ELEKTRAL ELEKTROMEKANİK SAN. VE TİC. A.Ş.

PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. INTRODUCTION

1.1 Purpose

This Personal Data Retention and Destruction Policy ("Policy") has been prepared in order to set forth the procedures and principles regarding retention and destruction activities carried out by the company as the "Data Controller".

Within this scope, it has been determined as a priority to ensure that the personal data of the Data Controller's employees, employee candidates, customers, and all natural persons whose personal data is held by the company for any reason, are processed in accordance with the Constitution of the Republic of Türkiye, international conventions, the Law No. 6698 on the Protection of Personal Data ("Law"), and other relevant legislation, within the framework of the Personal Data Processing and Protection Policy and this Personal Data Retention and Destruction Policy, and to ensure that data subjects can effectively exercise their rights.

1.2 Scope

The operations and procedures regarding the retention and destruction of personal data are carried out in accordance with this Policy prepared by the company for this purpose.

1.3 Abbreviations and Definitions

Term	Definition
Explicit Consent:	Consent that is related to a specific subject, based on information, and declared with free will.
Anonymization:	Rendering personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data.
Employee:	Employees of the Data Controller.
Electronic Environment:	Environments in which personal data can be created, read, modified and written by electronic devices.

Non-Electronic Environment:	All other written, printed, visual, etc. environments outside electronic environments.
Data Subject:	The natural person whose personal data is processed.
Relevant User:	Persons who process personal data within the data controller's organization or in line with the authority and instruction received from the data controller, excluding the person or unit responsible for the 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 Medium:	Any environment in which personal data processed wholly or partially automatically, or processed by non-automatic means provided that it forms part of any data recording system, is kept.
Personal Data Processing Inventory:	The inventory in which data controllers detail their personal data processing activities carried out depending on their business processes, by associating them with processing purposes and legal basis, data category, recipient group, and data subject group, and by describing the maximum retention period necessary for the purposes for which personal data is processed, the personal data envisaged to be transferred abroad, and the measures taken regarding data security.
Board:	Personal Data Protection Board.
Periodic Destruction:	The deletion, destruction or anonymization process to be carried out ex officio at repeating intervals specified in the personal data retention and destruction policy when all conditions for processing

	personal data set forth in the Law cease to exist.
Policy:	Personal Data Retention and Destruction Policy.
Data Recording System:	The recording system in which personal data is processed by being structured according to certain criteria.
Data Controllers Registry Information System:	The information system created and managed by the Presidency, accessible via the internet, which data controllers will use for applications to the Registry and other related procedures.
VERBIS:	Data Controllers Registry Information System.
Regulation:	Regulation on Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette dated 28 October 2017.

2. RESPONSIBILITIES AND DUTY DISTRIBUTIONS

All company employees actively support the responsible employees in implementing the technical and administrative measures adopted within the scope of this Policy, increasing employees' training and awareness, monitoring and continuous auditing, preventing unlawful processing of personal data, preventing unlawful access to personal data, and taking technical and administrative measures to ensure data security in all environments where personal data is processed, in order to ensure lawful retention of personal data.

3. RECORDING MEDIA

Personal data are retained securely and lawfully by the company in the environments listed in Table 1.

Table 1: Personal data retention media

Electronic Environments	Non-Electronic Environments
• Servers (domain, backup, e-mail, database, web, file sharing, etc.)	• Paper • Manual data recording systems (survey

• Software (office software)
• Information security devices (firewall, intrusion detection and prevention, antivirus, etc.)
• Personal computers (desktop, laptop)
• Mobile devices (phone, tablet, etc.)
• Optical discs (CD, DVD, etc.)
• Removable media (USB, memory card, etc.)
• Printers, scanners, photocopy machines

forms, application forms)
• Written, printed, visual media

4. EXPLANATIONS REGARDING RETENTION AND DESTRUCTION

The company retains and destroys personal data of employees, employee candidates and customers in accordance with the Law. Detailed explanations regarding retention and destruction are provided below, respectively.

4.1 Explanations Regarding Retention

In Article 3 of the Law, the concept of processing personal data is defined; Article 4 states that the processed personal data must be related to, limited and proportionate to the purpose of processing and must be retained for the period stipulated in the relevant legislation or required for the purpose for which they are processed; and Articles 5 and 6 list the conditions for processing personal data. Accordingly, within the scope of the company's activities, personal data are retained for the period stipulated in the relevant legislation or for the period appropriate for our processing purposes.

4.1.1 Legal Grounds Requiring Retention

Personal data processed within the scope of the company's activities are retained for the period stipulated in the relevant legislation.

Within this scope, personal data are retained pursuant to, inter alia:

- Law No. 6698 on the Protection of Personal Data,
- Turkish Code of Obligations No. 6098,
- Turkish Commercial Code No. 6102,
- Social Insurances and General Health Insurance Law No. 5510,
- Law No. 5651 on Regulating Publications on the Internet and Combating Crimes Committed Through Such Publications,
- Occupational Health and Safety Law No. 6331,
- Right to Information Law No. 4982,
- Public Procurement Law No. 4734,
- Law No. 3071 on the Exercise of the Right to Petition,

- Labor Law No. 4857,
- Higher Education Law No. 2547,
- Social Services Law No. 2828,
- Regulation on Occupational Health and Safety Measures to be Taken in Workplace Buildings and Annexes,
- Regulation on Archival Services,

and other secondary regulations currently in force under these laws, for the retention periods stipulated therein.

4.1.2 Processing Purposes Requiring Retention

The company retains the personal data it processes within the scope of its activities for the following purposes:

- Carrying out human resources processes.
- Ensuring corporate communication.
- Ensuring institutional security.
- Conducting statistical studies.
- Ensuring the keeping of accounting records.
- Performing activities and transactions arising from signed contracts and protocols.
- Within the scope of VERBIS, identifying the preferences and needs of employees, data controllers, contact persons, data controller representatives and data processors, arranging the services provided accordingly and updating them where necessary.
- Ensuring fulfillment of legal obligations as required or mandated by legal regulations.
- Ensuring transfer of information requested by public institutions and organizations.
- Maintaining communication with natural/legal persons who have a business relationship with the Data Controller.
- Making legal reporting.
- Serving as evidence in possible future legal disputes (burden of proof).

4.2 Reasons Requiring Destruction

Personal data shall be deleted, destroyed or anonymized by the company upon the request of the data subject or ex officio, in the following cases:

- Amendment or repeal of the relevant legislative provisions that constitute the basis for processing,
- Elimination of the purpose requiring processing or retention,
- Where processing is based solely on explicit consent, withdrawal of explicit consent by the data subject,
- Acceptance by the Authority of the application made by the data subject for deletion or destruction of personal data within the framework of the data subject's rights under Article 11 of the Law,

- Expiration of the maximum retention period that requires retention of personal data and absence of any condition justifying longer retention of personal data,

5. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN REGARDING RETENTION AND DESTRUCTION OF PERSONAL DATA

In order to ensure secure retention of personal data, prevent unlawful processing and access, and ensure lawful destruction of personal data, technical and administrative measures are taken by the company pursuant to Article 12 of the Law and Article 6/4 of the Law for special categories of personal data.

5.1 Technical Measures Regarding Retention

The technical measures taken by the company regarding retention of personal data it processes are listed below:

In accordance with technological developments related to personal data storage areas, hardware and software security systems are established to ensure information systems security against environmental threats. Access to personal data is granted only to authorized employees. Strong passwords are used in electronic environments where personal data are processed. Adequate security measures are taken for physical environments where special categories of personal data are processed, retained and/or accessed; physical security is ensured and unauthorized entry/exit is prevented. If special categories of personal data must be transferred via e-mail, they are transferred via a corporate e-mail address or by using a registered electronic mail (KEP) account. If transfer via paper is required, necessary measures are taken against risks such as theft, loss or viewing by unauthorized persons. The company also requests commitments from third parties it works with regarding fulfillment of certain standards for data retention. In addition, the company takes necessary precautions to prevent loss and unlawful use of personal data.

5.2 Administrative Measures Regarding Retention

The administrative measures taken by the company regarding retention of personal data it processes are listed below:

Employees are informed about technical and administrative risks related to retention of personal data and awareness is raised; and in cases where cooperation is carried out with third parties for retention of personal data, agreements with companies to which personal data are transferred include provisions setting forth the obligations and responsibilities of the persons to whom personal data are transferred to take necessary security measures for the protection and secure retention of transferred personal data.

5.3 Technical Measures Regarding Destruction

At the end of the retention period stipulated in the relevant legislation or required for the purpose for which they are processed, personal data are destroyed by the company ex officio or upon the application of the data subject, in accordance with the relevant legislation, using the methods specified below.

5.4 Deletion of Personal Data

Personal data are deleted using the methods provided in Table 2.

Table 2: Deletion of Personal Data

Data Recording Medium	Description
Personal Data on Servers	For personal data on servers whose retention period has expired, deletion is performed by the system administrator by removing the access authorization of relevant users.
Personal Data in Electronic Environment	Personal data in electronic environment whose retention period has expired are rendered inaccessible and non-reusable in any way for employees other than the database administrator (relevant users).
Personal Data in Physical Environment	For personal data kept in physical environment whose retention period has expired, they are rendered inaccessible and non-reusable in any way for employees other than the unit manager responsible for the document archive. In addition, blackening is applied by crossing out / painting over / erasing in a manner that makes it unreadable.
Personal Data on Portable Media	For personal data kept in flash-based storage media whose retention period has expired, they are encrypted by the system administrator, access authorization is granted only to the system administrator, and encryption keys are stored in secure environments.

5.5 Destruction of Personal Data

Personal data are destroyed by the company using the methods provided in Table 3.

Table 3: Destruction of Personal Data

Data Recording Medium	Description
Personal Data in Physical Environment	Personal data on paper whose retention period has expired are destroyed in paper shredders in an irrecoverable manner.
Personal Data on Optical / Magnetic Media	For personal data on optical and magnetic media whose retention period has expired, physical destruction methods such as melting, burning, or pulverizing are applied. In addition, magnetic media are passed through a special device and exposed to a high magnetic field, thereby rendering the data unreadable.

5.6 Anonymization of Personal Data

Anonymization of personal data means rendering personal data incapable of being associated with an identified or identifiable natural person in any way, even if matched with other data.

For personal data to be considered anonymized, it must be rendered incapable of being associated with an identified or identifiable natural person, even through the use of techniques appropriate for the recording medium and the relevant field of activity, such as re-identification by the company or third parties and/or matching the data with other data.

5.7 Administrative Measures Regarding Destruction

Destruction of data is carried out only by authorized employees of the company. Employees are informed within the scope of the legislation regarding protection and destruction of personal data. Necessary equipment, especially for physical destruction within the workplace, is kept available.

6. RETENTION AND DESTRUCTION PERIODS

With respect to personal data processed by the company within the scope of its activities;

Retention periods on a personal data basis for all personal data within the scope of activities carried out depending on processes are included in the Personal Data Processing Inventory; and retention periods on a process basis are included in this Personal Data Retention and Destruction Policy.

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

Table 4: Periods Regarding Retention and Destruction of Data

Process	Retention Period	Destruction Period
Customers	10 Years	6 Months Following Expiry of the Retention Period
Employees	15 Years After the Termination Date	6 Months Following Expiry of the Retention Period
Job Applicant Candidates	15 Years From the Application Date	6 Months Following Expiry of the Retention Period
Persons Contacting the Company Other Than the Data Subjects Above	10 Years	6 Months Following Expiry of the Retention Period

7. PUBLICATION AND RETENTION OF THE POLICY

The Policy is published in two different media: with wet signature (printed paper) and in electronic environment.

8. POLICY UPDATE FREQUENCY

The Policy is reviewed as needed and necessary sections are updated.

9. EFFECTIVE DATE

This Policy enters into force on 01.01.2020.

ELEKTRAL ELEKTROMEKANİK SAN. VE TİC. A.Ş.