AIGENCE

(MEHMET CAN BIYIK)

PERSONAL DATA RETENTION AND DESTRUCTION POLICY

TABLE OF CONTENTS

1. **Introduction**
   - a. Purpose
   - b. Scope
   - c. Abbreviations and Definitions
2. **Principles Adopted by MEHMET CAN BIYIK Regarding Personal Data Processing and Protection**
   - a. Compliance with Fundamental Personal Data Processing Principles
   - b. Compliance with Personal Data Processing Conditions
   - c. Compliance with Special Category Personal Data Processing Conditions
3. **Responsibilities and Task Distribution**
4. **Record Environments**
5. **Transfer of Personal Data**
   - a. Domestic Transfer of Personal Data
   - b. International Transfer of Personal Data
6. **Explanations Regarding Circumstances Requiring Retention and Destruction**
   - a. Explanations regarding retention
   - b. Circumstances requiring destruction
7. **Data Subject Rights and Processing of Requests by DATA CONTROLLER**
8. **Technical and Administrative Measures**
   - a. Technical measures
   - b. Administrative measures
9. **Personal Data Destruction Techniques**
   - a. Deletion of personal data
   - b. Destruction of personal data
   - c. Anonymization of personal data

10. **Retention and Destruction Periods**

11. **Periodic Destruction Period**

12. **Publication and Storage of the Policy**

13. **Policy Update Period**

14. **Effectiveness and Revocation of the Policy**

---

1. INTRODUCTION

a. Purpose

The purpose of this document, the Personal Data Retention and Destruction Policy ("Policy"), is to fulfill our obligations under Personal Data Protection Law No. 6698 ("KVKK" or "Law") and the Regulation on Deletion, Destruction or Anonymization of Personal Data ("Regulation"), published in the Official Gazette dated October 28, 2017, which constitutes the secondary regulation of the Law. This Policy has been prepared by MEHMET CAN BIYIK (hereinafter referred to as "DATA CONTROLLER") in its capacity as data controller to inform data subjects about the principles for determining the maximum retention period necessary for the purposes for which personal data are processed, as well as the deletion, destruction, and anonymization processes.

b. Scope

Personal data belonging to company employees, job candidates, service providers, visitors, and other third parties are within the scope of this Policy. This Policy applies to all record environments where the Company owns or manages personal data and all activities related to personal data processing.

c. Abbreviations and Definitions

Abbreviation	Definition
EXPLICIT CONSENT	Consent that is specific to a particular subject, based on information, and expressed by free will.
GDPR	General Data Protection Regulation No. 2016/679 of the European Union, which repealed Directive 95/46/EC on May 25, 2018.
RELEVANT USER	Persons who process personal data within the data controller organization or in accordance with the authority and instructions received from the data controller, excluding persons or units responsible for the technical storage, protection, and backup of data.
DESTRUCTION	Deletion, destruction, or anonymization of personal data.
LAW/KVKK	Personal Data Protection Law No. 6698.
RECORD ENVIRONMENT	Any medium containing personal data processed completely or partially automatically or non-automatically as part of any data recording system.
PERSONAL DATA	Any information relating to an identified or identifiable natural person.

Abbreviation	Definition
TRANSFER OF PERSONAL DATA	Sharing personal data in compliance with KVKK and Article 5 of this Policy with domestic or foreign institutions, organizations, suppliers, etc.
ANONYMIZATION OF PERSONAL DATA	Making personal data unable to be associated with an identified or identifiable natural person in any way, even when matched with other data.
PROCESSING OF PERSONAL DATA	Any operation performed on personal data, whether completely or partially automatic or non-automatic as part of any data recording system, such as obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, acquiring, making available, classifying, or preventing use.
DELETION OF PERSONAL DATA	Making personal data completely inaccessible and unusable for relevant users in any way.
DESTRUCTION OF PERSONAL DATA	The process of making personal data completely inaccessible, irretrievable, and unusable by anyone.
BOARD	Personal Data Protection Board
AUTHORITY	Personal Data Protection Authority
AUTOMATIC DATA PROCESSING	Personal data processing activities performed by an electrical or electronic system that reduces the need for human intervention or assistance to a minimum level, interconnected and interactive.
NON-AUTOMATIC DATA PROCESSING	Personal data processing activities performed with human intervention or assistance, i.e., manually.
SPECIAL CATEGORY PERSONAL DATA	Data concerning a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, association, foundation or trade union membership, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
PERIODIC DESTRUCTION	Deletion, destruction, and anonymization processes carried out ex officio at recurring intervals specified in the personal data retention and destruction policy when all conditions for processing personal data specified in the Law cease to exist.
DATA SUBJECT/CONCERNED PERSON	The natural person whose personal data is processed.
DATA CONTROLLER	The natural 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 published in the Official Gazette dated October 28, 2017.
POLICY	Personal Data Retention and Destruction Policy
DATA PROCESSOR	Natural or legal person who processes personal data on behalf of the data controller based on the authority given by the data controller.

Abbreviation	Definition
VERBIS	Data Controllers Registry Information System

2. PRINCIPLES ADOPTED BY THE COMPANY REGARDING PERSONAL DATA PROCESSING AND PROTECTION

a. Compliance with Fundamental Personal Data Processing Principles

The DATA CONTROLLER adopts the following fundamental principles for compliance with personal data protection legislation and maintaining such compliance:

(1) Processing personal data in accordance with law and rules of integrity The DATA CONTROLLER conducts personal data processing activities in accordance with law and rules of integrity, primarily in compliance with the Constitution of the Republic of Turkey and personal data protection legislation.

(2) Ensuring accuracy and currency of processed personal data When conducting personal data processing activities, the DATA CONTROLLER takes all necessary administrative and technical measures within technical possibilities to ensure the accuracy and currency of personal data.

(3) Processing personal data for specific, explicit, and legitimate purposes Personal data processing activities by the DATA CONTROLLER are conducted within specific, explicit, and lawful purposes determined before the commencement of personal data processing activities.

(4) Processing personal data in a manner that is relevant, limited, and proportionate to the purpose The DATA CONTROLLER processes personal data in connection with data processing conditions and only to the extent necessary for the performance of these services. In this context, the purpose of personal data processing is determined before commencing personal data processing activities, and data processing activities are not conducted based on the assumption that they may be used in the future.

(5) Retaining personal data for the period stipulated in relevant legislation or necessary for the purpose for which they are processed The DATA CONTROLLER retains personal data only for the period stipulated in relevant legislation or required by the data processing purpose. Accordingly, when the period stipulated in legislation expires or the reasons requiring personal data processing cease to exist, personal data are immediately deleted by the DATA CONTROLLER.

b. Compliance with Personal Data Processing Conditions

The DATA CONTROLLER conducts personal data processing activities in accordance with the data processing conditions set forth in Article 5 of KVKK. In this context, personal data processing activities are carried out when the following personal data processing conditions exist:

(1) Existence of Explicit Consent of the Personal Data Subject
(2) Explicit Provision of Personal Data Processing Activity in Laws

(3) Factual Impossibility of Obtaining Explicit Consent of Data Subject and Necessity of Personal Data Processing
(4) Personal Data Processing Activity Being Directly Related to the Establishment or Performance of a Contract
(5) Necessity of Personal Data Processing Activity for the DATA CONTROLLER to Fulfill Legal Obligations
(6) Necessity of Data Processing for the Establishment, Exercise, or Protection of a Right
(7) Data Subject Making Personal Data Public
(8) Necessity of Personal Data Processing Activity for the Legitimate Interests of the DATA CONTROLLER, Provided It Does Not Harm the Fundamental Rights and Freedoms of the Data Subject

c. Compliance with Special Category Personal Data Processing Conditions

Special category personal data may be processed by the DATA CONTROLLER under the following circumstances, provided that sufficient measures are taken:

(1) Health personal data may be processed by the DATA CONTROLLER under one of the following conditions:

- For the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and their financing, by persons under the obligation of confidentiality or by authorized institutions and organizations, or
- Existence of explicit consent of the personal data subject.

(2) Special category personal data other than health and sexual life (race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, association, foundation or trade union membership, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data) may be processed with the explicit consent of the data subject or in cases stipulated by law.

---

3. RESPONSIBILITIES AND TASK DISTRIBUTION

Title	Responsibility
Business Owner	Performing all necessary operations for business activities, coordinating data processing processes, representing the business to third parties, and conducting all operational processes

---

4. RECORD ENVIRONMENTS

Personal data are stored securely and in accordance with the law in the environments listed below:

Electronic Environments:

- Servers (Domain, backup, email, database, web, file sharing, etc.)
- Software

- Information security devices
- Personal computers (Desktop, laptop)
- Mobile devices (phone, tablet, etc.)
- Removable storage devices (USB, Memory Card, etc.)

---

5. TRANSFER OF PERSONAL DATA

Personal data may be shared by the DATA CONTROLLER with business and solution partners operating in software security, digital storage, and digital data processing sectors, as well as with DATA CONTROLLER affiliates for the purpose of service provision.

Within the framework of national and international legislation provisions, primarily KVKK, the DATA CONTROLLER may transfer the personal data it processes domestically or internationally. These transfers may be subject to transfer operations. During these processes, the provisions of Articles 8 and 9 of the KVK Law, Directive 95/46/EC, and GDPR provisions that repealed this directive are taken into consideration. The DATA CONTROLLER has fulfilled the conditions stipulated by the aforementioned law articles and directives regarding the domestic and international transfer of personal data.

a. Domestic Transfer of Personal Data

The DATA CONTROLLER may transfer the data it processes to third parties by obtaining explicit consent of the relevant person, under the authority granted by Articles 8 and 9 of KVKK and within the framework of this policy. The fundamental principles explained in Section 2 of this Policy have been detailed by the DATA CONTROLLER within the scope of ensuring compliance with personal data protection legislation and maintaining such compliance. The provisions of other laws regarding domestic transfer of personal data are reserved.

b. International Transfer of Personal Data

Personal data may be transferred abroad by the DATA CONTROLLER in accordance with Article 9 of KVKK under the following conditions:

(1) In accordance with personal data processing conditions,
(2) If the country to which the transfer will be made is among the countries with adequate protection announced by the Personal Data Protection Board, or if there is no adequate protection in the relevant foreign country, provided that the data controllers in Turkey and the relevant foreign country undertake adequate protection in writing and the permission of the KVK Board is obtained.

---

6. EXPLANATIONS REGARDING CIRCUMSTANCES REQUIRING RETENTION AND DESTRUCTION

Personal data belonging to data subjects are stored by the DATA CONTROLLER securely in the physical or electronic environments listed above, within the limits specified in KVKK and other relevant legislation, particularly for the sustainability of commercial activities, fulfillment of legal obligations, planning and performance of employee rights and benefits, and management of customer relations.

a. Explanations Regarding Retention

Personal data processed in accordance with law and this Policy may be retained under the following conditions:

- Retention of personal data due to their direct relevance to the establishment and performance of contracts,
- Retention of personal data for the purpose of establishing, exercising, or protecting a right,
- Retention of personal data being necessary for the legitimate interests of the DATA CONTROLLER, provided it does not harm the fundamental rights and freedoms of individuals,
- Retention of personal data for the purpose of the DATA CONTROLLER fulfilling any legal obligation,
- Explicit provision for retention of personal data in legislation,
- Existence of explicit consent of data subjects for retention activities requiring explicit consent of data subjects.

b. Circumstances Requiring Destruction

In accordance with the Regulation, personal data belonging to data subjects are deleted, destroyed, or anonymized by the DATA CONTROLLER ex officio or upon request in the following cases:

- Amendment or performance of relevant legislation provisions that form the basis for processing or storing personal data,
- Elimination of the purpose requiring processing or storing personal data,
- Elimination of the conditions requiring processing of personal data in Articles 5 and 6 of the Law,
- Withdrawal of consent by the relevant person in cases where personal data processing is based solely on explicit consent,
- Acceptance by the data controller of the application made by the relevant person regarding deletion, destruction, or anonymization of personal data within the scope of their rights under Article 11, paragraphs 2(e) and (f) of the Law,
- Rejection by the data controller of the application made by the relevant person for deletion, destruction, or anonymization of personal data, finding the response inadequate, or failure to respond within the period stipulated in the Law; complaint to the Board and finding this request appropriate by the Board,

- Expiration of the maximum period required for storing personal data, despite the existence of any condition that would justify storing personal data for a longer period.

---

7. DATA SUBJECT RIGHTS AND PROCESSING OF REQUESTS BY THE COMPANY

When data subjects submit their requests regarding their personal data to the DATA CONTROLLER in writing or through other methods determined by the KVK Board, the DATA CONTROLLER, in its capacity as data controller, ensures that the request is concluded within the shortest possible time and at most within thirty (30) days, according to the nature of the request, in accordance with Article 13 of the KVK Law. Data subjects must submit their requests regarding personal data in accordance with the Communiqué on Application Procedures and Principles to Data Controllers.

The DATA CONTROLLER may request information to verify whether the applicant is the owner of the personal data subject to the application, within the scope of ensuring data security. The DATA CONTROLLER may also ask questions to the personal data subject regarding their application to ensure that the personal data subject's application is concluded in an appropriate manner.

Applications by data subjects may be rejected by the DATA CONTROLLER with justification in cases such as the possibility of hindering the rights and freedoms of other individuals, requiring disproportionate effort, or the information being publicly available.

Data Subject Rights: Under Article 11 of the KVK Law, data subjects may apply to the DATA CONTROLLER to request:

(1) Learning whether their personal data has been processed,
(2) Requesting information about processed personal data,
(3) Learning the purpose of personal data processing and whether they are used appropriately for their purpose,
(4) Learning about third parties to whom personal data has been transferred domestically or internationally,
(5) Requesting correction of incomplete or inaccurate personal data and requesting notification of this correction to third parties to whom the data was transferred,
(6) Requesting deletion, destruction, or anonymization of personal data when the reasons requiring processing cease to exist, despite being processed in accordance with KVKK and other relevant legal provisions, and requesting notification of this action to third parties to whom the data was transferred,
(7) Objecting to adverse consequences arising from analysis of processed data solely through automated systems,
(8) Requesting compensation for damages suffered due to unlawful processing of personal data.

---

8. TECHNICAL AND ADMINISTRATIVE MEASURES

Technical and administrative measures are taken by the Board within the framework of sufficient measures

determined and announced by the Board for special category personal data in accordance with Article 12 of the Law and paragraph four of Article 6 of the Law, for the secure storage of personal data, prevention of unlawful processing and access, and lawful destruction of personal data.

a. Technical Measures

- Necessary measures are taken for the physical security of our business's information systems equipment, software, and data.
- To ensure information systems security against environmental threats, hardware (access control system allowing only authorized personnel to enter the system room, 24/7 monitoring system, ensuring physical security of edge switches forming the local area network) and software (firewalls, attack prevention systems, network access control, systems preventing malicious software, etc.) measures are taken.
- Risks aimed at preventing unlawful processing of personal data are identified, appropriate technical measures for these risks are ensured, and technical controls for the measures taken are conducted.
- Access procedures are established within the DATA CONTROLLER, and reporting and analysis activities related to access to personal data are conducted.
- Access to storage areas containing personal data is recorded, and inappropriate access or access attempts are kept under control.
- The Data Controller takes necessary measures through its suppliers to ensure that deleted personal data becomes inaccessible and unusable for relevant users.

b. Administrative Measures

- Necessary measures are taken for the physical security of our business's information systems equipment, software, and data.
- To ensure information systems security against environmental threats, hardware (access control system allowing only authorized personnel to enter the system room, 24/7 monitoring system, ensuring physical security of edge switches forming the local area network) and software (firewalls, attack prevention systems, network access control, systems preventing malicious software, etc.) measures are taken.
- Risks aimed at preventing unlawful processing of personal data are identified, appropriate technical measures for these risks are ensured, and technical controls for the measures taken are conducted.
- Access procedures are established within the DATA CONTROLLER, and reporting and analysis activities related to access to personal data are conducted.
- Access to storage areas containing personal data is recorded, and inappropriate access or access attempts are kept under control.
- The Data Controller takes necessary measures through its suppliers to ensure that deleted personal data becomes inaccessible and unusable for relevant users.

---

9. PERSONAL DATA DESTRUCTION TECHNIQUES

At the end of the period stipulated in relevant legislation or the storage period necessary for the purpose for which they are processed, personal data are destroyed by the DATA CONTROLLER ex officio or upon request by the relevant person in accordance with relevant legal provisions using the techniques specified below.

a. Deletion of Personal Data

Data Record Environment	Description
Personal Data on Servers	For personal data on servers whose required storage period has ended, the deletion process is performed by the system administrator by removing access authorization for relevant users.
Personal Data in Electronic Environment	Personal data in electronic environment whose required storage period has ended are made completely inaccessible and unusable for other employees (relevant users) except the database administrator.
Personal Data on Portable Media	Personal data stored in flash-based storage environments whose required storage period has ended are backed up by the system administrator and stored in secure environments with access authorization given only to the system administrator.

b. Destruction of Personal Data

Data Record Environment	Description
Personal Data in Digital/Optical/Magnetic Environment	Personal data in digital/optical media and magnetic environments whose required storage period has ended are irreversibly destroyed in digital environment.

---

10. RETENTION AND DESTRUCTION PERIODS

By the DATA CONTROLLER, regarding personal data processed within the scope of activities:

- Process-based retention periods are included in the Personal Data Retention and Destruction Policy.

Personal data whose retention periods have ended are subject to ex officio deletion, destruction, or anonymization by the Board.

Process	Retention Period	Destruction Period
Contract preparation and performance of contractual obligations	2 years following contract termination	During the first periodic destruction period following the end of retention period
Access to Used Software (email, etc.)	Upon termination of activity	During the first periodic destruction period following the end of retention period
Domain, backup, etc.	2 years following user departure	During the first periodic destruction period following the end of retention period
Conducting business activities and providing digital application services to users	2 years following user departure	During the first periodic destruction period following the end of retention period

---

11. PERIODIC DESTRUCTION PERIOD

Periodic destruction periods are determined as 12 months. The periodic destruction process is carried out annually within the DATA CONTROLLER during a suitable date between November-December months.

---

12. PUBLICATION AND STORAGE OF THE POLICY

The Policy is published in two different environments: wet-signed (printed paper) and electronic, and disclosed to the public on the website. The printed paper copy is stored at the office center.

---

13. POLICY UPDATE PERIOD

The Policy is reviewed as needed and necessary sections are updated. Updates are published on the website.