**ELOR HOLDING
&
GROUP COMPANIES**

**DATA PROTECTION POLICY**

ELOR HOLDING & GROUP COMPANIES

DATA PROTECTION POLICY

İçindekiler

[**1.1 Purpose** 3](#_Toc162515639)

[**1.2 Scope** 3](#_Toc162515643)

[**1.3 Abbreviations and Definitions** 3](#_Toc162515645)

**2. RESPONSIBILITIES AND TASK DISTRIBUTIONS…………………………………………**5

[**3.** **RECORD ENVIRONMENTS** 6](#_Toc162515646)

[**4.** **EXPLANATIONS REGARDING STORAGE AND DESTRUCTION** 6](#_Toc162515647)

[**4.1.2 Purposes of Processing Requiring Storage** 8](#_Toc162515648)

[**4.2 Reasons Requiring Destruction** 9](#_Toc162515649)

[**5.** **TECHNICAL AND ADMINISTRATIVE MEASURES** 9](#_Toc162515650)

[**5.1 Technical Measures** 9](#_Toc162515651)

[**5.2 Administrative Measures** 11](#_Toc162515675)

[**6.** **PERSONAL DATA DESTRUCTION TECHNIQUES** 13](#_Toc162515676)

[**7.** **STORAGE AND DESTRUCTION PERIOD** 14](#_Toc162515678)

[**8.** **PERIODIC DESTRUCTION PERIOD** 15](#_Toc162515679)

[**10. UPDATED PERIOD OF THE POLICY** 16](#_Toc162515681)

[**11.** **ENFORCEMENT AND REPEAL OF THE POLICY** 16](#_Toc162515683)

1. **INTRODUCTION**

## **1.1 Purpose**

## The Personal Data Protection Policy ("Policy") has been prepared by Elor Holding ("Holding") to establish the principles and procedures regarding the data processing, storage and destruction activities carried out by the Holding.

## In line with the mission, vision, and core principles determined in the Strategic Plan, the Holding prioritizes the processing of personal data belonging to Holding employees, job candidates, interns, service providers, suppliers, visitors, customers, and other third parties in accordance with the Constitution of the Republic of Turkey, international agreements, Law No. 6698 on the Protection of Personal Data ("Law"), and other relevant legislation to ensure that the rights of the data subjects are effectively exercised.

## The processing, storage and destruction of personal data are carried out by the Holding in accordance with the Policy prepared for this purpose.

## **1.2 Scope**

## This Policy applies to the personal data of Holding employees, job candidates, interns, service providers, suppliers, visitors, customers, and other third parties, which are owned by the Holding or processed by the Holding, including all record environments where personal data is processed, and activities related to the processing of personal data.

## **1.3 Abbreviations and Definitions**

|  |  |  |
| --- | --- | --- |
| **Recipient Group:** | **:**  | The category of natural or legal persons to whom personal data is transferred by the data controller. |
| **Explicit Consent** | **:**  | Consent based on informed and freely given choice regarding a specific subject matter. |
| **Anonymization** | **:**  | Rendering personal data unable to be associated with a specific or identifiable natural person in any way, even when matched with other data. |
| **Employee** | **:**  | Personnel of Elor Holding & Group Companies |
| **Electronic Environment** | **:**  | Environments where personal data can be created, read, modified, and written using electronic devices. |
| **Non-Electronic Environment** | **:**  | All other environments excluding electronic environments, such as written, printed, visual, etc. |
| **Service Provider** | **:**  | Natural or legal person providing services to Elor Holding within a specific contractual framework. |
| **Data Subject:** |  | **:**  | The natural person whose personal data is processed. |
| **Related User**  |  | **:**  | Individuals who process personal data within the data controller organization or based on the authority and instructions received from the data controller, excluding those responsible for the technical storage, protection, and backup of data. |
| **Destruction:** |  | **:**  | Deleting, destroying, or anonymizing personal data. |
| **Law**  |  | **:**  | Turkish Law No. 6698 on the Protection of Personal Data. |
| **Record Environment** |  | **:**  | Any environment where personal data is processed, whether entirely or partially automated or non-automated but forming part of any data recording system. |
| **Personal Data:** |  | **:**  | Any information relating to an identified or identifiable natural person. |
| **Personal Data Processing Inventory:** |  | **:**  | An inventory created by data controllers detailing the personal data processing activities carried out in accordance with their business processes. This inventory associates personal data processing activities with the purposes and legal bases of processing, data categories, recipient groups to whom the data is transferred, and the group of data subjects. It also specifies the maximum retention period necessary for the purposes for which the personal data are processed, as well as the personal data intended for transfer to foreign countries and the measures taken for data security. |
|  **Personal Data Processing:** |  | **:**  | Any operation performed on personal data, whether wholly or partially automated or non-automated, including obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, making available, classifying, or preventing the use of data. |

**Board** **:** Turkish Personal Data Protection Board.

|  |  |  |
| --- | --- | --- |
| **Sensitive Personal Data:** | **:**  | Data concerning individuals' race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, attire, membership in associations, foundations or trade unions, health, sex life, criminal record, and security measures, as well as biometric and genetic data. |
| **Periodic Destruction** | **:**  | The deletion, destruction, or anonymization of personal data carried out ex officio at recurring intervals as specified in the personal data retention and destruction policy when all conditions for the processing of personal data set forth in the law cease to exist. |

**Policy** **:** Personal Data Processing, Storage and Destruction Policy

|  |  |  |
| --- | --- | --- |
| **Data Processor**  | **:**  | Natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller. |
| **Data Recording System**  | **:**  | A system where personal data is structured and processed according to specific criteria. |
| **Data Controller**  | **:**  | 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. |
| **Data Controllers Registry Information System** | **:**  | The information system created and managed by the Presidency, accessible via the internet, which data controllers will use for registration and related procedures. |
| **VERBİS**  | **:**  | Data Controllers Registry Information System. |
| **Regulation**  | **:**  | Turkish Regulation on Deletion, Destruction, or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017. |

1. **RESPONSIBILITIES AND TASK DISTRIBUTIONS**

All units and employees of the Holding actively support responsible units in ensuring the proper implementation of technical and administrative measures taken within the scope of the Policy, increasing the awareness and training of unit employees, monitoring and continuously auditing, preventing the unlawful processing of personal data, preventing unauthorized access to personal data, and ensuring the lawful storage of personal data by taking technical and administrative measures to ensure data security in all environments where personal data is processed.

The titles, units, and job descriptions of those involved in the storage and destruction processes of personal data are provided in Table 1.

#### *Table 1: Distribution of Responsibilities for Storage and Destruction Processes*

|  |  |  |
| --- | --- | --- |
| **TITLE**  | **DEPARTMENT** | **ASSIGNMENT**  |
| "Personal Data Protection Committee (All Department Managers)" | Personal Data Protection Committee  | They are responsible for ensuring compliance with the policy by employees.  |
| Human Resources Department Manager |  Human Resources Department | They are responsible for the preparation, development, implementation, publication, and updating of the policy in relevant environments. |
| Information Technology Department Manager | Information Technology Department | They are responsible for providing the technical solutions needed for the implementation of the policy |
| Legal Department Representative,All Department Managers of Elor Holding"  | All Departments and Employees of Elor Holding | They are responsible for implementing the Policy in accordance with their duties |

# **RECORD ENVIRONMENTS**

#

Personal data is securely stored in compliance with the law in the environments listed by the Holding in Table 2.

#### *Table 2: Personal Data Storage Environments*

|  |  |
| --- | --- |
| Electronic Environments | Non-Electronic Environments |
| * Servers (domain, backup, email, database, web, file sharing)
* Software (all holding software, email systems)
* Information security devices and software (firewall, intrusion detection and prevention, log file, antivirus, etc.)
* Personal computers (desktop, laptop)
* Mobile devices (phone, tablet, etc.)
* Optical disks (CD, DVD, etc.)
* Removable media (USB, Memory Card, etc.)
* Printer, scanner, photocopier
 | * Paper
* Manual data recording systems (survey forms, visitor logbook)
* Written, printed, visual environments

   |

# **4.** **EXPLANATIONS REGARDING STORAGE AND DESTRUCTION**

The personal data of employees, job applicants, interns, service providers, suppliers, visitors, and customers with whom Elor Holding or its affiliated organizations are in relation, are stored and disposed of in accordance with the Law.

In this context, detailed explanations regarding storage and disposal are provided below, respectively.

**4.1 Explanations Regarding Storage**

In Article 3 of the Law, the concept of processing personal data is defined, while Article 4 stipulates that processed personal data must be relevant, limited to the purposes for which they are processed, and kept for the period prescribed by relevant legislation or as necessary for the purposes for which they were processed. Articles 5 and 6 list the conditions for processing personal data.

Accordingly, within the scope of its activities, the Holding retains personal data for the period prescribed by relevant legislation or as necessary for the purposes of processing. The retention and disposal periods are detailed in the data inventory in accordance with the process.

**4.1.1 Legal Grounds Requiring Storage**

Personal data processed within the scope of activities in the Holding is retained for the period prescribed by relevant legislation. In this context, personal data is retained for the durations envisaged under the following laws and regulations:

* Turkish Law No. 6698 on the Protection of Personal Data,
* Turkish Civil Code No. 6098,
* Turkish Commercial Code No. 6102,
* Turkish Law No. 5510 on Social Insurance and General Health Insurance,
* Turkish Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed through These Publications,
* Turkish Tax Procedure Law No. 213 and related legislation,
* Turkish Occupational Health and Safety Law No. 6331,
* Turkish Labor Law No. 4857,
* Turkish Social Services Law No. 2828,
* Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Attachments, as well as other secondary regulations in force under these laws.

The legal and operational reasons for data retention are detailed in the data inventory

### **4.1.2 Purposes of Processing Requiring Storage**

The Holding retains the personal data processed within the scope of its activities for the following purposes:

* Conducting Emergency Management Processes
* Conducting Information Security Processes
* Managing Job Applicant and Internship Application Processes
* Fulfilling Contractual and Legal Obligations for Employees
* Conducting Processes Related to Employee Benefits and Welfare
* Conducting Employee Satisfaction and Engagement Processes
* Conducting Audit / Ethics Activities
* Conducting Training Activities
* Managing Access Permissions
* Ensuring Compliance of Activities with Regulations
* Conducting Financial and Accounting Operations
* Ensuring Physical Space Security
* Tracking and Managing Legal Affairs
* Conducting Internal Audit / Investigation / Intelligence Activities
* Conducting Communication Activities
* Planning Human Resources Processes
* Conducting Business Activities / Audits
* Conducting Occupational Health / Safety Activities
* Conducting Business Continuity Activities
* Managing Procurement Processes for Goods / Services
* Managing Sales Processes for Goods / Services
* Organizing and Managing Events
* Conducting Performance Evaluation Processes
* Conducting Contract Processes
* Ensuring Compliance with Applicable Laws
* Implementing Wage Policies
* Ensuring the Security of Data Controller Operations
* Providing Information to Authorized Individuals, Institutions, and Organizations
* Foreign Personnel Work and Residence Permit Procedures
* Conducting Management Activities

## **4.2 Reasons Requiring Destruction**

Personal data is deleted, destroyed, or anonymized by the Holding in the following circumstances:

* Changes or revocation of relevant legislative provisions forming the basis for processing,
* Cessation of the purpose requiring processing or storage of personal data,
* Withdrawal of explicit consent by the data subject in cases where processing of personal data is based solely on explicit consent,
* Acceptance by the Holding of the data subject's application for deletion and destruction of personal data within the framework of the data subject's rights under Article 11 of the Law,
* Refusal by the Holding to comply with the data subject's request for deletion, destruction, or anonymization of personal data, dissatisfaction with the response provided, or failure to respond within the period specified in the Law; lodging a complaint with the Authority and the Authority finding the complaint justified,
* Expiry of the maximum retention period required for personal data storage and absence of any conditions justifying the continued retention of personal data.

In these cases, personal data is deleted, destroyed, or anonymized upon the request of the data subject or ex officio by the Holding

# **5. TECHNICAL AND ADMINISTRATIVE MEASURES**

#

In accordance with Article 12 of the Law and Article 6, paragraph 4, of the Law, special measures determined and announced by the Authority for sensitive personal data are taken by the Holding within the framework of technical and administrative measures to ensure the secure storage of personal data, prevent its unlawful processing and access, and ensure the lawful destruction of personal data

**5.1 Technical Measures**

## The technical measures taken by the Holding concerning the processing of personal data include:

## Ensuring network and application security

## Regular password changes for domain accounts every six months, along with the implementation of multi-factor authentication in appropriate structures

## Conducting penetration tests to identify risks, threats, vulnerabilities, and any existing weaknesses in the Holding's information systems, and taking necessary measures

## Continuous monitoring of risks and threats that may affect the continuity of information systems through information security incident management

## Managing access to information systems, user authorization, user account management, and access and authorization matrix through security policies at the Holding level

## Access to cloud environments is controlled through defined access permissions for relevant users using username and password, ensuring the security of stored personal data

## Implementation of security measures in information technology systems procurement, development, and maintenance according to relevant procedures

## Physical documents are shredded or destroyed by burning within the company premises or through outsourced services

## Implementation of necessary measures for the physical security of information technology equipment, software, and data

## Implementation of hardware (fingerprint access control system allowing access only to authorized personnel in the server room, fire extinguishing system, and air conditioning system) and software (firewalls, intrusion prevention systems, network access control, antivirus software) measures to ensure information systems security against environmental threats

## Identification of risks to prevent the unlawful processing of personal data, ensuring the implementation of technical measures appropriate to these risks, and conducting technical controls on the measures taken

## Backing up personal data by our company and the cloud service providers we use, ensuring the security of the backed-up personal data

## USB port usage is disabled within the Holding. In case of a usage requirement, the System Administrator grants temporary usage permission to the requesting user. Once the need is fulfilled, the USB port is disabled for the respective user.

## Establishment of access control procedures within the Holding, including reporting and analysis of access to personal data

## Logging access to areas where personal data is stored, keeping track of inappropriate accesses or access attempts

## Ensuring that deleted personal data is inaccessible and cannot be reused for relevant users by the Holding

## Establishing a system and infrastructure by the Holding to report to the data subject and the Authority in case personal data is unlawfully obtained by others

## Installing appropriate security patches and keeping information systems up to date by monitoring security vulnerabilities

## Using strong passwords in electronic environments where personal data is processed, and not accepting passwords that do not comply with the password policy

## Log records are kept in compliance with Law No. 5651 without any user intervention. Data backup programs ensuring the secure storage of personal data are used.

## SSL security certificates are used on the Holding's website to ensure secure access.

## Continuous monitoring of the implementation of cybersecurity measures to ensure their effectiveness.

## **5.2 Administrative Measures**

* The administrative measures taken by the Holding concerning the processing of personal data are listed below:
* For General Personal Data:
* Providing training sessions on communication techniques, technical knowledge skills, Labor Law, and other relevant legislation to enhance the qualifications of employees, aiming to prevent unlawful processing and unauthorized access, and to ensure the security and retention of personal data.
* Establishing authorization matrices for employees.
* Having employees sign confidentiality agreements related to the activities conducted by the Holding.
* Developing disciplinary procedures to be applied to employees who do not comply with security policies and procedures.
* Establishing corporate policies and procedures on access, information security, usage, personal data storage, and destruction, and implementing them.
* Revoking access privileges for employees undergoing job changes or leaving the company.
* Fulfilling the obligation to inform relevant individuals by the Holding before commencing the processing of personal data.
* Implementing necessary security measures for physical access to locations containing personal data.
* Monitoring the security of personal data processing.
* Compiling an inventory of personal data processing activities.
* Conducting periodic and unplanned audits internally within the Holding.
* Raising awareness among data processors regarding data security.
* Conducting internal and external audits of data processors' data security operations.
* Providing information security training to employees.
* Contracts signed contain provisions regarding the protection of personal data and are kept in locked cabinets.
* Notification has been made to the Data Controllers Registry Information System (VERBIS).
* Risk/threat assessments have been conducted concerning the protection of personal data.
* Personal data is minimized as much as possible.
* Personal data security issues are promptly reported.

For Special Categories of Personal Data:

* In addition to the technical measures taken:
* Regular training sessions are conducted on special categories of personal data security in accordance with the laws and related regulations.
* Privacy agreements are established.
* Access privileges and durations for users with access to data are clearly defined.
* Periodic authorization checks are conducted.
* Access privileges are immediately revoked for employees undergoing job changes or leaving the company.
* Inventories assigned by the data controller are promptly returned.
* Adequate security measures (such as protection against electrical leakage, fire, water damage, theft, etc.) are ensured according to the nature of the environment where special categories of personal data are stored.
* Physical security of these environments is ensured to prevent unauthorized access. When transferring data in paper format, necessary precautions are taken against risks such as theft, loss, or unauthorized access, and documents are sent in the format of "classified documents."
* If special categories of personal data need to be sent via email, they are encrypted and sent using a certified electronic mail system or corporate email account.
* Secure encryption/cryptographic keys are used for special categories of personal data and managed by different units.

# **6.PERSONAL DATA DESTRUCTION TECHNIQUES**

#

## At the end of the retention period prescribed by relevant legislation or required for the purposes for which they were processed, personal data is destroyed by the Holding either ex officio or upon request from the data subject, in accordance with the provisions of the relevant legislation, using the following techniques

##### **6.1 Personal Data Deletion**

##### Personal data is deleted using the methods provided in Table 3.

##### Table 3: Personal Data Deletion

|  |  |  |
| --- | --- | --- |
| Data Recording Environment |  | Explanation |
| **Personal Data Stored on Servers**  |  | For personal data on the servers whose retention period has expired, the system administrator removes the access authorization of the relevant users and deletes them. |
| **Personal Data Stored in Electronic Environments** | Personal data stored in electronic environments, whose retention period has expired, becomes inaccessible and unusable for all employees except the database administrator (relevant users). |
| **Personal Data Stored in Physical Environments** | For physical records of personal data whose retention period has expired, access is restricted and rendered unusable for all employees except the unit manager responsible for the document archive. Additionally, a blackout process is applied by crossing out/painting over/erasing in a way that renders the information unreadable. |
| **Personal Data Found on Portable Media** | Personal data stored in flash-based storage environments is encrypted. The personal data stored in these environments are deleted using appropriate software, and access and retrieval permissions for the deleted data are revoked for the relevant users. |
| **Personal Data Stored in Cloud Environments** | Access to personal data stored in cloud environments is provided encrypted. Data in the cloud system is deleted by the system administrator using the delete command, and access and retrieval permissions for the personal data in these environments are revoked for the relevant users. |

##### **6.2 Destruction of Personal Data**

##### Personal data is destroyed by Holding using the methods provided in Table 4.

##### Table 4: Destruction of Personal Data

|  |  |
| --- | --- |
| Data Recording Environment | [Explanation](https://tureng.com/tr/turkce-ingilizce/explanation) |
| **Personal Data Stored in Physical Media** | Expired personal data stored in paper format are destroyed irreversibly either by shredding using paper shredders or by incineration, ensuring they cannot be retrieved. |
| **Personal data stored on Optical / Magnetic Media** | The personal data stored in optical and magnetic media whose storage period has expired are subjected to the overwrite method for destruction, preventing the retrieval of old data. |
| **Personal data stored in cloud environments** | During the storage and utilization of personal data in cloud environments, it is imperative to encrypt them using cryptographic methods. Specifically, separate encryption keys must be utilized for each cloud solution, especially for personal data wherever possible. Upon termination of the cloud computing service relationship, all copies of the encryption keys necessary to make the personal data usable must be destroyed. |

# **STORAGE AND DESTRUCTION PERIOD**

Holding, all personal data processed within the scope of its activities are subject to specific retention periods, which are documented in the Personal Data Processing Inventory for individual personal data, in VERBIS for data categories, and in the Personal Data Storage and Destruction Policy for process-based retention periods.

The Personal Data Protection Committee may update these retention periods as necessary. Upon expiration of the retention periods, personal data is subject to deletion, destruction, or anonymization by the Information Technologies departments.

#### *Table 5: Table of storage and destruction times by process*

|  |  |  |
| --- | --- | --- |
| **SÜREÇ**  | **SAKLAMA SÜRESİ**  | **DESTRUCTION PERIOD** |
| Contract processes | 10 years following  | During the first periodic destruction following the end of the storage period |
| Execution of Holding's Communication Activities | 10 years following the termination of the activity | During the first periodic destruction following the end of the storage period |
| Execution of Human Resources Processes | 10 years following the termination of the activity | During the first periodic destruction following the end of the storage period |
| Log Records | Maximum 2 years | During the first periodic destruction following the end of the storage period |
| Execution of Hardware and Software Access Processes  | 2 years from the date of entry into the system | During the first periodic destruction following the end of the storage period |
| Keeping Visitor and Meeting Participant Records | 2 years following the end of the event | During the first periodic destruction following the end of the storage period |
| Legal Proceedings | 10 years from the date of termination of correspondence | During the first periodic destruction following the end of the storage period |
| Financial Transactions | 10 years following the termination of the commercial relationship/activity | During the first periodic destruction following the end of the storage period |
| Camera(CCTV) Recordings | 4 Months  | During the first periodic destruction following the end of the storage period |
| Records of deletion or destruction of personal data | 1 year from deletion or destruction | During the first periodic destruction following the end of the storage period |
| Records regarding employee candidates and references | 1 month after the application date | During the first periodic destruction following the end of the storage period |

# **PERIODIC DESTRUCTION PERIOD**

According to Article 11 of the Regulation, Holding has determined the periodic destruction period as 6 months. Accordingly, periodic destruction process is carried out in June and December each year at Holding. All unit managers are responsible for the implementation and management of the Personal Data Storage and Destruction Policy. In case of incidents such as breaches or security vulnerabilities occurring during the Storage and Destruction Process, requirements of Nonconformity and Corrective Action Procedure are applied.

**9. PUBLISHING AND STORAGE OF THE POLICY**

# The policy is published electronically, announced to the public on the website and kept in the document management system.

# **10. UPDATED PERIOD OF THE POLICY**

# The policy is reviewed annually and updated as needed to address any necessary changes in the relevant sections.

# **11.** **ENFORCEMENT AND REPEAL OF THE POLICY**

The policy is deemed effective following its publication on Holding's and related group companies' websites. If a decision is made to revoke it, the hard-copy original versions of the Policy are cancelled by a decision of the Board of Directors (by stamping or writing "cancelled") and signed, then stored for a minimum of 5 years. Electronic documents are cancelled by authorized personnel with password control.