ELOR HOLDING AND GROUP COMPANIES

RETENTION OF PERSONAL DATA AND DESTRUCTION POLICY

ELOR HOLDING AND GROUP COMPANIES
Personal data retention and destruction POLICY

Contents

1.INTRODUCTION

1.1 purpose

Personal data retention and destruction policy ("policy"), Elor holding ("holding company"), which is operated on transactions and business activities related to storage and disposal has been prepared in order to determine the procedures and principles.

Holding company; the strategic plan, mission, vision and guiding principles in accordance with; holding employeesna, candidates runningnainternsto, service providers,na, suppliers, visitorsto download, customers and other third parties of personal data of the Turkish republic constitution, international agreements, the law on protection of personal data No. 6698 ("Law") and other applicable legislation of the concerned persons in accordance with the rights that are processed as a priority to ensure the effective use of it is committed.

The business and operations for the disposal and storage of personal data, in accordance with the policy, which was prepared by pressing and holding in this regard is performed.

1.2 Scope

Holding employeesna, candidates runningnainternsto, service providers,na, suppliers, visitorsto download, customers and other third parties the personal data of the holding is within the scope of this Privacy Policy and are owned by or Holdingce managed environments and with regard to the processing of personal data personal data processed recording of all activities to which this policy applies.

1.3 abbreviations and definitions

Recipient Group	**:**	personal data is the natural or legal person the category of the data transferred by the principal.
Explicit consent	**:**	a specific topic related to informed consent are described based on free will.
Making anonymous	**:**	personal data, by matching with other data or identifiable natural person cannot be linked to a specific ID in no way even making.
Running	**:**	Elor holding staff.
Electronic media	**:**	personal data of the electronic devices can be created with it can be read, can be written where can be changed and environments.
Electronic non-media	**:**	electronic media outside of all written, printed, visual, etc. other environments.

Service provider	:	Elor holding within the framework of the natural or legal person that provides a particular service contract.
Contact	:	personal data is processed by a real person.
About User	:	technically, Data storage, data protection and backup, which is responsible for excluding the person or unit responsible for authorization and in accordance with the instruction or data from within the organization responsible for are the people who process personal data.
Destruction	:	of personal data deletion, destruction or has been rendered anonymous.
Law	:	The Law No. 6698 On Protection Of Personal Data.
Recording media	:	fully or partially automated, or be part of any data recording system to record non-personal data processed in any environment that contains automated ways.
Personal data	:	all kinds of information about identified or identifiable natural person specific ID.
Personal Data Processing inventory for	:	the data of persons responsible for business processes depending on the course of performing that personal data processing activities and the legal reason for processing personal data purpose of the data category, data is transferred to the recipient group and associating with a group of people created by the subject of personal data required for the purposes they are processed and the maximum conservation of the duration of the measures prescribed by explaining the transfer of personal data to foreign countries and data protection detaylandirdik the inventory.
Personal Data Processing	:	the personal data are fully or partially automated, or be part of any data recording system to record non-automatic means obtaining, recording, storage, storage, modification, rearrangement, disclosure, transfer, acquisition, can be obtained by making the introduction of classification or for use to avoid , such as data, any operation that is performed on.
Assembly	:	Personal Data Protection Board
Qualified special personal data	:	of persons, race, ethnic origin, political opinion, philosophical belief, religion and sect, or other beliefs, costume and clothing, Association or trade union membership, health, sexual life, criminal convictions and security measures data and biometrics and genetic data.

Extinction	**:**	the disappearance of all of the conditions of law in the case of the processing of personal data retention and destruction of personal data in and repeated at intervals specified in the policy ex officio be performed to delete, destroy, or the process of making anonymous.

Policy **:** Personal Data Retention and destruction Policy

Process data	**:**	the data on behalf of the principal by the power vested in responsible for data is the natural or legal persons who process personal data.
Data recording system	**:**	personal data of specific criteria configured according processed by the recording system.
Responsible for data	**:**	determines the purposes and means of the processing of personal data, the establishment and management of a natural or legal person responsible for data recording system.
Principals Registration Information System Data	**:**	Data refers to the record of responsible and accessible over the internet for their use in other related processes on the record, the president created and managed by the information system.
VERBIS	**:**	the registry data of the information system responsible for
Regulation	**:**	October 28, 2017 published in the official gazette of personal data deletion, destruction or anonymization on regulation.

2.RESPONSIBILITY AND TASK DISTRIBUTIONS

All units of the holding company and employees, technical and administrative measures that are being taken under the policy by the units responsible for the proper implementation of staff training and awareness raising, monitoring and continuous control to prevent unlawful processing of personal data, personal data, and preventing access to personal data is processed for purposes of lawful and unlawful storage of personal data in all environments technical and administrative measures for ensuring data security issues to the units responsible for the introduction of active support.

The names of the retention and disposal of personal data involved in the process, units, and mission belonging to the distribution of are given in Table 1.

Table 1: retention and disposal processes in task distribution

Title of	UNIT	TASK
Committee for the protection of personal data (All Unit Managersi)	the committee for the protection of personal data	policy is responsible for the employees to comply with.

The Human Resources Unit Manager	Human Resources Unit	of the policy preparation, development, implementation, is responsible for updating and posting about.
Information Technologies for the Y UnitManager	Information Technology unit	of the policy implementation is responsible for providing the needed technical solutions.
Legal Yeffective, Elor Holding All Unit Managers	Elor HT Oldingum units and Employees	as appropriate to their duties is responsible for the conduct of policy.

3.RECORDING MEDIA

By holding personal data in Table 2 are listed in environments that are stored in a safe manner in accordance with law.

Table 2: personal data storage environments

Electronic environments	non-electronic media,
servers (domain, backup, e-mail, database, web, file sharing, I) ✓ Software (all holding up signIsteps of the software, and e-mail systems), ✓ information security devices and software (firewall, intrusion detection and Prevention, log file, antivirus , etc.) ✓ Personal computers (desktop, notebook) ✓ mobile devices (phone, tablet, etc.) ✓ Optical drives (CD, DVD , etc.) ✓ Removable drives (USB, memory card, etc.) ✓ Printer, scanner, copier	✓ Paper ✓ , manual data recording systems (survey forms, visitor entry book) ✓ Written, printed, visual environments

4.COMMENTS REGARDING THE RETENTION AND DISPOSAL

By holding employeesIrunning candidates, interns, then, the service provider ofthose, suppliers, visitors , and customersi as a third party, the relationship of their employees or organizations referenced in the holding of personal data are stored and destroyed in accordance with the law.

In this context, the storage and disposal related to detailed explanations below, respectively, have been given.

4.1 Storing Comments On

Article 3 of the law defined the concept of the processing of personal data in Article 4, the personal data processed in connection with the purpose they are processed, limited and restrained to be stipulated in the relevant legislation or be retained as long as needed for the purpose they are processed that should be indicated, 5, and 6 th item in terms of the processing of personal data in were counted.

Accordingly, the holding (holding company) within the framework of the activities or personal data are stored until the appropriate time to our processing purposes stipulated in the relevant legislation. Storage and disposal on the basis of the duration of the process in the table the data in the inventory was determined as detailed.

4.1.1 Legal Reasons To Keep That Requires

Holdingde, the personal data processed within the framework of the activities shall be retained until such time as the relevant legislation. In this context, personal data;

- Law No. 6698 on protection of personal data
- Turkish code of obligations No. 6098,
- Turkish Commercial Code numbered 6102,
- Social insurance and General Health Insurance Law No. 5510,
- The arrangement of the material in these publications through the internet 5651 and the law on combating crime,
- 213 the Tax Procedure Law and related legislation
- No. 6331 Occupational Health and Safety Act,
- 4857 and
- Law No. 2828 on social services
- Workplace health and safety requirements for buildings and supplements to be taken in this law which are in force in accordance with other secondary legislation

in the framework prescribed until the retention period is stored. Data retention for legal and operational reasons, the data in the inventory was determined as detailed.

4.1.2 Purpose Of Processing That Requires You To Keep

Holding within the framework of activities in which stores personal data for the following purposes.

- Emergency Situation Management Processes Execution
- Information Security Processes Execution
- Running Candidates and Intern Application Process Execution
- Employees of the Business, Contractual and regulatory requirements from Sourced Liabilities instead of to be brought
- Employees for the side of the Rights and Interests of the process Execution
- Employee Satisfaction and Commitment of the processes of Execution
- The Audit / Ethics Activities Execution
- Training Activities Execution
- The Access Authorization Of The Execution
- Of Activities Regulations For The Proper Conduct
- Finance And Accounting Jobs Execution
- Physical Space, The Security Of Supply
- Legal Jobs Monitoring and Execution
- Internal Audit/ Investigation / Intelligence Activities Of The Conduct
- Communication Activities Execution
- Human Resources Processes Planning
- Business Activities Of Execution / Control
- Business Health / Safety Activities In The Conduct
- Business Continuity To Ensure Activities Execution
- Goods / Services To Buy Purchasing Process Execution
- Product / Service Sales Process Execution
- Organization and Event Management
- Performance Evaluation Of The Process Execution
- Contract Process Execution
- Is our company subject that is with the laws Compliance Ensure
- Wage Policy In The Conduct
- Data Responsible For The Operations Of The Safety Supply
- Authorized Persons, Institutions and organizations to Information Giving
- Foreign Personnel Working And Living With The Permission Of Operations
- Management Of Activities Execution

4.2 The Reasons Of Destruction

Personal data;

No modification or processing that form the basis for repeal of the provisions of the relevant legislation,

- The purpose of that require to be stored,processed or elimination
- Processing personal data in the event that only occurred pursuant to the terms of explicit consent, taking back the explicit consent of the person concerned,

- Pursuant to Article 11 of the law, the rights of the person concerned regarding his application, within the framework of the holding of the destruction or deletion of your personal data to be accepted by,
- Holding, of personal data by the person concerned, the deletion, destruction or anonymization to reject the reference to find out the answer with the demand itself or in the law in cases that do not respond within the stipulated time; and this request is approved by the board to file a complaint to the board,
- Past that is the maximum period that requires the storage of personal data and personal data for longer to keep the current lack of any circumstances that would make it right,

in case, at the request of the person concerned, deleted, destroyed by the holding company, or ex officio deleted, destroyed, or anonymous form to returnto the R.

5.TECHNICAL AND ADMINISTRATIVE MEASURES

Your personal data secure in a manner in storing, the law it's against as processing and access prevention with personal data law is appropriate as destroyed to be to the law, Article 12 , article , article of the law, Article 6 , article , article fourth , paragraph by special qualified personal data to the board by the determined and ref of adequate measures within the framework of the Holding by technical and administrative measures are taken.

5.1 Technical Measures

Committed in relation to personal data received by holding technical measures are listed below:

- Network security and application security is provided
- Passwords are changed every 6 months, employees of the domain. Also appropriate structures in multifactor authentication is performed.
- Infiltration (Penetration) tests with our informatics systems for holding risk, threat, vulnerability, and, if applicable, the necessary precautions are taken by the openings uncovered.
- Information Security Incident Management with real-time analysis results of the risks and threats that will affect the sustainability of information systems by an Information Technology Department are monitored on a continuous basis.
- Access to Information Systems, authorization of users and user account management, access and authority Matrix Holding on the basis of your security policies are made through and controlled.
- Cloud environments, the respective users access to authorized identification through the user name and password with login can. This way the stored personal data security is ensured.

- Information technology systems procurement, development and maintenance within the scope of the security measures relevant to the procedures are implemented according.
- Of physical documents in a paper with grinder by burning or by taking within the company or external service is destroyed.
- Holding information systems, equipment, software, and data necessary for the physical safety precautions are taken
- Environmental threats to ensure the security of Information Systems, hardware (fingerprint access control system that allows only authorized personnel of the room entry system, air conditioning system and fire extinguishing system) and software (firewalls, attack prevention systems, network access control, anti-virus software) measures are taken**.**
- Identify risks to prevent unlawful processing of personal data, is provided for precautionary measures to take appropriate technical measures to those risks, and technical controls.
- The responsibility of our company and the companies that we have received personal cloud service that is backed up data is being backed up and the security of personal data is ensured
- To use the USB port is closed under the holding. In case the need arise to use the system administratorrequesting the-user - term use allow. In case of termination of need, the USB port is turned off for that user
- The holding company within the access control procedureU studies are performed by creating access to personal data related to reporting and analysis
- They recorded personal access to the storage areas where the data resides improper access or access attempts are kept under control**,**
- Holding personal data will not be accessible to interested users deleted and re-provides the necessary precautions to be used.
- In the case of personal data obtained by unlawful people and others to report to the board about this situation by holding an appropriate system and infrastructure has been established.
- Are followed and the appropriate security patches and vulnerabilities of information systems being installed are kept up to date
- Strong passwords are used and processed personal data in electronic environments. In accordance with the password policy of non-passwords are not accepted.
- 5651 No. the law is appropriate as log records user intervention won't be in a way that they are kept. Providing safe and secure storage of personal data, data backup programs are used.
- Holding company Internet page, youda SSL Secure Access using a security certificate are provided.

Cyber security is constantly monitored and implementation of measures have been taken.

5.2 Administrative Measures

Committed by administrative measures in relation to holding personal data received are listed below:

- For the improvement of the quality of employees, to prevent unlawful processing of personal data, personal data, and preventing access and the provision of unlawful storage of personal data, communication techniques, skills, technical knowledge, business law and other relevant legislation are provided with training about.
- The competence Matrix was created for employees.
- Employees have signed confidentiality agreements that are executed by holding activities.
- Security policies and procedures applicable to employees who violate the disciplinary procedure was prepared.
- Access, information security, use of personal data, storage and disposal issues of corporate policies and procedures are prepared and was put into effect.
- Change the task or work separated from the powers of the employees in this field is removed.
- Before starting the processing of personal data by holding the contacts of lighting the obligation is fulfilled.
- The input to the output that contain personal data necessary security measures are taken with the physical environment.
- Personal data are made in the pursuit of security**.**
- The processing of personal data of the inventory was prepared.
- For holding periodic and non-periodic unscheduled inspections are carried out.
- Data service providers the functioning of awareness about data security provided.
- The perpetrators responsible for data datan data security for internal and external audits.
- Information security training for employees givenyou.
- Signed contracts includes provisions on the protection of personal data. Contracts are kept in locked cabinets.
- Data Caused, Registration Information System (VERBIS) notification reviewed.
- Kisisel data protection, in particular to the risk/threat assessment are reviewed.
- Your personal data is reduced as much as possible.
- Personal data security issues are reported quickly.

<u>Special qualified personal data for received technical measures:</u>
Received technical measures , as well as,

- The law , and to it is attached the regulations with your specific qualified personal data security issues, regular as training is given.
- Confidentiality agreements are made.
- The data access Authority with users, authorization scopes and durations of the net as are defined.
- Periodic as authorization checks are performed.
- Task change with , or even work from the separated employees of this field authorities immediately removed.

- In this context, the data responsible for by itself, allocated to the inventory returned to you are.
- Special qualified personal data is located in the environment of nature according to adequate security measures (electrical leakage, fire, water, flood, theft , etc. situations against) IS used, it is sure to be necessary.
- In this environment, the physical security ensuring unauthorized entry Downs is prevented. The data paper and the environment through the transfer if you need to the documents of the theft, loss , or or unauthorized persons by to be seen as such risks against the necessary precautions are taken, and the paperwork “Privacy - Grade documents” in the format they are sent.
- Special qualified personal data to electronic mail Via will be sent necessarily encrypted as and PEP or corporate mail account using your sent.
- Special qualified personal data for secure encryption/ cryptographic keys are being used and different departments are managed.

6.PERSONAL DATA DESTRUCTION TECHNIQUES

The period prescribed in the relevant legislation or for the purpose they are processed at the end of the retention period for the personal data required by the holding, ex officio or upon the request of the person concerned, again in accordance with the provisions of the legislation are destroyed by the following techniques.

6.1 Deletion Of Your Personal Data

The personal data will be deleted with the method given in Table 3.

Table 3: The Deletion Of Your Personal Data

Data recording media	Description
in the server located in Field the personal data to	that requires the server to the storage of personal data is located in time for the end of the relevant user is removed by the system administrator and the access privileges of the deletion is done.
The electronic Environment In Located of personal data to	electronic environment that requires the storage of personal data, located in the term of time, the database manager harie other employees (the users) that is made inaccessible and cannot be used again in any way.

Located in the physical environment in which personal data	is maintained in the physical environment of the archives for the storage of personal data requires that the end of that time, except for the responsible manager document that is made for all employees and cannot be used again. Also read above in a way that cannot be drawn/painted/wiping process is applied to dimming
portable media on personal data	Flash-based storage environments is maintained in your personal data are stored in encrypted form. Personal data that is maintained in these environments with the appropriate software is deleted, and the deleted users access to the data and bringing it back to the corresponding powers in question is eliminated.
Cloud Thatrtam in Yer Alan Kisisel Vcurves of the	personal data in the cloudhave access to e - encrypted is provided. Cloud data is deleted with the Delete command in the system by the system administrator, and in these circumstances, users have access to the powers of the related personal data and bringing it back is eliminated.

6.2 Destruction Of Personal Data

By holding your personal data, by the methods in Table 4 are destroyed.

Table 4: Destruction Of Personal Data

Data recording Environment	Description
located in the physical environment personal data to	the end of time paper, in a medium that requires the storage of personal data, the paper trimming machine by burning or by taking within the company or external service irreversibly destroyed.
Optical / magnetic media located personal data to	optical media, magnetic media as of the end of time that requires the storage of personal data , overwriting the method is applied to the operation to be destroyed the old data and bringing back prevented this.

Personal data in the cloud	in a cloud environmentthat the storage and use of personal data during cryptographic methods to encrypt your personal data and where possible, especially the service received each separate encryption keys for cloud solution must be used. Cloud computing service when a relationship ends, all copies of the encryption keys used to be required to bring the personal data must be destroyed.

7. RETENTION AND DESTRUCTION OF ALL TIMES

By holding, in relation to personal data that are being processed within the scope of activities;

- Depending on the process within the scope of activities that are performed with respect to all personal data the personal data on the basis of the processing of personal data storage time in the inventory of
- Data storage period on the basis of categories verbis the record;
- Storage period of personal data retention and destruction Policy on the basis of the process

it takes time.

Over time the storage in question, if necessary, will be updated by the committee for the protection of personal data.

The retention period for the personal data, which ended ex officio delete, destroy, or the process of making Anonymous Information Technology Unit is carried out by.

Table 5: Table, Storage and disposal on the basis of the duration of the process

The process	**retention period**	**disposal of the period of**
preparation of the contract	the contract expira expiration , followii year	retention period following the expiration of the first periodic destruction in the time of
Holding Communication activities of the execution	of the activity from the following expiration the end of 10 years	of the retention period following the expiration destruction in the time of the first periodic
Human Resources processes for the execution	of the activity from the following expiration the end of 10 years	of the retention period following the expiration of the first periodic destruction in the time
Log Records	Maximum of 2 years	following the expiration of the storage period at the time of the destruction of the first periodic

access to the hardware and software of the process Execution	from the date of entry into the system 2 yIl	destruction following the expiration of the retention period, the first periodic in the time of
the visitor and Meeting Attendees	end of the activity after the cessation of the 2 year	period following the expiration of the retention time of the first periodic destruction
of transactions legal	exit from the correspondence of 10 years from the date	following the expiration of the retention period of the first periodic destruction in the time of the
financial transactions	of the business relationship/10 years after the end of the activity	following the expiration of the retention period of the first periodic destruction at the time of
the camera Records	4 Months	following the expiration of the storage period at the time of the first periodic destruction
or deletion of your personal data for the destruction of records	from the date of the deletion or destruction 1. year	following the expiration of the retention period in the time of the first periodic destruction of the
candidates Running and references related records	after the reference date 1 month	following the expiration of the storage period in the period of the first periodic destruction of
the financial transactions	Commercial relationship/Activities of discontinuation from a 10 - year	period following the expiration of the retention time of the first periodic destruction

8. THE TIME OF THE PERIODIC DESTRUCTION

In accordance with Article 11 of regulation is determined as the duration of the periodic destruction of holding 6 months. Accordingly, the holding in each year, in the months of June and December of the periodic destruction process is carried out.

Personal data retention and destruction policy is responsible for the implementation and management of unit managers. Storage and disposal in the activities specified in the process in the event the violation occurred, the security weakness in inappropriate situations, such as non-compliance and corrective action procedure requirements apply.

9. THE POLICY OF PUBLICATION AND STORAGE

Politics, published electronically on the Web page to the public are announced and document management system are kept.

10.THE PERIOD OF THE POLICY IS UPDATED

Policy 1 time per year and is reviewed when needed and in need of change sections are updated**.**

11.REPEAL THE POLICY EFFECT AND

Politics, Holding and relevant to the group companies have been published on the website after it has entered into force is considered. Repeal of deciding the case, the policy is cancelled with the decision of the board of directors signed copies of old wet (shot by writing or cancellation cancellation Bowl) shall be signed and kept for at least 5 years. With documents in electronic media by persons authorized to control to cancel the password is cancelled.

Data Owner Application Form