DOCUMENTS
Security Begins With Awareness ™

“DATA STORAGE AND DESTRUCTION POLICY OF KARMASIS INFORMATION TECHNOLOGY SOLUTIONS JOINT STOCK COMPANY FOR PERSONAL DATA”

1. INTRODUCTION

1.1 Purpose

This Personal Data Storage and Destruction Policy (hereinafter referred to as "Policy") is applicable to Karmasis Bilişim Çözümleri Ticaret Anonim Şirketi (hereinafter referred to as "COMPANY") in accordance with the current legislation and is based on the national principles accepted for personal data destruction. It includes the framework and principles for necessary destruction work under the relevant legislation.

Article 7, paragraph 3 of the Personal Data Protection Law No. 6698 (hereinafter referred to as the "Law") states that "procedures and principles for the deletion, destruction, or anonymization of personal data shall be regulated by a regulation." Based on this provision and the first paragraph of article 22 (e) of the Law, the Personal Data Protection Board (hereinafter referred to as the "Board") has prepared the Regulation on Deletion, Destruction, or Anonymization of Personal Data (hereinafter referred to as the "Regulation"), which was published in the Official Gazette dated 28 October 2017 and numbered 30224.

In light of the above regulation, the purpose of this Policy is to determine the procedures and principles for the deletion, destruction, or anonymization of personal data processed by the COMPANY in accordance with the Regulation, in the course of carrying out its activities.

1.2 Scope

This Policy covers the personal data of the employers/representatives, employees, job applicants, interns, third parties with whom we cooperate, and employees of third parties with whom we cooperate, with whom the COMPANY has a legal relationship. This Policy is applied to all record environments and activities related to personal data processing, where personal data owned or managed by the COMPANY are processed.

1.3. Definition

Concept	The definition
Recipient Group	Category of real or legal person to whom personal data are transferred by the data controller.
Explicit Consent	The explicit consent given based on information regarding a specific subject matter and expressed with free will.

Anonymization - Rendering personal data anonymous in such a way that the data subject cannot be identified or linked to an identified or identifiable natural person, even through the use of other data.
Electronic Environment - The environments in which personal data can be created, read, modified, and written using electronic devices.
Non-electronic Environment - The other environments such as written, printed, visual, etc. that are outside of electronic environments.
Data Subject - Data subject whose personal data is being processed.
Related User - The individuals who process personal data within the organization of the data controller, or on behalf of the data controller based on the authority and instructions they have received, except for the person or unit responsible for technically storing, protecting, and backing up the data.
Irreversible Destruction - Deletion, destruction or anonymization of personal data.
Law - Law No. 6698 on the Protection of Personal Data.
Recording Media - The environment in which personal data that is processed either entirely or partially by automatic means or processed as part of any data recording system that is not automatic is located.

Personal Data - Any information relating to an identified or identifiable natural person.

Data Subject - Data subject whose personal data is being processed.

Processing of Personal Data - The processing of personal data refers to any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Personal Data Processing Inventory - The inventory created by data controllers by associating the personal data processing activities they carry out in accordance with their business processes with the purpose of processing personal data, data category, recipient group to which the data is transferred, and the group of data subjects, and by detailing the maximum period required for the purposes for which personal data are processed, the personal data intended to be transferred to foreign countries, and the measures taken for data security.

Board - Personal Data Protection Board.

Institution - Personal Data Protection Authority.
Special Category Personal Data - Personal data of individuals related to their race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, dress and appearance, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as their biometric and genetic data.
Periodic Destruction - The process of deletion, destruction, or anonymization to be automatically performed at recurring intervals specified in the personal data retention and destruction policy in case all the processing conditions of personal data specified in the Law are eliminated.
Policy - The policy on which data controllers rely as a basis for determining the maximum period necessary for the purpose of processing personal data and for the process of deletion, destruction, and anonymization.
Registry - The registry of data controllers maintained by the Presidency of the Personal Data Protection Board.

VERBIS - Data Controllers Registry Information System.
Data Processor - The natural or legal person who processes personal data on behalf of the data controller based on the authorization given by the data controller.
Data Recording System - Record system where personal data is processed in a structured manner according to specific criteria.
Data Controller - Data Controller refers to the real or legal person who determines the purposes and means of processing personal data, and is responsible for establishing and managing the data recording system.
Regulation - The Regulation on Deletion, Destruction or Anonymization of Personal Data, which was published in the Official Gazette dated 28.10.2017 and numbered 30224 and entered into force.

2. RESPONSIBILITIES and TASK DISTRIBUTIONS

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

The distribution of titles, units, and job descriptions of those involved in the storage and destruction processes of personal data are given below.

Table 1: Distribution of responsibilities for storage and destruction processes.

Title	Human Resources Officer
Department	Human Resources
Job Description	Ensuring compliance with the storage period of personal data of employees, job applicants, and interns, managing the periodic destruction process, receiving and responding to requests for information regarding the rights of employees as stipulated by the 'Law', and ensuring that they are informed about their rights.
Title	Accounting/Finance Officer
Department	Accounting/Finance
Job Description	Ensuring compliance with the retention periods of processes within its responsibility, managing the periodic destruction process, checking the continuation of the obligation to keep books and documents arising from the Turkish Commercial Code and Tax Legislation, and whether the obligations have ceased.
Title	Other Officials

Department	Occupational Health and Safety, Import, Purchasing, Sales Department, Technical Support Department
Job Description	Ensuring compliance with the retention period of processes within their duties, management of periodic destruction process, continuation of document retention obligations related to contracts and relevant legislation, and verification of whether the obligations have ceased or not.

3. RECORD KEEPING SYSTEMS

Personal data is securely stored in the environments listed in Table 2 by the Institution.

Table 2: Personal data storage environments

Electronic Environments

- Servers (Domain, backup, email, database, web, file sharing, etc.)
- Softwares (office softwares)
- Information security devices (firewall, log file, antivirus, etc.)
- Mobile devices (phone, tablet, etc.)
- Optical disks (CD, DVD, etc.)
- Removable storage devices (USB, memory card, etc.)
- Printer, scanner, photocopier
- Removable storage devices such as USB, hard disk
- Desktop and laptop computers

Non-electronic Environments

- Paper
- Manual data recording systems
- Written, printed, visual media
- Folders

• Files

4. EXPLANATIONS REGARDING STORAGE AND DESTRUCTION

The personal data of natural persons, including but not limited to employees, job applicants, interns, bank officials, Cyberpark personnel, employee relatives, shareholders/partners, business partners, business partner representatives, employers, employer representatives, references, insurance company/agency representatives, witnesses, suppliers, supplier employees, supplier representatives, persons who purchase products or services, employees of such persons, and authorized representatives of such persons, are stored and destroyed in compliance with the Law by the "Company". Detailed explanations regarding storage and destruction are provided below in order.

4.1. Explanations on Storage

The concept of processing personal data is defined in Article 3 of the "Law", and Article 4 states that the processed personal data must be relevant, limited and proportional to the purposes for which they are processed and must be kept for the period prescribed by the relevant legislation or for the duration necessary for the purposes for which they are processed. Articles 5 and 6 list the conditions for processing personal data.

Accordingly, personal data within the scope of "COMPANY" activities are stored for the period prescribed by the relevant legislation or for the duration necessary for our processing purposes in accordance with the law.

4.1.1 Legal Grounds Requiring Storage

"COMPANY" keeps the personal data processed within the scope of its activities for the duration specified in the secondary legislation, primarily including but not limited to;

• Tax Procedure Law No. 213

• Identity Notification Law No. 1774

• Labor Law No. 4857

• Social Security and General Health Insurance Law No. 5510

• Law No. 5651 on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications

• Turkish Code of Obligations No. 6098

• Turkish Commercial Code No. 6102

• Occupational Health and Safety Law No. 6361

• Law No. 6698 on the Protection of Personal Data

4.1.2. Processing Purposes Requiring Storage

“ŞİRKET” stores the personal data it processes within the scope of its activities for the following purposes:

• Conducting emergency management processes

• Conducting information security processes

• Conducting employee candidate / intern / student selection and placement processes
• Conducting job application processes of employee candidates

• Conducting employee satisfaction and loyalty processes

• Fulfillment of contractual and legal obligations arising from employment for employees

• Conducting processes related to employee benefits and interests

• Conducting audit / ethical activities

• Conducting training activities

• Conducting access authorization processes

• Conducting activities in compliance with legislation

• Conducting finance and accounting affairs

• Conducting processes related to loyalty to the company / product / service

• Providing physical space security

• Conducting assignment processes

• Tracking and conducting legal affairs

• Conducting internal audit / investigation / intelligence activities

• Conducting communication activities

• Planning human resources processes

• Conducting business activities / control

• Conducting occupational health / safety activities

• Receiving and evaluating proposals for the improvement of business processes

• Conducting business continuity activities

• Conducting procurement processes for goods / services

• Conducting post-sales support services for goods / services

• Conducting sales processes for goods / services

• Conducting production and operation processes for goods / services

• Conducting activities for customer satisfaction

• Organizational and event management

• Conducting performance evaluation processes

• Conducting risk management processes

• Conducting contract processes

• Conducting strategic planning activities

• Following up on requests / complaints

• Ensuring the security of movable property and resources

• Conducting supply chain management processes

• Conducting the implementation of the wage policy • Conducting product / service marketing processes

• Ensuring the security of data controller operations

• Providing information to authorized individuals, institutions, and organizations

• Conducting management activities

4.2. Reasons Requiring Disposal

Personal Data ;

• Amendment or revocation of relevant legislation that constitutes the basis for processing,

• Elimination of the purpose requiring the processing or storage of personal data,

• Withdrawal of explicit consent of the data subject in cases where the processing of personal data is based solely on explicit consent,

• Acceptance of the application made by the data subject for the deletion and destruction of personal data within the framework of the rights of the data subject according to Article 11 of the "Law",

• Rejection by the Company of the application made by the data subject for the deletion or destruction of personal data, finding the response insufficient, or failing to respond within the period prescribed in the "Law"; filing a complaint with the "Board" and approval of the request by the "Board",

• Deletion, destruction, or anonymization of personal data by the "COMPANY" upon the request of the data subject or ex officio, if the maximum storage period requiring the retention of personal data has expired and there is no condition justifying the storage of personal data for a longer period.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

To ensure the secure storage of personal data, prevention of unlawful processing and access, and lawful destruction of personal data, "COMPANY" takes technical and administrative measures in accordance with Article 12 and Article 6(4) of the "Law" within the framework of sufficient measures determined and announced by the "Board" for special categories of personal data.

5.1. Technical Measures

The measures taken by the "COMPANY" regarding the personal data it processes are listed below:

• Network and application security are ensured.

• The security of personal data stored in the cloud is ensured.

• Authorization matrix has been created for employees.

• Access logs are regularly maintained.

• Data masking is applied when necessary.

• Up-to-date anti-virus systems are used.

• Firewalls are used.

• User account management and authorization control system are applied and their follow-up is also performed.

• Log records are kept without user intervention.

• Intrusion detection and prevention systems are used.

• Cybersecurity measures have been taken and their implementation is constantly monitored.
• Encryption is applied.

• Penetration testing is performed.

• Special category personal data transferred on portable memory, CD, DVD media are transferred by encrypting.

• Data loss prevention software is used.

5.2. Administrative Measures:

The measures taken by "COMPANY" regarding the personal data it processes are listed below:

- There are disciplinary regulations containing data security provisions for employees.
- Awareness and training sessions on data security are held for employees at certain intervals.
- Confidentiality commitments are made.
- The authorities in this area are removed for employees who undergo job changes or leave the company.
- Signed contracts contain data security provisions.
- Personal data security problems are reported quickly.
- Personal data security is monitored.
- Necessary security measures are taken for entry and exit to physical environments containing personal data.
- The security of physical environments containing personal data is ensured against external risks (fire, flood, etc.).
- The security of environments containing personal data is ensured.
- Personal data is minimized as much as possible.
- Personal data is backed up, and the security of backed up personal data is also ensured.
- Current risks and threats are identified.
- Protocols and procedures for personal data security of a special nature are identified and implemented.
- Periodic and/or random audits are conducted and commissioned internally within the organization.

6. Techniques for Destroying Personal Data

The personal data is destroyed by "COMPANY" through the following techniques in accordance with the relevant legislation, either ex officio or upon request of the related person, at the end of the retention period prescribed by the relevant legislation or required for the purposes for which they were processed.

6.1. Deletion of Personal Data

Personal data is deleted using the methods listed in Table 3:

Table 3: Deletion of personal data.

Data Recording Medium	Description
Personal data in physical environment	- Personal data stored in physical media is deleted by using the redaction method or by storing the document in a secure environment where it cannot be accessed by any relevant users.

Data Recording Medium	Description
Personal Data Stored on Servers	- For personal data stored on servers whose storage period has ended, access rights of related users are revoked by the system administrator and deletion process is performed.

Data Recording Medium	Description
Personal data stored in databases	- Access to personal data in the database is blocked by assigning roles and permissions to the relevant user.

Data Recording Medium	Description
Personal data on portable devices (such as USB, hard disk, CD, DVD)	- Access to the file is blocked for the relevant user.

6.2. Destruction of Personal Data

As a company, the methods we use to lawfully destroy personal data are as follows:

Table 4: Destruction of Personal Data

Data Recording Medium	Description
Personal data in physical media	- Paper-based personal data that have reached the end of the storage period requiring their preservation are destroyed in paper shredders in a way that cannot be reversed.
Data Recording Medium	Personal data stored on environmental devices (network devices, flash-based environments, optical systems, etc.) and local systems.
Description	Devices containing personal data are destroyed by physical processes such as burning, shredding into small pieces, and melting. In addition, the demagnetization method is used to render the personal data on the device unreadable and

destroy it. However, the deletion process is also applied by entering random data onto the existing data with special software, preventing the recovery of old data.

6.3. Anonymization of Personal Data

Anonymization of personal data refers to the state where personal data is made unidentifiable with any means and cannot be associated with an identified or identifiable natural person even if matched with other data. For personal data to be considered anonymized, appropriate technical measures must be used in terms of record environment and related business area, such as the return of personal data by the data controller or third parties and/or the matching of data with other data, so that it cannot be associated with an identified or identifiable natural person.

7. RETENTION AND DESTRUCTION PERIODS

As for the personal data being processed within the scope of the activities by "COMPANY":

• The retention periods for all personal data related to the activities carried out depending on the processes are stated on the Personal Data Processing Inventory at the individual personal data level;

• The retention periods based on data categories are registered on VERBIS;

• The retention periods based on processes are included in this Personal Data Retention and Disposal Policy."

The process of destroying personal data is carried out by "COMPANY" in accordance with the relevant legislation for each relationship, in line with the storage periods determined. Personal data whose storage periods have expired are deleted, destroyed, or anonymized at periodic destruction intervals determined by "COMPANY".

Table 5: Process-Based Data Retention and Destruction Periods Table

PROCESS	RETENTION PERIOD	DESTRUCTION PERIOD
Human Resources employee processes.	15 years from the date the employee leaves the company.	In the first 6-month periodic destruction period following the end of the retention period.
PROCESS	RETENTION PERIOD	DESTRUCTION PERIOD
Processing of candidate-related processes.		

From the application date, 1 year.

In the first 6-month periodic destruction period following the end of the storage period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Management of processes related to interns.

10 years from the end of the internship.

During the first 6 months of the periodic disposal period following the end of the storage period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Execution of contract processes.

10 years following the termination of the contract.

During the first 6-month periodic destruction period following the end of the retention period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Occupational Health and Safety Processes.

15 years.

During the first 6 months of the periodic destruction period following the end of the retention period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Execution of Sales Processes.

15 years.

First 6-month periodic destruction period following the expiration of the retention period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Execution of Technical Support Processes.

10 years.

First 6-month periodic destruction period following the expiration of the retention period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Execution of Import and Procurement Processes.

10 years.

First 6-month periodic destruction period following the end of the retention period.

PROCESS - RETENTION PERIOD - DESTRUCTION PERIOD

Execution of Accounting and Finance Processes.

10 years.

During the first 6-month periodic destruction period following the end of the retention period.

The obligation to delete, destroy, or anonymize personal data whose storage periods have expired is fulfilled by the departments listed under the "2. RESPONSIBILITIES AND TASK DISTRIBUTIONS" section.

8. PERIODIC DESTRUCTION PERIOD

According to Article 11 of the Regulation, the periodic destruction period has been determined as [6] months by the "COMPANY". Accordingly, "COMPANY" carries out periodic destruction process in June and December every year.

9. PUBLISHING AND STORAGE OF THE POLICY

The Policy shall be published in two different mediums, namely, a printed (hard copy) version with wet signatures and an electronic version, and made publicly available on the company's website. A printed copy shall also be kept in the file of the Human Resources Department.

10. POLICY UPDATE PERIOD

The Policy is updated as needed and when there are changes in the processes.

11. ENTRY INTO FORCE AND ABOLITION OF THE POLICY

This "Policy" shall enter into force after being published on the company's website. In case of a decision to repeal it, the old hard copies of the "Policy" shall be cancelled with

the company's stamp and signature of a company authorized person (by affixing a cancellation stamp or writing "cancelled"), signed, and kept by the Human Resources Department for at least 5 years.