ED ZEMİN TEKNOLOJİLERİ A.Ş.

PERSONAL DATA RETENTION AND DISPOSAL POLICY

TABLE OF CONTENTS

1. Purpose
2. Definitions
3. Scope
4. Reasons Requiring Retention and Disposal of Personal Data
5. Storage Media
6. Retention and Disposal Periods; Periodic Disposal
7. Disposal
8. Technical and Administrative Measures for Retention and Processing of Personal Data
9. Implementation
10. Retention of the Policy
11. Policy Violation and Violation Review
ANNEX-A / Retention and Disposal Periods Table
ANNEX-B / Table of Persons Involved in Retention and Disposal Processes

1. Purpose

1. This Personal Data Retention and Disposal Policy (Policy) has been prepared in accordance with Article 5 of the Regulation on Deletion, Destruction or Anonymisation of Personal Data, and in line with the personal data processing inventory of the Data Controller (Company).
2. This Policy sets out the principles of the Company regarding retention and disposal of personal data in order to ensure compliance with the applicable law and secondary legislation.
3. This Policy has been prepared to determine the procedures and principles regarding storage and disposal activities carried out by the Company.
4. This Policy observes the following principles set out in the Personal Data Protection Law No. 6698 (Law) for the processing of personal data: lawful and fair processing; accuracy and up-to-date data; processing for specified, explicit and legitimate purposes; relevant, limited and proportionate processing; and retention for the period stipulated by law or required for the processing purpose.
5. This Policy applies to all physical and electronic documents/media, including originals and copies, arranged within the scope of the Company's activities.
6. Applicable legislation may require the Company to retain certain records for certain periods. Non-compliance with such retention periods may expose the Company to sanctions and penalties, obstruct the administration of justice, cause loss of evidentiary value of legal evidence and/or significantly damage the Company's position in legal proceedings. Therefore, this Policy: (i) contains an "ANNEX-A / Retention and Disposal Periods Table" prepared within the scope of applicable legislation, setting out processes and specific retention periods; and (ii) contains an "ANNEX-B / Table of Persons Involved in Retention and Disposal Processes", identifying the persons/units within the Company responsible for retention and disposal processes and their duties.
7. All employees of the Company are obliged to fully understand and implement this Policy.

2. Definitions

Unless otherwise specified as a proper noun or separately defined within this Policy, the terms listed below shall have the meanings attributed to them:

TERM	DEFINITION
Explicit Consent	Consent related to a specific subject, based on information and expressed with free will.
Recipient Group	Category of natural or legal persons to whom personal data is transferred by the Data Controller.
Active Records	Records currently in use for the operation, administration and management of the Company.
Inactive Records	Records that are not in use but whose retention periods have not expired as they may need to be processed later.
Anonymisation	Rendering personal data impossible to associate with an identified or identifiable natural person in any way, even when matched with other data.
Employee	Natural persons working within the Data Controller.

Degaussing	The process of passing magnetic media through a device exposing it to a very high magnetic field, thereby rendering the data on it unreadable.
Electronic Media	Media in which data is held, logical or arithmetic operations are applied, and operations such as modification, deletion, retrieval or transfer are performed automatically or semi-automatically with minimal human intervention.
Non-Electronic Media	Manual processing activities connected to a data filing system that facilitate access and interpretation of manually prepared records.
Physical Destruction (for Electronic Data)	Physical destruction of optical and magnetic media by melting, burning, or pulverising.
Service Providers	Natural and legal persons engaged in commercial activities to sell products or services to the Data Controller, and natural and legal persons acting as intermediaries for such services.
Two-Factor Authentication	A verification system consisting of a combination of username and password with a separate external authentication system (mobile phone, security question, cryptographic key, etc.).
Secondary Legislation	Any regulation, circular, communiqué, principle decision or similar administrative decision or general opinion issued or adopted by the Personal Data Protection Authority pursuant to the Law.
Data Subject	The natural person whose personal data is processed.
Relevant Users	Persons within the Data Controller's organisation or processing personal data pursuant to authority and instructions from the Data Controller, excluding those responsible for technical storage, protection and backup of data.
Disposal	Any one or all of the operations of deletion, destruction and/or anonymisation.
Law	Personal Data Protection Law No. 6698.
Masking/Pseudonymisation	Operations such as striking out, painting over, blurring or starring out the entirety of personal data so that it cannot be associated with an identified or identifiable natural person.
Storage Medium	Any medium in which personal data processed fully or partly automatically or non-automatically as part of a data filing system is held.
Personal Data	Any information relating to an identified or identifiable natural person.
Registered Electronic Mail (REM/KEP)	The qualified form of email that provides legal evidence regarding its use, including sending and delivery of electronic messages.
Personal Data Processing	The inventory created by the Data Controller associating

Inventory	personal data processing activities carried out in connection with its business processes with the purposes, legal bases, data categories, recipient groups and data subject groups, containing retention periods required for processing purposes, personal data planned to be transferred to foreign countries, and security measures.
Personal Data Protection Board (Board)	The Board established under the Law.
Personal Data Protection Authority (Authority)	The public authority established under the Law.
Data Processor	Natural or legal persons who process personal data on behalf of the Data Controller based on authority granted by the Data Controller.
Data Controller	The natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data filing system.
Registry of Data Controllers (VERBİS)	The publicly accessible registration system maintained by the Presidency of the Authority in which Data Controllers are required to register pursuant to the Law.
Data Contact Person	The natural person notified during VERBİS registration to ensure communication with the Authority regarding obligations under the Law and secondary legislation.
Periodic Disposal	The deletion, destruction or anonymisation process repeated at regular recurring intervals specified in the personal data retention and disposal policy, where all conditions for processing personal data have ceased to exist.
Overwriting	Overwriting existing data with meaningless random data on magnetic media and rewritable optical media.

3. Scope

This Policy applies to all personal data processing activities of the Company as the Data Controller, and to all employees of the Company.

4. Reasons Requiring Retention and Disposal of Personal Data

The Company is required to retain personal data for the periods specified in the personal data processing inventory and this Policy. Personal data shall be retained for the duration of the processing purposes and no longer. The reasons requiring retention of personal data include statutory obligations, contractual relationships, legitimate interests, and compliance with the Law. The reasons requiring disposal of personal data include: expiry of the retention period; cessation of the purpose requiring processing; withdrawal of explicit consent; request by the data subject; and any other legal reason.

5. Storage Media

Personal data may be stored in electronic media (servers, computers, mobile devices, optical discs, magnetic media, etc.) and non-electronic media (paper, printed forms, written/typed/printed documents, etc.). The Company takes appropriate technical and administrative measures to ensure security in all storage media.

6. Retention and Disposal Periods; Periodic Disposal

Personal data is retained for the periods specified in ANNEX-A. Periodic disposal is performed every 6 (six) months. Within this scope, all personal data whose processing conditions have ceased to exist is deleted, destroyed or anonymised during each periodic disposal.

7. Disposal

7.1. Deletion

Deletion of personal data is the process of making personal data inaccessible and unavailable to relevant users. The following methods may be used for deletion: deleting from databases; deleting from files (electronic deletion); and rendering physical documents inaccessible.

7.2. Destruction

Destruction of personal data is the process of making personal data irrecoverable by any means. Destruction methods applicable to personal data include:

- Physical Destruction: Physical destruction of optical and magnetic media by melting, burning, or pulverising.
- Degaussing: Exposing magnetic media to a high magnetic field to render the data on it unreadable.
- Overwriting: Overwriting existing data with meaningless random data on magnetic media and rewritable optical media.

7.3. Anonymisation

Anonymisation of personal data means rendering the data impossible to associate with an identified or identifiable natural person in any way, even when matched with other data. Anonymisation methods include: data masking, data aggregation, data derivation, data shuffling/noise addition, k-anonymity, l-diversity and t-closeness techniques.

8. Technical and Administrative Measures for Retention and Processing of Personal Data

In order to ensure proper retention and security of personal data, and taking into account the nature and status of personal data, the Company takes physical, technical and administrative measures to prevent unauthorised modification, loss, potential damage, unauthorised processing or access, risks arising from human action or natural or physical environmental impacts. In addition:

8. Penetration tests are conducted to identify risks, threats, vulnerabilities and weaknesses in the Company's information systems and necessary measures are taken.
9. Real-time analyses through information security incident management continuously monitor risks and threats affecting the continuity of information systems.

10. Access to information systems and user authorisation are managed through access and authorisation matrices and security policies via corporate active directory.
11. Necessary physical security measures are taken for the Company's information systems equipment, software and data.
12. Hardware and software measures (access control systems, 24/7 monitoring, firewalls, intrusion prevention systems, network access control, anti-malware systems, etc.) are implemented to ensure information security against environmental threats.
13. Risks related to preventing unlawful processing of personal data are identified, appropriate technical measures are taken, and technical controls are conducted.
14. Access procedures are established within the Company and reporting and analysis activities regarding access to personal data are conducted.
15. Access to personal data storage areas is logged and inappropriate access or access attempts are monitored.
16. The Company takes necessary measures to ensure that deleted personal data is inaccessible and cannot be reused by relevant users.
17. A system has been established by the Authority to notify the data subject and the Board if personal data is obtained by others through unlawful means.
18. Security vulnerabilities are monitored, appropriate security patches are installed, and information systems are kept up to date.
19. Strong passwords are used in electronic environments where personal data is processed.
20. Secure logging systems are used in electronic environments where personal data is processed.
21. Data backup programmes that ensure secure storage of personal data are used.
22. Access to personal data stored in electronic and non-electronic media is restricted in accordance with access principles.
23. A separate policy has been determined for the security of special categories of personal data.
24. Employees involved in processing of special categories of personal data have received training on the security of such data, confidentiality agreements have been concluded, and access authorisations for users with access to such data are defined.
25. Electronic media in which special categories of personal data are processed, retained and/or accessed are protected using cryptographic methods; cryptographic keys are stored in secure environments; all transaction logs are recorded; security updates of the media are continuously monitored; and regular security tests are conducted and their results recorded.
26. Physical security measures are taken for physical environments in which special categories of personal data are processed, retained and/or accessed, and unauthorised entry and exit is prevented.
27. Where special categories of personal data must be transferred via email, it is sent encrypted using corporate email or a Registered Electronic Mail (KEP) account. Where transfer via portable memory, CD, DVD or similar media is required, data is encrypted using cryptographic methods and the cryptographic key is stored in a different environment. Where transfer between servers in different physical environments is required, data transfer is carried out by establishing a VPN between servers or using SFTP. Where transfer via paper is required, necessary measures are taken against risks such as theft, loss or unauthorised viewing, and documents are sent in "confidential" format.
28. At a minimum, security measures consistent with the Company's policies and applicable industry standards are taken.
29. All employees are responsible for ensuring the secure retention of all personal data they process. Personal data cannot be shared, disclosed or communicated orally, in writing or in any other manner with any unauthorised third party, whether accidentally or otherwise.

30. If employees share personal data without authorisation or act contrary to the requirements of this Policy, this must be reported immediately to the Data Controller Contact Person. This may generally result in disciplinary action and/or, depending on the circumstances, constitute grounds for the employee's termination for just cause pursuant to Article 25 of the Labour Law.
31. Physical copies containing personal data must be kept in locked cabinets or drawers; electronic copies must be subject to all security criteria set out in the Information Systems General Standards and Security Policy.
32. Personal data, whether in electronic or physical copy, may not be kept at employees' homes, on laptops or other personal portable devices or at locations outside the workplace.
33. Under normal circumstances, personal data shall not be kept at employees' homes, on laptops, personal portable devices or remote locations. Where Company management approves storage outside the workplace premises, employees must comply with all security criteria set out in the "Information Systems General Standards and Security Policy".
34. The employee responsible for managing portable electronic devices or removable media shall ensure: (i) backups of data stored on such devices and media in secure storage environments; (ii) appropriate encryption of special categories of personal data and other sensitive data; (iii) that special categories of personal data or other sensitive data are not copied to portable storage devices without consulting the Data Controller Contact Person or Data Officer, along with applicable encryption and protection measures; and (iv) that laptops, mobile devices and computer-based storage media containing special categories of personal data and other sensitive data are not left unattended in the office.
35. Employees may not copy and/or download documents containing personal data registered on secure Company programmes to their personal computers unless necessary; and where such documents have been downloaded or copied, after the processing purpose is complete and the document has been saved to Company servers and/or relevant programmes if it is to be used by the Company, the employee must promptly delete such electronic copy.

9. Implementation

- Publication: This Policy shall be made available to employees by the Data Controller.
- Effective Date: This Policy enters into force upon publication.
- Changes: Prior to making changes to this Policy, the Data Controller Contact Person or Data Officer may request such changes from the Data Controller. Policy changes are made by the Data Controller.

10. Retention of the Policy

The Data Controller is responsible for publishing and retaining this Policy. Each department manager is responsible for implementing this Policy. Questions regarding implementation of this Policy should be directed to the Data Controller Contact Person and Data Officer.

11. Policy Violation and Violation Review

36. If an employee fails to comply with this Policy, the department manager shall conduct a review to determine the scope and impact. Where deemed necessary, appropriate corrective measures shall be taken to mitigate the risk arising from the violation. Depending on the severity of the violation, the employee may be subject to disciplinary action (including potential termination).

37. If it is determined that follow-up actions are appropriate, the department manager shall contact the Data Controller Contact Person, Senior Management and the Human Resources Directorate and shall take the necessary steps to implement the required actions.

ANNEX-A / Retention and Disposal Periods Table

PROCESS	RETENTION PERIOD	DISPOSAL PERIOD
Occupational Health and Safety Processes	10 years from termination of employment relationship	In the first periodic disposal following the expiry of the retention period
Contract Processes	10 years from termination of employment relationship	In the first periodic disposal following the expiry of the retention period
Communication Activities	10 years from termination of employment relationship	In the first periodic disposal following the expiry of the retention period
Human Resources Processes	15 years from termination of employment relationship	In the first periodic disposal following the expiry of the retention period
Job Applicant Processes	1 year from conclusion of application process	In the first periodic disposal following the expiry of the retention period
Cybersecurity Incident Management	5 years from recording	In the first periodic disposal following the expiry of the retention period
Hardware and Software Access Processes	2 years from recording	In the first periodic disposal following the expiry of the retention period
Visitor and Meeting Participant Registration	2 years from conclusion of the event	In the first periodic disposal following the expiry of the retention period
CCTV Recordings	1 year from recording	In the first periodic disposal following the expiry of the retention period
Customer Data	10 years from termination of	In the first periodic

	business relationship	disposal following the expiry of the retention period
Procurement Processes	10 years from termination of business relationship	In the first periodic disposal following the expiry of the retention period
Accounting and Finance Processes	15 years from recording	In the first periodic disposal following the expiry of the retention period
General Assembly and Board of Directors Transactions	10 years from recording	In the first periodic disposal following the expiry of the retention period
Official and Legal Proceedings	20 years from termination of legal relationship	In the first periodic disposal following the expiry of the retention period
Travel Processes	1 year from conclusion of travel	In the first periodic disposal following the expiry of the retention period
Mail, Cargo and Shipment Records	5 years from recording	In the first periodic disposal following the expiry of the retention period

ANNEX-B / Table of Persons Involved in Retention and Disposal Processes

All employees of the Company are responsible for actively supporting the persons responsible for the implementation of the Policy and taking of the technical and administrative measures set out in this Policy.

TITLE	UNIT	DUTY
General Manager	Management	Responsible for ensuring employees act in accordance with the Policy.
Data Controller Contact Person	-	Responsible for the execution of the Policy within the Data Controller.
Information Systems Department	Information Systems Security	Responsible for providing technical solutions required for Policy implementation, informing management for necessary investments, and conducting and internally auditing deletion, destruction and anonymisation in electronic

		storage media.
Human Resources Department	Human Resources, Administrative Affairs, Security	Responsible for executing the Policy in accordance with their duties, and for supervising other unit managers and employees including Archive, Security and other units.
Legal Department	Legal	Responsible for providing legal solutions required for Policy implementation, and for matters such as document preparation and other operations for implementation.