PERIOD	DESTRUCTION PERIOD
Identity	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Communication	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Location	2 Years	During the first periodic destruction cycle following the end of the retention period
Personnel	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Legal Action	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Customer Transaction	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Physical Space Security	2 Years	During the first periodic destruction cycle following the end of the retention period
Transaction Security	2 Years	During the first periodic destruction cycle following the end of the retention period
Risk Management	10 Years	During the first periodic destruction cycle following the end of the retention period
Finance	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Professional Experience	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Visual and Auditory Records	2 Months	During the first periodic destruction cycle following the end of the retention period
Health Information	15 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Criminal Convictions and Security Measures	10 years following the termination of the contract	During the first periodic destruction cycle following the end of the retention period
Biometric Data	Not Stored	Not Stored

8. PERIODIC DESTRUCTION PROCESS

The Company determines the periodic destruction period as 6 months, to be carried out every June and December.

9. PUBLICATION AND STORAGE OF THE POLICY

The Policy is published in wet-signed hard copy and electronic format and disclosed on the Company's website.

10. POLICY UPDATE PERIOD

This Policy is reviewed and updated as required.