CRONIMET
Turkey Metal Ticaret A.Ş.

CRONIMET TURKEY METAL TİCARET A.Ş.

DATA STORAGE AND DISPOSAL POLICY

This Data Retention and Disposal Policy prepared within the scope of the Law on the Protection of Personal Data Compliance Project (hereinafter *referred to as the "**Policy**")* Law on the Protection of Personal Data No. 6698 published and enacted in the Official Gazette No. 29677 on April 7th, 2016 *(hereinafter referred to as "**LPPD**" and/or "**Law**")* It has been prepared in order to determine the current status of CRONIMET TURKEY METAL **TİCARET A.Ş.** ("CRONIMET" or "**Company**") against the provisions of Article 7 titled Deletion, Disposal or Anonymization of Personal Data and Article 17 titled Crimes and Regulation on Deletion, Disposal orAnonymization of Personal Data and to determine what needs to be done legally within the framework of these determinations *(hereinafter referred to as "**Storage and Destruction Processes**")*.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose

Law on the Protection of Personal Data No. 6698 *(hereinafter referred to as "**LPPD**" and/or "**Law**")* In accordance with the provisions of Article 7 titled Deletion, Disposal or Anonymization of Personal Data and Crimes and Regulation on Deletion, Disposal orAnonymization of Personal Data, CRONIMET shows maximum sensitivity to the proper storage of personal data obtained during the execution of its activities within the scope of the relevant regulations, Law and secondary legislation and, if necessary, to destruct the personal data at the end of the period stipulated in the relevant legislation or required for the purpose for which they are processed.

Thereby, in line with this sensitivity, this Personal Data Storage and Destruction Policy ("**Policy**") has been prepared and the principles of the process management regarding the data storage and disposal activities carried out by CRONIMET have been determined by the procedure.

The following explanations are given about the methods followed for the storage and destruction/ disposal of personal data obtained during CRONIMET activities, and the process for the storage and destruction of personal data is carried out from the beginning to the end in accordance with this Policy.

1.2. Scope

This Policy prepared by CRONIMET regarding the storage and destruction of personal data in all kinds of electronic and/or printed media has been handled and prepared by observing the LPPD and other legislation on personal data and international regulations and guidance documents in this field.

Personal data belonging to CRONIMET employees, employee candidates, customers, members, service providers, suppliers, business partners, visitors and other third parties are covered by this Policy and this Policy is applied in all personal data recording environments owned and/or managed by CRONIMET and in activities for personal data processing.

1.3. Abbreviations and Definitions

Recipient Group	:	It refers to the category of natural or legal persons to whom personal data are transferred by the data controller.
Explicit Consent	:	It means a consent about a specific subject based on information and expressed in free will.
Anonymization	:	Making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.
Employees	:	It means the employees of CRONIMET TURKEY METAL TİCARET A.Ş..
Electronic Environment	:	These are the environments where personal data can be

		created, read, changed and written with electronic devices.
Non-Electronic Medium /Media	:	These are all written, printed, visual and similar media other than electronic media.
Service Provider	:	It refers to the real or legal person who provides services to CRONIMET within the framework of a specific contractual relationship with CRONIMET.
Relevant Person / Personal Data Owner	:	Real persons whose personal data shall be processed. As can be understood from the definition of personal data, the protection of the Law is only related to the real person and this person is defined as "the relevant person/ the person concerned".
Relevant User	:	Refers to the persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, except the person or unit responsible for the storage, protection and backup of the data technically.
Disposal	:	It refers to the deletion, destruction/ disposal or anonymization of personal data.
Law	:	Law on Protection of Personal Data No. 6698
Recording Medium	:	Any environment in which personal data are processed, which are fully or partially in automated ways or non-automated ways provided that being part of any data recording system.
Personal Data	:	means any information relating to an identified Personal data is any information that shows the personal, professional and family characteristics of the individual and is suitable for distinguishing that individual from other individuals and revealing their qualifications. This information includes issues such as the identity, ethnicity, physical characteristics, health, education, employment status, sexual life, family life, communication with others, residence address, credit card, personal thoughts and beliefs, association and union memberships, shopping habits etc.

Personal Data Processing Inventory	:	It means the inventory in which the data controllers describe the personal data processing activities they carry out depending on their business processes; the purposes of personal data processing, the legal reason for data processing, the data category, the maximum period they create by associating the transferred recipient group and the data subject group and the measures taken for the purposes for which the personal data are processed, the personal data envisaged to be transferred to foreign countries and the data security.
Processing of the Personal Data	:	Any operation performed on personal data such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system.
Deletion of Personal Data		The process of making personal data inaccessible and unavailable in any way for relevant users.
Disposal of Personal Data		The process of rendering personal data inaccessible, unrecoverable and unusable by anyone in no way.
Board	:	Personal Data Protection Board.
Institution	:	Personal Data Protection Authority.
Sensitive Personal Data -	:	Data on race, ethnicity, political and philosophical views, religion, sect and other beliefs, appearance and attire, association, foundation, or labor union membership, health, sexual life, criminal records, and security measures, along with biometric and genetic data.
Periodic Destruction	:	In the event that all of the conditions for processing personal data specified in the Law disappear, the deletion, destruction or anonymization process to be carried out ex officio at recurring intervals specified in the personal data storage and destruction policy.
Politics	:	Personal Data Retention and Destruction/Disposal Policy
Data Processor	:	A natural or legal person who processes personal data on his behalf on the basis of the authority conferred by the data officer.
Data Registration System	:	Refers to the recording system in which personal data is structured and processed according to certain criteria.

Data Controller	:	The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.
Data Controllers Registry Information System / Abbreviation: VERBIS	:	Refers to the register of data controllers kept by the Presidency of the Personal Data Protection Authority.
Regulation	:	Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28.10.2017.

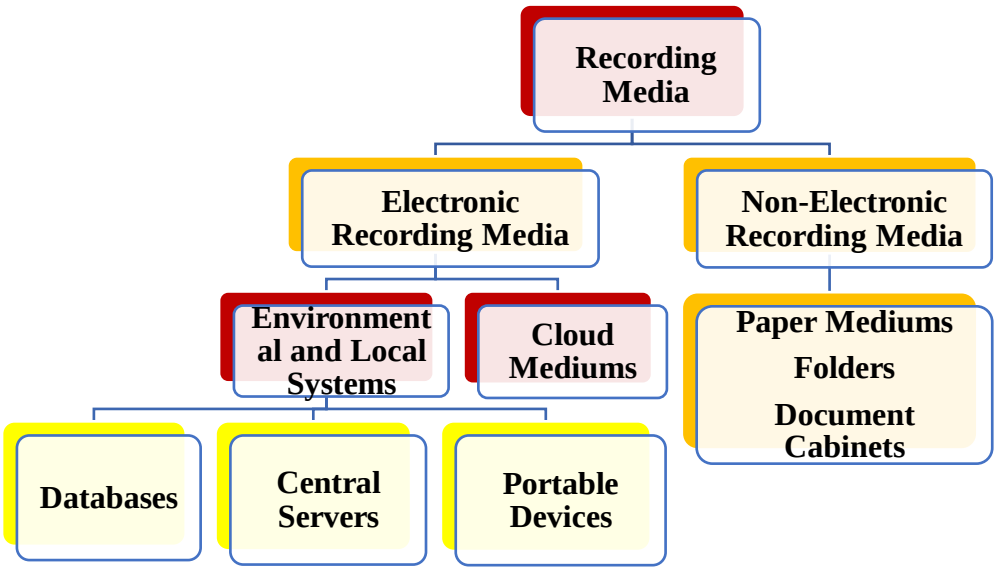
2. DISTRIBUTION OF RESPONSIBILITIES and DUTIES

All CRONIMET employees and their affiliated departments are within the scope of this Policy regarding the processing of personal data and are responsible for the proper implementation of the technical, legal and administrative measures envisaged to be taken in accordance with the Policy, increasing the level of training and awareness of data protection processes, carrying out periodic or random auditing and preventing the unlawful processing of personal data and unlawful access to personal data and ensuring the lawful storage of personal data. All operations regarding the deletion, disposal and anonymization of personal data are recorded and such records are kept for at least 3 (three) years, excluding other legal obligations. In this context, the titles, departments and job descriptions of those involved in the storage and destruction of personal data are as follows:

Title	Department	Task Description
[***]		Responsible for the execution of the policy, its publication, updating, provision and implementation of administrative measures in the relevant environments.
[***]		Responsible for providing and implementing the technical solutions and measures needed in the implementation of the Policy.
[***]		Responsible for the compliance of employees with the policy, supervision and general coordination.

3. RECORDING MEDIUM

CRONIMET keeps the personal data obtained during the execution of its activities within the scope of its commercial and legal regulations and secondary legislation in the electronic and/or non-electronic environments listed below:



4. EXPLANATIONS ON STORAGE AND DISPOSAL OF PERSONAL DATA

Personal data belonging to employees, employee candidates, customers, service providers, suppliers, business partners, visitors and other third parties are stored and destroyed by CRONIMET in accordance with the provisions of the Law and the Regulation on Deletion, Destruction or Anonymization of Personal Data. Legal regulations subject to CRONIMET, secondary legislation and binding opinions and notifications of the Authority are taken into consideration in all storage and disposal processes.

Although CRONIMET aims to store the most up-to-date personal data for the period it processes as a company policy for the shortest possible time and to minimize the stored data as much as possible, CRONIMET, as the data controller, also stores the personal data it processes for certain periods of time, taking into account its legal obligations within the framework of data processing purposes and legal reasons. However, in the case of longer archiving studies carried out for public interest and statistical purposes and for other reasons, it shall take all appropriate technical and administrative measures possible by clearly explaining these reasons. In this case, information on other measures to be taken specific to the incident will be made with a protocol and this protocol containing additional regulations will be considered as an integral part of this policy.

In this context, detailed explanations regarding storage and disposal are given below:

4.1. Explanations Regarding Storage

In Article 3 of the Law, the concept of processing of personal data is defined, in Article 4, it is stated that the processing activity should be related, limited and measured to the purpose for which the processed personal data are processed and should be kept for the period

stipulated in the relevant legislation or for the purpose for which they are processed, and in Articles 5 and 6, the processing conditions of personal data are specified.

4.1.1. Legal Reasons Requiring Storage

Personal data processed within the framework of CRONIMET activities are stored for the period stipulated in the relevant legislation and in this context, personal data are stored based on the following legal reasons:

- Law on Protection of Personal Data No. 6698,
- Turkish Code of Obligations No. 6098,
- Social Security and General Health Insurance Law No. 5510,
- Occupational Health and Safety Law No. 6331,
- Labour Law No. 4857,
- Regulation on Health and Safety Measures to be Taken in Workplace Building and Extensions
- Law No. 5651 on Regulating Internet Broadcasting and Combating Crimes Committed Through Internet Broadcasting,
- Regulation on Facilitation of Customs Procedures
- It is clearly stipulated in the provisions of other secondary regulations in force in accordance with the above-mentioned legal regulations and other legislation, including but not limited to such provisions,
- By CRONIMET, provided that it is directly related to the establishment or performance of the contracts to which it is a party,
- It is mandatory for CRONIMET to fulfill its legal obligation,
- In the event that personal data is revealed to the public by the person concerned himself/herself,
- In the event that data processing is obligatory for the establishment, use or protection of a right,
- Provided that it does not harm the fundamental rights and freedoms of the relevant person, it is an obligation to process data for legitimate interests of CRONIMET.

4.1.2. Processing Purposes Requiring Storage

Personal data processed within the framework of CRONIMET activities detailed above are processed limited to the following purposes:

- Carrying out human resources processes,
- Providing corporate communication,
- Ensuring workplace safety,
- To be able to perform work and transactions as a result of contracts and protocols signed,
- To ensure that our legal obligations are fulfilled as required or mandated by legal regulations,
- Liaising with real/legal persons in business relationship with CRONIMET,
- Performing the works and transactions/practices that it is legally obliged to perform,
- Fulfilling the burden of proof for possible legal disputes

Personal data are processed for their purposes and during the processing, the Law and secondary legislation are taken into consideration.

4.2. Reasons for Destruction/Disposal

Personal data:

- Amendment or relevance of the provisions of the relevant legislation constituting the basis for its processing,
- Absence of the purpose that requires processing or storage,
- If the processed data loses its up-to-dateness, loses its accuracy,
- In cases where the processing of personal data takes place only in accordance with the explicit consent condition, the relevant person's withdrawal of his/her consent,
- Pursuant to Article 11 of the Law, the application made by CRONIMET regarding the deletion and destruction of the personal data of the person concerned within the framework of his/her rights is accepted,
- In the event that the application made by CRONIMET with the request of deletion, destruction or anonymization of the personal data of the relevant person is rejected, the relevant person finds the answer inadequate or does not respond within the period stipulated in the Law; filing a complaint to the Board and this request is approved by the Board,
- In cases where the maximum period requiring the storage of personal data has passed and there is no condition to justify the storage of personal data for a longer period, CRONIMET deletes, destroys or anonymizes the personal data upon the request of the relevant person or ex officio.

At the end of the period stipulated in the relevant legislation or the storage period required for the purpose for which they are processed, personal data are destroyed by CRONIMET ex officio and/or upon the application of the relevant person to CRONIMET with the use of following techniques.

4.3. Personal Data Disposal Methods

4.3.1. Deletion of Personal Data

Personal data processed by CRONIMET are deleted as follows:

Data storage medium	Description
a. Electronic Recording Media – **Environmental and Local Systems** – **Cloud Mediums**	○ **Those** whose retention period from personal data in electronic environment expires are made inaccessible andunusable in any way for other employees (relevant users) who are authorized to access the database except for the database administrator. ○ The system administrator revokes the access authorization of the relevant users and deletes the personal data on the servers and the storage period expires. ○ Personal data stored in flash-based storage environments and whose storage period expires are encrypted by the system administrator and access authority is given only to the system

	administrator and stored in secure environments with encryption keys.
b. Non-Electronic Recording Media	Personal data kept in the physical environment and expired by the storage period are made inaccessible and unavailable to employees in any way. In addition, the blackout process is also applied by scratching/ painting/wiping in a way that cannot be read.
* * * CRONIMET *may use one or more of the abovementioned deletion methods, may develop new deletion methods if different storage media are used, may use newly developed deletion methods in addition to existing methods or together with these methods.*	

4.3.2. Destruction / disposal of Personal Data

Personal data processed by CRONIMET are destroyed as follows:

Data storage medium	Description
a. Electronic Recording Media – **Environmental and Local Systems** – **Cloud Mediums**	**Physical Destruction Method** It is the process of physical destruction of optical and magnetic media containing personal data, in ways and means such as melting, burning or pulverizing. Data is made inaccessible by processes such as melting, burning, pulverizing or passing optical or magnetic media through a metal grinder. **De-Magnetization (Degauss)** By exposing the magnetic media to a high magnetic field, it is ensured that the data on it becomes unreadable and re-readable. **Override** Reading and recovering old data is prevented by writing random data consisting of 0's and 1's at least seven times on magnetic media and rewritable optical media. **Securely Deleting Personal Data From Software** Personal data held in the cloud environment is deleted by digital command in a way that cannot be recovered again, and when the cloud computing service relationship ends, all copies of the encryption keys necessary to make personal data available are destroyed. The data deleted in this way cannot be accessed again.

b. Non-Electronic Paper Media	Those whose period of time required to be stored from personal data in the paper environment has expired are irreversibly destroyed in paper trimmers (sheddar).
* * * CRONIMET *may use one or more of the above-mentioned disposal methods, may develop new disposal methods if different storage media are used, may use newly developed disposal methods in addition to existing methods or together with these methods.*	

4.3.3. Anonymization of Personal Data

Anonymization of personal data means making personal data unlikely to be associated with any identifiable real person in any way even when personal data is paired with other data. In order for personal data to be anonymized; Personal data must be rendered unrelated to an identified or identifiable natural person, even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of personal data by the data controller or third parties and / or matching the data with other data.

CRONIMET may use one or more of the following anonymization methods and may use K-Anonymity [UN2] (K-Anonymity), L-Diversity [UN3] and T-Closeness [UN4] (T-Closeness) statistical methods when using these anonymization methods:

Lower and Upper Limit Coding/ Global Coding	:	For a particular variable, the intervals of that variable are defined and categorized. If the variable does not contain a numerical value, then close data within the variable is categorized. The values within the same category are combined.
Regional Hide	:	It is the process of deleting information that may be distinctive regarding the data in the data table where the personal data is collectively anonymized.
Removing Variables	:	It is the removal of one or more of the direct identifiers included in the personal data of the person concerned and used to identify the person concerned in any way.
Generalization.	:	It is the process of gathering personal data belonging to many people and making them statistical data by removing their distinctive information.
Micro Merge	:	With this method, all records in the dataset are first arranged in a meaningful/ tangible order and then the whole set is divided into a certain number of sub-sets.

		Then, the value of the determined variable of each sub-set is averaged and the value of that variable of this subset is changed with the average value. In this way, since the indirect identifiers in the data will be corrupted, it is difficult to associate the data with the relevant person.
Data Mixing and Disruption	:	The direct or indirect identifiers in the personal data are confused or distorted with other values, their relationship with the relevant person is broken and they are ensured to lose their descriptive qualities.

5. STORAGE and DISPOSAL PERIODS and METHOD

Without prejudice to the fact that a longer period is regulated in the law and/or related legislation and secondary regulations or a longer period is foreseen for statute of limitations, deprivation of rights, storage periods and similar reasons, the personal data processed by CRONIMET are stored with the methods and periods specified in the Storage and Disposal Table attached to this policy and are destroyed by the methods specified at the end of the storage periods (CRONIMET reserves the right to use different disposal methods, provided that it is not limited to the listed destruction methods.). *(See **Annex- Storage and Disposal Table**)*

6. Periodic destruction period

Within the scope of the provisions of the Regulation on the Deletion, Destruction/Disposal or Anonymization of Personal Data, CRONIMET deletes, destroys/disposes or anonymizes the personal data whose processing conditions have disappeared in the event that all the conditions for processing the personal data in the Law have disappeared, with a process to be carried out ex officio at repeated intervals specified in this Personal Data Storage and Destruction/Disposal Policy. Periodic destruction processes are repeated every **6 (six) months** in June and December each year.

7. TECHNICAL and ADMINISTRATIVE MEASURES

In accordance with the Law, it is essential that CRONIMET takes the technical and administrative measures announced as the necessity of the Retention and Destruction Processes in a structured, updated, effective and accountable manner in order to prevent the secure storage and unlawful processing of personal data and/or unlawful access to these personal data.

7.1. Technical Measures

The technical measures taken in relation to personal data processed by CRONIMET are listed below:

- With leakage (penetration) tests, the risks, threats, vulnerabilities and gaps, if any, against CRONIMET information systems are identified and necessary measures are taken.

- As a result of real-time analyzes with information security incident management, risks and threats that will affect the continuity of information systems are constantly monitored.
- Access to information systems and authorization of users are carried out through security policies through the access and authorization matrix and the corporate active directory.
- Necessary measures are taken for the physical security of CRONIMET information systems equipment, software and data.
- In order to ensure the security of information systems against environmental threats, hardware (access control system that allows only authorized personnel to enter the system room, 24/7 monitoring system, ensuring the physical security of the edge switches that make up the local area network, fire extinguishing system, air conditioning system, etc.) and software (firewalls, attack prevention systems, network access control, systems that prevent harmful software, etc.) measures are taken.
- Risks to prevent unlawful processing of personal data are identified, technical measures are taken in accordance with these risks and technical checks are made for the measures taken.
- Access procedures are created in CRONIMET and reporting and analysis studies are carried out regarding access to personal data.
- Access to storage areas where personal data is stored is recorded and inappropriate access or access attempts are kept under control.
- CRONIMET takes the necessary technical measures to ensure that the deleted personal data are not accessible and reusable for the relevant users.
- In the event that personal data are obtained illegally by others, a suitable system and infrastructure have been established by CRONIMET to notify this situation to the relevant person and the Board, and the responsible persons within CRONIMET regarding these notifications have been determined.
- Security vulnerabilities are monitored and appropriate security patches are installed, and information systems are kept up-to-date.
- Strong passwords are used in electronic environments where personal data are processed.
- Secure record keeping (logging) systems are used in electronic environments where personal data are processed.
- Data backup programs are used that ensure the safe storage of personal data.
- Access to personal data stored in electronic or non-electronic media is restricted according to access principles.
- A separate policy has been determined for the security of sensitive personal data.
- Sensitive personal data security training has been provided for employees involved in the processing of sensitive personal data, confidentiality agreements have been made, and the authorities of users with access to data have been defined.
- Electronic environments where sensitive personal data is processed, stored and/or accessed are stored using cryptographic methods, cryptographic keys are kept in secure environments, all transaction records are logged, security updates of the environments are constantly monitored, necessary security tests are regularly performed / performed, test results are recorded,

- Adequate security measures are taken in the physical environments where sensitive personal data are processed, stored, and/or accessed and physical security prevents any unauthorized entry or access.
- If sensitive personal data needs to be transferred via e-mail, it is transferred encrypted via corporate e-mail address or using Kep account.
- If it needs to be transferred through media such as portable memory, CD, DVD, it is encrypted by cryptographic methods and the cryptographic key is kept in different media.
- In case of transfer between servers in different physical medium, data transfer is performed by establishing VPN between servers or by using sFTP method,
- If it is necessary to transfer the document through paper media (hardcopy), necessary measures are taken against risks such as theft, loss or unauthorized viewing of the document and the document is sent in a "confidential/classified" format.

7.2. Administrative Measures

The administrative measures taken regarding the personal data processed by CRONIMET are listed below:

- Trainings are provided to increase the awareness of employees on the subject and to contribute to their professional development, to increase their technical knowledge skills, to prevent unlawful processing of personal data, to prevent unlawful access to personal data, and to ensure that personal data are protected in accordance with the law.
- In relation to the activities carried out by CRONIMET, employees are required to sign confidentiality agreements containing deterrent criminal sanctions, which are prepared by taking into account their job description, experience, competence on the subject and effectiveness in management and governance.
- A disciplinary procedure has been prepared for employees who do not comply with security policies and procedures.
- Before starting to process personal data, CRONIMET fulfills its obligation to inform the relevant persons in accordance with the conditions required by the Law.
- Personal data processing inventory has been prepared.
- Periodic and random audits are carried out within the company.
- Information security trainings are provided for employees.

8. PUBLICATION and STORAGE

The policy is published in two different media, wet signed (printed paper) and electronic. Printed paper copy is also stored in the IT Department file.

9. UPDATE PERIOD

When the policy is needed and probably once every 6 (six) months, it is reviewed in June and December each year and the necessary sections are updated.

10. ENFORCEMENT

The policy shall be deemed to have entered into force on [* * *] and if it is decided to repeal or change it, it shall be canceled with the decision of the Board of Directors (by making a red cancellation stamp or writing cancellation) and its new form shall be signed and published

on the website. The new version enters into force to be published on the website upon the decision of the board of directors.

CRONIMET TURKEY METAL TİCARET A.Ş. Board

[***] [***] [***]

[UN1] – *If there are other media used, it is necessary to determine them and if there is an environment specified here but not used, they should be removed from here.*

[UN2] – *In anonymized datasets, if the indirect identifiers were combined with the correct combinations, the identifiers of the persons in the records were identifiable or the information about a particular person became easily predictable, which undermined the confidence in the anonymization processes and accordingly, the anonymized datasets had to be made more reliable by various statistical methods.*

[K-Anonymity] – *It has been developed to prevent the disclosure of information specific to individuals with singular characteristics in certain combinations by enabling identification of more than one person with specific fields in a dataset. If there is more than one record of combinations created by combining some of the variables in a dataset, the possibility of identifying the people corresponding to this combination decreases.*

[UN3] – *The L-Diversity method, which is formed by studies conducted on the deficiencies of anonymity, takes into account the diversity of sensitive variables corresponding to the same combinations of variables.*

[UN4] – *Although the diversity method provides diversity in personal data, there are situations in which the said method does not provide sufficient protection because it does not deal with the content and degree of sensitivity of personal data. As such, the process of calculating the degree of intimacy of personal data and values within themselves and anonymizing the data set by dividing it into subclasses according to these intimacy degrees is called the T-Closeness method.*

STORAGE AND DISPOSAL TABLE

	Data Processing Activity /Document	Data Category	Recording Medium	Storage Method	Storage Purpose	Storage Duration	Disposal Method	Disposal Period
1st	Resumes	Name, surname, TR ID, Address, e-mail, telephone, date of birth, gender, marital status, photo, educational information, work experiences	Non-Electronic	Computer, m	Managing job application processes of employee candidates	2 years	Deleting files	At the first periodic destruction following the end of the storage period
			Non-Electronic -	Hardcopy			Paper disposal or cropping machines	
2.	Employee Personal File Document	Name, surname, TR ID, Address, e-mail, telephone, date of birth, gender, marital status, photo, educational information, professional experience, information of dependent persons, salary information, criminal record, health report, permission information.	Electronic	Computer, email	Fulfillment of obligations arising from employment contract and legislation and employment contract for employees, benefits and benefits processes for employees execution, planning of human resources processes, execution/ supervision of work activities, execution of occupational health/ safety activities	10 years following the end of business relationship	Deleting files	At the first periodic destruction following the end of the storage period
			Non-Electronic -	Non-Electronic -			Paper disposal or cropping machines	
3.	Contracts	Customer/supplier/business partner name surname, TR ID number, tax ID number, address, contact information, IBAN number, signature circular, legal transaction information	Electronic	Database, Computer	Fulfillment of contractual obligations, execution of supply chain management processes, proper performance of payment services, execution of after-sales support services, execution of customer relationship management processes, execution of storage and archive activities	10 years following the termination of the contract	Deleting files	At the first periodic destruction following the end of the storage period
			Non-Electronic -	Non-Electronic -			Paper disposal or cropping machines	
4.	Information and Documents of Shareholders	Identity information, contact information, professional experience, legal transaction information, financial information	Electronic	Database, Computer	Conducting management activities, informing authorized persons, institutions and organizations, following up and conducting legal affairs, conducting financial and accounting affairs, conducting internal audit/ investigation /intelligence activities	10 years following the end of business relationship	Deleting files	At the first periodic destruction following the end of the storage period
			Non-Electronic -	Paper media, folders			Paper disposal or cropping machines	
5.	Accounting Document	Invoices, receipts, payment records,	Electronic	Database Computer, Software	Execution of management activities, fulfillment of financial obligations, fulfillment of obligations arising from BRSA legislation, follow-up of transaction records	10 years following the end of relevant work/ activity -	Trust from software	At the first periodic destruction following the end of the storage period
			Non-Electronic -	Paper media, folders			Paper disposal or cropping machines	
6.	General Assembly and Board of Directors Transactions	Minutes of the General Assembly, resolutions of the Board of Directors, circular of signatures, power of attorney, list of attendance	Electronic	Database, Computer	Carrying out the management activities of the company, taking internal decisions, fulfilling the obligations arising from the companies and tax law legislation	As long as the company continues	Deleting files	At the first periodic destruction following the end of the storage period
			Non-Electronic -	Paper media, folders			Paper shredding or clipping machines, by scratching method	
7.	Potential Product/Service Recipient Information, Business card,	Identity information, contact information	Non-Electronic -	Closet, physical file	Conducting communication activities, conducting marketing processes of products/ services, conducting advertising/ campaign/ promotion processes	5 years	Paper disposal or cropping machines	At the first periodic destruction following the end of the storage period