

KAFEİN YAZILIM HİZMETLERİ TİCARET A.Ş.

Personal Data Retention and Destruction Policy

Version:2

Tarih: 1.06.2024

Document Details

Kafein Kafein Yazılım Hizmetleri Ticaret A.Ş.

Address: YTÜ, Davutpaşa Campus, Çifte Havuzlar Neighborhood, Old London Asphalt Street, Incubation Center A2 Block No:151/1B Inner Door No: B01, Esenler / Istanbul

Phone: +90 212 924 20 30

Fax: +90 212 483 70 27

Email: info@kafein.com.tr

Document Title

Personal Data Retention and Destruction Policy

Version

Date

02

1.06.2024

Version	Date	Reason for Change
02.00	1.06.2024	Kanun Değişikliği

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose

1.2. Scope

1.3. Abbreviations and Definitions

2. RESPONSIBILITIES AND TASK DISTRIBUTION

5

3. DATA RECORDING MEDIA

4. EXPLANATIONS ON RETENTION AND DESTRUCTION

4.1. Explanations Regarding Retention

4.1.1. Legal Grounds Requiring Retention

4.1.2. Purposes Requiring Retention

4.2. Explanations Regarding Destruction

5. TECHNICAL AND ADMINISTRATIVE MEASURES

5.1. Technical Measures

5.2. Administrative Measures

6. TECHNIQUES FOR DESTRUCTION OF PERSONAL DATA

6.1. Deletion of Personal Data

6.2. Destruction of Personal Data

6.3. Anonymization of Personal Data

7. RETENTION AND DESTRUCTION PERIODS

12

8. PERIODIC DESTRUCTION PERIOD

9. PUBLICATION AND STORAGE OF THE POLICY
10. POLICY UPDATE PERIOD
11. ENFORCEMENT AND REVOCATION OF THE POLICY

1. INTRODUCTION

1.1. Purpose

Kafein Yazılım Hizmetleri Ticaret A.Ş. (“**Kafein**” or the “**Company**”) pays utmost attention to the retention and destruction of personal data in compliance with the Constitution of the Republic of Turkey, the Law on the Protection of Personal Data No. 6698 (“**KVKK**”), the Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28.10.2017 and numbered 30224 (“**Regulation**”), and other applicable legislation, regarding the personal data of real persons including employees, employee candidates, interns, intern candidates, visitors, supplier representatives, supplier employees, individuals who receive products or services, potential product or service recipients, shareholders/partners, members of the board of directors, and other third parties.

For this reason, as the data controller, we determine and carry out the maximum retention period required for the purpose of processing and the procedures and durations regarding the destruction of all personal data obtained during the execution of our business processes, in accordance with this Personal Data Retention and Destruction Policy (the “**Policy**”).

Furthermore, during the retention and destruction processes of personal data, we take all necessary technical and administrative measures to prevent the unlawful retention or destruction of such data. As Kafein, we attach great importance to the protection of privacy and the safeguarding of data security at the highest level during personal data retention and destruction processes.

This Policy contains explanations regarding the methods we follow for the retention and destruction of personal data obtained during the course of our activities. In the event of any conflict between the applicable legislation and this Policy, our Company acknowledges that the provisions of the applicable legislation shall prevail.

1.2. Scope

This Policy covers all personal data processed by Kafein belonging to real persons including employees, employee candidates, interns, intern candidates, visitors, supplier representatives, supplier employees, individuals receiving products or services, potential product or service recipients, subcontractor employees, shareholders/partners, members of the board of directors, and other third parties.

The Policy pertains to the retention and destruction of these personal data processed by the Company in any electronic or physical environment and has been prepared in consideration of the KVKK, all primary and secondary applicable legal regulations, as well as relevant international standards and guiding documents in this field.

In addition, in cases where data processed by Kafein and/or the group companies and/or holdings it is part of are also processed by such group companies or holdings, the data may be processed by the group companies or holding for the purpose of conducting their activities in line with their principles, objectives, goals, and strategies, and for the protection of the rights, interests, and reputation of the relevant companies. In such cases, if a data transfer from one data controller to another occurs under the Law, the relevant Company shall inform the data subject at the stage of personal data collection that their personal data may be transferred to group companies and/or holdings.

1.3. Abbreviations and Definitions

Concept	Definition
Electronic environment	Environments where personal data can be created, read, modified, and written using electronic devices.
Group companies and/or holding	Refers to the group of companies or holding company that Kafein is part of.
Destruction	The process of deletion, disposal, or anonymization of personal data.
Data subject	The natural person whose personal data is processed.
Relevant user	The person who processes personal data within the data controller's organization or in accordance with the authority and instructions received from the data controller, excluding the person or unit responsible for technical storage, protection, and backup of data.
KVKK	The Turkish Personal Data Protection Law No. 6698.
Redaction	Processes such as crossing out, painting over, or blurring personal data so that the data can no longer be associated with an identified or identifiable person.

Personal data	Any information relating to an identified or identifiable natural person.
Board	The Personal Data Protection Board.
Policy	The policy that forms the basis for determining the maximum retention period of personal data and the deletion, destruction, and anonymization operations.
Anonymization of personal data	Rendering personal data impossible to link with an identified or identifiable person, even by matching with other data.
Deletion of personal data	Making personal data processed by automated means partially or completely inaccessible and unusable for relevant users.
Disposal of personal data	Making personal data completely inaccessible, irretrievable, and unusable by anyone.
Periodic destruction	The deletion, destruction, or anonymization of personal data carried out at recurring intervals as specified in the personal data retention and destruction policy, when all conditions for processing are no longer met as per KVKK.
Data processor	The natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller.
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.
Regulation	The Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28.10.2017 and numbered 30224.

2. RESPONSIBILITIES AND TASK DISTRIBUTION

The distribution of titles, departments, and job descriptions of personnel involved in the storage and destruction processes of personal data is provided below.

Responsible	Duty
[Human Resources IT Quality]	Responsible for preparing, developing, updating, and publishing this Policy.
[Human Resources IT Quality]	Responsible for periodically reviewing this Policy.
[Senior Management Executive Committee Chairman]	Responsible for approving this Policy.
[All Employees]	Responsible for complying with this Policy and providing necessary support in the preparation, development, and all activities related to personal data storage and destruction processes.

3. DATA RECORDING MEDIA

Electronic Environments	Physical Environments
<ul style="list-style-type: none"> • Databases (email database, file sharing, web, backup, etc.) • Softwares • Desktop and laptop computers • Information security devices (e.g., firewalls) • Portable devices (external hard drives, USB sticks, etc.) • Application automations 	<ul style="list-style-type: none"> • Folders • Files • Archive rooms

4. EXPLANATIONS ON RETENTION AND DESTRUCTION

Kafein ensures that the personal data of real persons, including employees, job applicants, interns, intern candidates, visitors, supplier representatives, supplier employees, persons receiving products or services,

potential recipients of products or services, subcontracted workers, shareholders/partners, board members, and other third parties, are stored and destroyed in compliance with the Personal Data Protection Law (KVKK). Detailed explanations regarding storage and destruction are provided below in sequence.

4.1. Explanations Regarding Retention

Many regulations in the legislation require personal data to be retained for a certain period. Therefore, we store the personal data we process for the period stipulated in the relevant legislation, or if no such period is specified, for as long as necessary to fulfill the purposes for which the personal data is processed.

In cases where personal data is processed for multiple purposes, if all processing purposes cease to exist, the data will be deleted, destroyed, or anonymized ex officio, or upon the request of the relevant person, provided that there is no legal obstacle to deletion under the legislation.

4.1.1. Legal Grounds Requiring Retention

Personal data processed within the scope of activities at Kafein is retained for the period stipulated in the relevant legislation. Within this framework, personal data is retained for the storage periods prescribed by:

- Law No. 6698 on the Protection of Personal Data
- Turkish Code of Obligations No. 6098
- Turkish Commercial Code No. 6102
- Labor Law No. 4857
- Occupational Health and Safety Law No. 6361
- Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications
- Other secondary regulations in force, primarily including those listed above.

4.1.2. Purposes Requiring Retention

The Company retains personal data processed within the scope of its activities for the following purposes:

- Emergency Management Processes
- Information Security Processes
- Management of Job Applicant Processes
- Selection and Placement Processes for Job Candidates/Interns/Students

- Fulfillment of Employment Contract and Legal Obligations for Employees
- Administration of Employee Benefits and Perquisites
- Conducting Audit/Ethics Activities
- Implementation of Training Activities
- Management of Access Authorizations
- Ensuring Compliance of Operations with Legislation
- Execution of Finance and Accounting Tasks
- Ensuring Physical Facility Security
- Management of Assignment Processes
- Monitoring and Execution of Legal Affairs
- Monitoring and Execution of Personnel Affairs
- Monitoring and Execution of Business Development Activities
- Conducting Internal Audit / Investigation / Intelligence Activities
- Management of Communication Activities
- Planning of Human Resources Processes
- Execution and Supervision of Business Operations
- Implementation of Occupational Health and Safety Activities
- Ensuring Business Continuity Activities
- Receiving and Evaluating Suggestions for Business Process Improvement
- Execution of Goods/Services Procurement Processes
- Execution of Goods/Services Sales Processes
- Execution of Goods/Services Production and Operation Processes
- Execution of After-Sales Support Services for Goods / Services
- Management of Customer Relationship Processes
- Execution of Activities Aimed at Customer Satisfaction
- Organization and Event Management
- Management of Performance Evaluation Processes
- Execution of Advertising/Campaign/Promotion Processes
- Execution of Storage and Archiving Activities
- Management of Contract Processes
- Monitoring of Requests/Complaints
- Execution of Supply Chain Management Processes
- Administration of Compensation Policy
- Ensuring Security of Data Controller Operations

- Execution of Talent/Career Development Activities
- Providing Information to Authorized Persons, Institutions, and Organizations
- Providing Information to Judicial and Legal Authorities
- Providing Information to Law Enforcement Agencies
- Creation and Monitoring of Visitor Records

4.2. Explanations Regarding Destruction

Personal data shall be deleted, destroyed, or anonymized by the Company upon the request of the data subject, or ex officio, under the following circumstances:

- Amendment or repeal of the relevant legislation governing the processing of the data,
- The purpose requiring the processing or retention of the data no longer exists,
- In cases where the processing of personal data is based solely on explicit consent, the data subject withdraws their explicit consent,
- The Company accepts the data subject's application for deletion and destruction of personal data within the scope of their rights under Article 11 of the Personal Data Protection Law (KVKK),
- If the Company rejects the data subject's request for deletion or destruction, provides an insufficient response, or fails to respond within the timeframe stipulated by the KVKK; in such cases, the data subject may file a complaint with the Personal Data Protection Board, and if the Board deems the request appropriate,
- The maximum retention period required for the storage of personal data has expired and there is no justified reason to retain the data for a longer period.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

In accordance with Articles 12 and 6 of the Personal Data Protection Law (KVKK), the Company takes technical and administrative measures within the scope of sufficient precautions determined and announced by the Board for special categories of personal data to ensure the secure storage of personal data, prevent unlawful processing and access, and ensure the lawful destruction of personal data.

5.1. Technical Measures

Measures taken by Kafein regarding the personal data it processes are as follows:

- Network and application security are ensured,
- Closed system networks are used for personal data transfers via network,
- Key management is applied,

- Security measures are taken within the scope of procurement, development, and maintenance of IT systems,
- Up-to-date antivirus systems are used,
- Firewalls are used,
- Personal data security is monitored,
- Personal data is minimized as much as possible,
- Personal data is stored anonymously whenever possible,
- Personal data is backed up, and the security of the backups is ensured,
- User account management and authorization control systems are applied and monitored,
- Intrusion detection and prevention systems are used,
- Penetration testing is conducted,
- Cybersecurity measures have been implemented and are continuously monitored,
- Encryption is applied.

5.2. Administrative Measures

The measures taken by Kafein regarding the personal data it processes are as follows:

- Disciplinary regulations including data security provisions are in place for employees,
- Regular training and awareness activities on data security are conducted for employees,
- An authorization matrix is created for employees,
- Corporate policies are implemented regarding access, information security, usage, storage, and destruction,
- Confidentiality agreements are signed,
- Access rights of employees who have changed roles or left the company are revoked,
- Signed contracts include data security provisions,
- Personal data security policies and procedures are established,
- Personal data security incidents are reported promptly,
- Necessary security measures are taken for physical areas containing personal data,
- Security of physical areas containing personal data against external risks (fire, flood, etc.) is ensured,
- Security of environments containing personal data is maintained,
- Periodic and/or random internal audits are conducted and enforced,
- Existing risks and threats are identified, and
- Awareness of data-processing service providers is ensured.

6. TECHNIQUES FOR DESTRUCTION OF PERSONAL DATA

At the end of the retention period stipulated by the relevant legislation, or when the retention period necessary for the purpose of processing the personal data has expired, the personal data shall be destroyed by the Company either ex officio or upon the request of the data subject, in accordance with the applicable legal provisions, using the methods specified below.

6.1. Deletion of Personal Data

As Kafein, the techniques we employ to lawfully delete personal data are as follows:

Data Storage Medium	Explanation
Personal Data in Physical Environment	Personal data stored in physical environments is kept in a secure area where the relevant users have no access whatsoever, and then deleted using the redaction method. The redaction process involves, whenever possible, cutting out the personal data on the document; if not possible, making it invisible using permanent ink that cannot be reversed or read by technological means.
Personal Data in Databases	Access to personal data in databases is restricted by assigning roles and permissions to the relevant user.
Personal Data in Central Servers	The access rights of the relevant user to the directory containing the personal data files are revoked.
Personal Data on Portable Devices (USB, Hard disk, CD, DVD, etc.)	Files containing personal data are stored in encrypted form, and access to these files is blocked for the relevant user.

6.2. Destruction of Personal Data

As Kafein, the technical methods we apply to ensure the lawful destruction of personal data are as follows:

Data Storage Medium	Explanation
Physical Personal Data	Personal data in physical form is destroyed by shredding with a paper shredder or by incineration.
Personal Data in Cloud Environments	Personal data stored in cloud environments is encrypted using cryptographic methods during storage and use. Destruction of the encryption keys results in the deletion of the personal data in these environments.
Personal Data in Environmental (network devices, flash-based media, optical systems, etc.) and Local Systems	Devices containing personal data are destroyed through physical processes such as burning, shredding into small pieces, or melting. Additionally, demagnetization is applied to render personal data unreadable and thus destroyed. Furthermore, specialized software overwrites existing data with random data to prevent recovery, ensuring complete destruction.

6.3. Anonymization of Personal Data

Anonymization of personal data means rendering personal data in such a way that, even if matched with other data, it cannot be associated with an identified or identifiable natural person under any circumstances.

For personal data to be considered anonymized, it must be processed using appropriate techniques—regarding the data storage medium and the relevant activity area—so that it cannot be linked to an identified or identifiable natural person, even by the data controller or third parties through reversal or matching with other data. Our company anonymizes data in this manner.

7. RETENTION AND DESTRUCTION PERIODS

The processes of automatic deletion, destruction, or anonymization of personal data whose retention periods have expired are carried out by the relevant departments. The retention periods of personal data are determined within the framework of the periods stipulated in the applicable legislation.

Within this framework, if the retention of the relevant data by Kafein is evaluated according to the lawful processing grounds for personal data and special categories of personal data as set forth in Articles 5 and 6

of the KVKK, the retention periods for the related personal data are determined based on these lawful grounds. The destruction process of personal data is carried out by Kafein in accordance with the retention periods established in compliance with the relevant legislation for each relationship. Personal data whose retention periods have expired are deleted, destroyed, or anonymized by Kafein according to the predetermined periodic destruction schedules.

Process	Retention Period	Destruction Period
Execution of human resources processes	30 years from the termination of employment	At the first scheduled destruction period following the end of the retention period
Execution of processes related to job applicants	1 year from the application date	At the first scheduled destruction period following the end of the retention period
Execution of contractual relationships	10 years following the termination of the contract	At the first scheduled destruction period following the end of the retention period
Log record tracking systems	2 years	At the first scheduled destruction period following the end of the retention period
Processes related to website visitors	1 year	At the first scheduled destruction period following the end of the retention period
Execution of processes related to camera records and physical visitors	90 days	At the first scheduled destruction period following the end of the retention period

8. PERIODIC DESTRUCTION PERIOD

According to Article 11 of the Regulation, the periodic destruction interval has been determined by Kafein as [6] months.

9. PUBLICATION AND STORAGE OF THE POLICY

The original of the Policy is maintained within the [quality management system documentation] environment, and an electronic copy is published in a location accessible to employees.

10. POLICY UPDATE PERIOD

The Policy is updated whenever necessary or when there are changes in the processes.

11. ENFORCEMENT AND REVOCATION OF THE POLICY

This Policy shall enter into force on [June 1, 2024] with the approval of the [executive board]. In the event of a decision to revoke the Policy, the previously signed hard copies of this Policy shall be cancelled by the [quality management representative] with the written approval of the [executive board] (by stamping “Cancelled” or annotating the cancellation) and signed accordingly. The cancelled documents shall be retained by the [quality management representative] and destroyed by the [quality management representative] with the written approval of the [executive board] at the end of the retention period.