“KORUMA KLOR ALKALİ SANAYİ VE TİCARET ANONİM ŞİRKETİ”

POLICY ON PERSONAL DATA STORAGE AND DEMOLITION

09.12.2019

INDEX

1. PREAMBLE 3

2. PURPOSE OF THE POLICY 3

3. SCOPE OF THE POLICY 3

4. DEFINITIONS 3

5. REGISTRY MEDIUMS 5

6. REASONS REQUIRING PERSONAL DATA STORAGE AND DEMOLITION 5

7. SECURITY OF PERSONAL DATA 6

8. DEMOLITION OF PERSONAL DATA 7

8.1. Reasons Requiring Demolition of Personal Data 7

8.2 Erasure of Personal Data 7

8.3 Destruction of Personal Data 8

8.4 Anonymization of Personal Data 8

8.5 Personnel in charge of Personal Data Storage and Demolition 9

8.6. Personal Data Categories 9

8.7. Person Group Related to Personal Data 11

8.8. Personal Data Category and Person Group Matching 12

8.9. Storage and Demolition Periods 13

8.10 Periodical Demolition Process 17

1. PREAMBLE

"KORUMA KLOR ALKALİ SANAYİ VE TİCARET ANONİM ŞİRKETİ" *(Hereinafter referred to as "Company")* places great importance on personal data protection. We show sensitivity in protection of personal data of our partners, customers, employees, candidate employees, company officials, employees of affiliates, company employees that we work together, shareholders, officers, visitors and third parties. *"Policy on Personal Data Protection"* displaying the principles adopted by the Company on processing and protection of personal data, is submitted for the relevant parties' information on the website.

2. PURPOSE OF THE POLICY

The Policy on Personal Data Storage and Demolition Policy (Hereinafter referred to as "Demolition Policy") determines the principles and procedures in relation to the security and erasure, destruction and anonymization of personal data, which are processed during the various proceedings within the body of our Company.

3. SCOPE OF THE POLICY

This Demolition Policy includes any personal data of our partners, customers, employees, candidate employees, company officials, employees of affiliates, company employees that we work together, shareholders, officers, visitors and third parties processed wholly or partly in automatic or non-automatic ways (on condition that it is a part of any data registry system).

4. DEFINITIONS

In this Policy;

a. **Explicit Consent:** means freely given, specific and informed consent,
b. **Anonymizing:** means rendering personal data impossible to link with an identified or identifiable natural person, in any manner including matching them with other data,
c. **Data subject:** means the natural person, whose personal data is processed,
d. **Relevant user:** means people processing personal data within the body of the organization of data controller or in accordance with the authority and instruction

given by the data controller apart from person or unit being responsible for technically storage, protection and backup of data,

e. **Demolition:** means erasure, destruction and anonymization of personal data,
f. **Law:** means the Law on Personal Data Protection No. 6698 dated 24 March 2016
g. **Registry Medium:** means any medium where personal data, which is processed wholly or partly in automatic or non-automatic ways (on condition that it is a part of any data registry system), exists,
h. **Personal data:** means all the information relating to an identified or identifiable natural

person,

i. **Processing of personal data:** means any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,
j. **Personal data processing inventory:** means an inventory that data controllers creates their personal data processing activities based on business process by linking with personal data processing purposes, data category, recipient group and data subject group, and that they explain and detail the period necessary for the purposes of personal data processing, personal data stipulated to be transferred to foreign countries and the measures taken for the data security,
k. **Policy on personal data storage and demolition:** means the policy that data controllers use as a base for determining the maximum period necessary for the purpose of processing of personal data, and for erasure, destruction and anonymization,
l. **Board:** means the Personal Data Protection Board,
m. **Authority:** the Personal Data Protection Authority,
n. **Periodical demolition:** means the transactions of erasure, destruction or anonymization that might be performed ex officio at repeating intervals stated in the policy on personal data storage and demolition in case all of the conditions of personal data processing set forth in the Law are abated,

o. **Registry:** means data controllers' registry kept by the Directorate of the Personal Data Protection Authority,

p. **Processor:** means the natural or legal person who processes personal data on behalf of the controller upon his authorization,

q. **Data registry system:** means the registry system which the personal data is registered into through being structured according to certain criteria,

r. **Controller:** means the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

As to the definitions that are not stated herein, the definitions set forth in the law and regulations shall apply.

5. REGISTRY MEDIUMS

Registry mediums where the company keeps personal data are the computers being used on behalf of the company, programs such as J-HR, LOGO, Mikado, Cloud Systems, shared/unshared disk drivers used for data storage over the network, paper, unit cabinets, and archive. The Company will include other registry mediums that it may use to the Demolition Policy in addition to the mentioned registry mediums.

6. REASONS REQUIRING PERSONAL DATA STORAGE AND DEMOLITION

The Company may process your data in case of existence of one or some of the following conditions;

- Explicit consent of data subject,
- It is clearly stipulated under the Laws, explicit consent could not be taken due to actual impossibility, it is directly related to the establishment or execution of a contract,
- It is mandatory for the Company to fulfill its legal obligation,
- It is made public by data subject,
- It is mandatory in order to establish, exercise or protect a right,

- It is mandatory for the legitimate interest of the Company

You may review the Policy on Personal Data Protection being available at www.koruma.com address in order to obtain detailed information about the processing of personal data.

Data subjects' personal data is demolished during the first periodical demolition to be made once the abovementioned reasons of processing of personal data are abated. All transactions in relation to erasure, destruction and anonymization of personal data are recorded and the aforesaid records are kept at least three years.

7. SECURITY OF PERSONAL DATA

The Company takes the necessary technical and organizational measures of any kind for providing the appropriate security level in order to prevent unlawful processing of personal data and unlawful access to personal data, and to preserve personal data.

Within this scope, first of all, our Company performed a study in relation to the determination of what the processed personal data is, and then determined the risks which may arise concerning the protection of such data by taking into account that whether the processed personal data is a special-quality data, and the necessary technical and organizational measures for minimizing or eliminating the risks have been put into practice.

In order to provide the security of personal data, the personnel and managers are being provided trainings in an attempt to prevent personal data from being explained and shared unlawfully and to create awareness in relation to the Law on Personal Data Protection.

Furthermore, the employees getting involved in personal data processing are requested to sign confidentiality agreements as a part of their employment process, and the necessary discipline process is carried out in case it is determined that the employees have acted in contrary to the security policies and procedures.

Personal data included in the data processing by the company have been limited for access on personnel basis, and the limited number of personnel has been granted authority to access personal data, which relates to the business process that they carry out. Data processing carried out by the personnel is recorded. All across the company, as to the personal data

processing, we take care to abide by the principle of "Everything is forbidden unless permitted".

In order to prevent unlawful processing of personal data and unlawful access to personal data, technical systems have been established with a view to follow-up and audit of processes in relation to processing of personal data. Regular internal audits have been carried out in order to prevent unlawful processing of personal data and unlawful access to personal data.

With the intention of preventing unlawful access to personal data and preserving such data in secure medium, technical methods having appropriate security levels are being used, and the aforesaid methods are being updated in compliance with the developing technology.

In case of any attack inside or outside to the data registry system of the company, in order to recognize this situation early and to provide early intervention, which software and services works at information networks and whether there is any leakage or any action, which should not happen, are being checked regularly, transaction activities of all users are kept on a regular basis.

8. DEMOLITION OF PERSONAL DATA

8.1. Reasons Requiring Demolition of Personal Data

Despite being processed in compliance with the legal legislation, the Company erase, destruct or anonymize personal data ex officio or upon demand by the data subject, upon disappearance of reasons which require the process or the period stipulated under the legislation expires.

The Company chooses the most appropriate methods of demolition of personal data among erasure, destruction or anonymization, and takes all necessary technical and organizational measures to erase, destruct or anonymize the personal data in compliance with the law.

8.2. Erasure of Personal Data

Erasure of personal data means making the personal data inaccessible and non-reusable for the relevant users in any manner. The Company takes all necessary technical and

organizational measures in order to make the erased personal data in accessible and non-reusable for the relevant users.

During the process of erasure of personal data, personal data being subject of the erasure is determined, the relevant users having authority to access to the aforesaid personal data and such authorities on the personal data are determined, and the relevant users' authorities to access, recover and re-use the aforesaid data are removed.

Personal data being available as papers, are erased by using darkening method. Darkening method means making personal data on the relevant document invisible for the relevant users by using marking ink or by cutting in a way that cannot be recovered and read in technological analysis.

In databases where personal data is available, the relevant lines where personal data is available are erased with database commands (Delete etc.), and as to the personal data being available at file operating system, personal data is erased through delete commands of the file in the operating system or it is erased by removing the relevant users' access rights in the file or index where the file is available.

8.3. Destruction of Personal Data

Destruction of personal data means making personal data inaccessible, irrecoverable and non-reusable for everyone in any manner. The Company takes all necessary technical and organizational measures in relation to the destruction of personal data.

In order to destruct personal data, all copies of data are determined, and according to the type of system where data is available, demagnetizing, fusing, burning or powdering or grinding through a metal grinder optic media and magnetic media for data including magnetic media, and burning for data being available as papers.

8.4. Anonymization of Personal Data

Anonymization of personal data is making personal data impossible to link with an identified or identifiable natural person, in any manner including matching them with other data.

The purpose of anonymizing of personal data is to break the connection between data and a person defined by this data. The methods such as grouping, masking, reproducing, generalizing and making random in automatic or non-automatic ways applicable to records in data registry system where personal data is kept, are among the methods of anonymization.

8.5 Personnel in charge of Personal Data Storage and Demolition

Title	Duty	Responsibility
Personal Data Protection Officer	Compliance with the Law on Personal Data Protection, Responsible for implementing Personal Data Storage and Demolition	All across the company, compliance with the Law on Personal Data Protection, secondary legislation and Board resolutions and audit, providing compliance with the Policy on Personal Data Storage and Demolition and managing personal data demolition process in accordance with periodical demolition periods.
Information Technology Officer	Responsible for implementing Personal Data Storage and Demolition	In relation to the process within the scope of its duties, providing compliance with the Policy on Personal Data Storage and Demolition and managing personal data demolition process in accordance with periodical demolition periods.
Human Resources Officer	Responsible for implementing Personal Data Storage and Demolition	In relation to the process within the scope of its duties, providing compliance with the Policy on Personal Data Storage and Demolition and managing personal data demolition process in accordance with periodical demolition periods.

8.6. Personal Data Categories

Personal Data Category	Personal Data Category Definition
Identification Data	means the data including real person's identification information. Identity card including information such as TR Identification number, mother-father name, date of birth, place of birth, marital status, gender, driving license, passport, professional card, tax number, signature information, Social Security Institution number and other data
Contact Information	Telephone number, e-mail address, address, fax number, IP address and other data

Education Information	Alma mater, diploma, course, seminar, conference attendance certificate, exam results, foreign language and other data
Medical Information	Blood type, medical examination by on-site doctor, vaccination card, health certificate of any kind
Candidate Employee Information	Personal data obtained through curriculum vitae and job application forms by the company during job application process (identification and contact information, nationality, health, criminal status and safety measures information, military service status, education and work experiences, certificates, fields of interests, references, marital status, family and relatives information, foreign language information, private vehicle information, driver's license status, real estate status (rent-ownership), type of application to the company, salary from the last employment
Employee Information	Data that must be included in the personal file of employees as required by the law and data constituting employee personal rights (Copy of identity card, identity register copy (e-government and civil registry), certificate of settlement and other address details (e-government), criminal record (e-government), copy of diploma, blood type card, copy of driving license, copy of marriage certificate, copy of identity card of spouse and children, copy of military service discharge certificate, photo, copy of bank book, copy of former education and seminars, tetanus vaccination card, hemogram (blood count), urinalysis, audiometry, lung diagram 35x35, pulmonary function test, fasting blood glucose and electrocardiogram for motorcycle courier, src3 certificate for drivers (international freight shipment) and/or src4 certificate (national freight shipment), psychotechnics certificate for drivers)
Special Quality Personal Data	Individual's race, ethnic origin, political thought, philosophic belief, religion, sect or other beliefs, appearance, membership to association, foundation or union, health, sexual life, criminal status and data in relation to security measures, and biometric and genetic data.

Legal Action Information	Data processed for the protection of rights and claims of the company, collection of debts, execution of obligations and legal liabilities
Financial Information	Bank account number and account details, documents showing financial status, salary and payroll details, private health insurance amount, premium details and other data
Physical Environment Security Information	Camera records while entering into and within the building and facilities of the company, license plate details, records at security points
Family Members and Relatives Information	Data concerning the data subject' family members (spouse, mother, father and child), relatives and emergency contacts
Location Information	GPS data detecting the location of person using the vehicle of the company

8.7. Person Group Related to Personal Data

Person Group	Person Group Definition
Employees of Company, Affiliates and Business Partners, Intern	All real persons including the employees of our company and affiliates, and shareholders and officers working at legal entities and real persons with whom our company has a business relation
Candidate Employee, Candidate Trainee Employee	Real person applying to our company in any way or submitting its curriculum vitae for review
Company Partners	Real persons being partner of the Company
Customers of the Company, Person receiving Goods or Services	Real persons benefiting from goods and services provided by our Company
Authorized Person	Authorized person working at the relevant public/private institution
Potential person receiving Goods or Services	Real persons requesting to benefit from goods and services provided by our company
Visitor	Real persons visiting building, facility and website of the Company
Supplier	Parties providing services in compliance with orders and instruction and based on a contract in order to carry out the commercial activities of the Company
Employees of Supplier	Employees working at supplier companies having a commercial relation with our Company
Affiliates	Koruma Temizlik Anonim Şirketi, İzmit Sakarya Nakliyat Kimya Gıda ve Hayvancılık Sanayi Ticaret Limited Şirketi

Business Partners	Parties that the Company establishes a business partnership in order to carry out its commercial activities
Legally Authorized Institutions and Organizations and Private Law Legal Entities	As per the provisions of relevant legislation, legally authorized institutions and organizations and private law legal entities that the Company is obliged to share information and document
Sub-employer	Persons being in the capacity of employer, undertaking a work at some part and addition of a work of the Company and employing workers on their own behalf at this workplace and its additions
Employees of Sub-employer	Employees of sub-employer having a commercial relation with our Company

8.8. Personal Data Category and Person Group Matching

Personal Data Category	Person Group
Identification Data	Employees of Company, Affiliates and Business Partners, Candidate Employees, Company Partners, Customers of Company, Potential Customers of Company, Visitor, Supplier, Business Partners, Company Official, Intern
Contact Information	Employees of Company, Employees of Affiliates and Business Partners, Candidate Employee, Company Partners, Customers of Company, Potential Customers of Company, Visitor, Supplier, Business Partner, Company Official, Intern
Education Information	Employees of Company, Affiliates and Business Partners, Candidate Employees, Company Partners, Customers of Company, Potential Customers of Company, Visitor, Supplier, Business Partners, Company Official, Intern
Medical Information	Company, Affiliates and Business Partners, Their Employees, Candidate Employees, Company Partners, Company Official, Intern
Candidate Employee Information	Candidate Employee

Employee Information	Employees of Company, Company Official, Intern
Special Quality Personal Data	Employees of Company, Affiliates and Business Partners, Candidate Employees, Company Partners, Customers of Company, Potential Customers of Company, Visitor, Supplier, Business Partners, Company Official, Intern
Legal Action Information	Employees of Company, Affiliates and Business Partners, Company Partners, Customers of Company, Potential Customers of Company, Supplier, Company Official, Intern
Financial Information	Employees of Company, Affiliates and Business Partners, Candidate Employee, Company Partners, Customers of Company, Potential Customers of Company, Supplier, Business Partners, Company Official
Physical Environment Security Information	Employees of Company, Affiliates and Business Partners, Candidate Employees, Company Partners, Customers of Company, Potential Customers of Company, Visitor, Supplier, Business Partners, Company Official, Intern
Location Information	Employees of Company, Affiliates and Business Partners, Company Official

8.9. Storage and Demolition Periods

Work Process	Person Group	Personal Data Category	Storage Period	Demolition Period
Advance Payment to Employees	Employees of Company	Identification Data, Contact Information, Financial Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Payment Transactions	Person receiving goods or services, Suppliers	Identification Data, Contact Information, Financial Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period
Legal Process	Person receiving goods or services	Identification Data, Contact Information, Financial Information, Customer Transaction Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period
Letter of Guarantee	Person receiving goods or services	Identification Data, Contact Information, Financial Information	10 years after termination of relation	Within 180 days following the expiry of storage period

Receiving Process				
Customer Portfolio Creating Process	Potential person receiving goods or services (Customer)	Identification Data, Contact Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period
Access to Internet and Electronic Mail Account Process	Employees of Company, Visitors	Identification Data, Contact Information	2 years	Within 180 days following the expiry of storage period
System Account Defining Process	Employees of Company, Business Partners	Identification Data, Contact Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period
Information System Devices Allocation Process	Employees of Company	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Personnel List and Contact Persons Determination Process	Employees of Company	Identification Data, Contact Information, Health Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period
Keeping Visitors Records	Visitors, Suppliers	Identification Data, Physical Environment Security Information	1 month	Within 180 days following the expiry of storage period
Keeping Shift List	Employees of Company	Identification Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Conducting Performance Assessment Process	Employees of Company	Identification Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Quality Management Process	Employees of Company	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Export Consignments	Person receiving goods or services	Identification Data, Contact Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period

Sending Customer Greeting Card Process	Person receiving goods or services	Identification Data, Contact Information	10 years	Within 180 days following the expiry of storage period
Customer Portfolio Creating Process	Potential person receiving goods or services (Customer)	Identification Data, Contact Information	10 years as of termination of contractual relation	Within 180 days following the expiry of storage period
Process of Process Documents	Employees of Company, Company Officials	Identification Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Data Entry to Public Institutions Process	Employees of Company, Company Officials	Identification Data, Contact Information, Financial Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Shared Information for Events Process	Employees of Company	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Visa-Reservation Process	Employees of Company	Identification Data, Special Quality Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Incentive Notice Process	Employees of Company	Identification Data, Contact Information, Education Information, Employee Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Public-Supported Project Management Process	Employees of Company	Identification Data, Contact Information, Education Information, Employee Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Taking and Assessing Advices for Recovery of Business Process, Conducting/Auditing Business Activities	Employees of Supplier	Identification Data, Contact Information, Professional Experience Information, Education Information	1 year as of termination of contractual relation	Within 180 days following the expiry of storage period
Business Card Creating Process	Employees of supplier, Business Partners, Authorized Person of Supplier, Person receiving goods or services	Identification Data, Contact Information	1 year	Within 180 days following the expiry of storage period
Conducting Contract Process	Employees of Supplier, Authorized People of Supplier	Identification Data, Contact Information, Financial Information	10 years after termination of contractual relation	Within 180 days following the expiry of storage period
Employment Procedure	Employees of Company, Interns	Employee Information	10 years after leave of employment	Within 180 days following the expiry of storage period
Recruitment Process	Candidate Employee, Candidate Intern Employee	Identification Data, Contact Information, Professional Experience, Health Information, Criminal	2 years	Within 180 days following the expiry of storage period

		Status and Security Measures		
Education Process	Employees of Company, Interns	Identification Data, Education Information, Professional Experience Information, Health Information, Financial Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Switchboard Process	Visitors, Person receiving goods or services, Potential Customers of Company, Suppliers	Identification Data, Contact Information	1 year	Within 180 days following the expiry of storage period
Creating Visitors' Records Process	Visitors, Employees of Company, Employees of Supplier+E32:E49	Identification Data, Physical Environment Security Information and Contact Information	1 year	Within 180 days following the expiry of storage period
Legal Processes	Employees of Company, Company Partners, Company Official	Identification Data, Legal Action Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Communicatio n Process	Employees of person receiving goods or services, employees of Company	Identification Data, Contact Information	2 years	Within 180 days following the expiry of storage period
Visa-Reservati on Process	Employees of Company	Identification Data, Contact Information	10 years	Within 180 days following the expiry of storage period
Operation of Business Process	Employees of Company	Identification Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Payroll Process	Employees of Company	Identification Data, Employee Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Payroll Allocation Process	Employees of Company	Identification Data, Employee Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Making/Renew ing Insurance Process	Employees of Company	Identification Data, Financial Information, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Conducting and Auditing of Business Activities	Employees of Company	Identification Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Giving Meal Card Process	Employees of Company	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Performing Internal Announcement Process	Employees of Company	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Conducting Education and Audit Activities	Business Partners	Identification Data, Education Information, Professional Experience	2 years	Within 180 days following the expiry of storage period

		Information, Contact Information		
Social Media Management Process	Employees of Company, Company Partners, Company Official, Visitors	Identification Data, Visual and audial records	2 years	Within 180 days following the expiry of storage period
Commodity Debit in the name of Employees	Employees of Company	Identification Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Occupational Health and Safety Process	Employees of Company	Identification Data, Contact Information, Health Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Polyclinic Registry Book	Employees of Company	Identification Data	10 years as of leave of employment	Within 180 days following the expiry of storage period
Occupational Health and Safety Education Process	Employees of Company, Employees of Business Partners	Identification Data, Professional Experience Information	10 years after leave of employment	Within 180 days following the expiry of storage period
Occupational Health and Safety Assignments	Company officials, other	Identification Data, Professional Experience Information	10 years	Within 180 days following the expiry of storage period
Keeping Environment Authority Records Process	Employees of Company	Identification Data, Professional Experience Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Shuttle Process	Employees of Supplier	Identification Data, Health Information, Criminal status and safety measures	10 years after termination of contractual relation	Within 180 days following the expiry of storage period
Allocation and Management of Vehicle	Employees of Company, Employees of Supplier	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Port Services Process	Employees of Company, Employees of Supplier	Identification Data, Contact Information, Special quality data	10 years	Within 180 days following the expiry of storage period
Disinfection Service Process	Employees of Supplier	Identification Data, Contact Information, Criminal status and safety measures, Professional experience, Health Information	10 years	Within 180 days following the expiry of storage period
Management of Traffic Fines	Employees of Company	Identification Data, Contact Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Security Documents Follow-up Process	Employees of Company, Employees of Supplier	Identification Data, Contact Information, Professional experience information, biometric data	10 years	Within 180 days following the expiry of storage period

Creating Lists of Employees	Employees of Company	Identification Data, Contact Information, Health Information	10 years as of leave of employment	Within 180 days following the expiry of storage period
Physical Environment Security Process	Employees of Company, Candidate Employee of Company, Company Partners, Customers of Company, Potential Customers of Company, Visitor, Supplier, Business Partners, Company Official	Physical Environment Security Information, Identification Data	1 month	Within 180 days following the expiry of storage period

8.10 Periodical Demolition Process

As per article 7 of the Law on Personal Data Protection, personal data is periodically demolished in case of disappearance of reasons requiring data processing or expiry of period stipulated in the legislation although it was processed in accordance with the legal legislation. Our company erase, destruct or anonymize personal data at the first periodical demolition process following the date when the obligation to erase, destruct or anonymize personal data arises. Periodical demolition is performed at 6 months' time intervals which is two times in a year for all personal data.

All transactions in relation to erasure, destruction and anonymization of personal data are recorded, and the aforesaid records are kept for 3 years apart from other legal obligations.