PERSONAL DATA RETENTION AND DESTRUCTION POLICY

INTRODUCTION AND PURPOSE OF THE POLICY

This Personal Data Retention and Destruction Policy ("**Policy**") has been prepared by Feedback4e Yazılım Danışmanlık A.Ş. in its capacity as a data controller, in order to fulfill our obligations under the Turkish Personal Data Protection Law No. 6698 ("**KVKK**" or "**Law**") and the European Union General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"). The Policy also serves as a basis for the implementation of the Regulation on the Deletion, Destruction, or Anonymization of Personal Data ("**Regulation**"), which was published in the Official Gazette on October 28, 2017, as a secondary regulation to the Law, and for the fulfillment of obligations under Article 17 of the GDPR regarding the right to erasure (right to be forgotten). The Policy aims to determine the maximum retention period necessary for the purpose for which personal data is processed, as well as to guide the processes of deletion, destruction, and anonymization, and to inform data subjects about these processes.

SCOPE

This policy covers all personal data held by the organization, including data related to all employees, consultants, subsidiaries, suppliers, and other natural and legal persons with whom the organization has a legal relationship in situations where personal data is shared. It applies to personal data and special categories of personal data, as defined by law, that are processed either fully or partially by automated means or by non-automated means, provided that they form part of a data filing system. Unless otherwise specified in the policy, personal data and special categories of personal data will be collectively referred to as “Personal Data.”

AUTHORITIES AND RESPONSIBILITIES

Within the organization, all employees, consultants, external service providers, and anyone else who stores and processes personal data on behalf of the organization are responsible for fulfilling the requirements related to data destruction as specified by the Law, the Regulation, and this Policy. Each business unit is responsible for retaining and protecting the data generated within its own business processes.

The responsibility for receiving or accepting notifications and correspondence from the Data Protection Authority on behalf of the data controller, as well as for processes such as registration in the registry, lies with the "Data Controller Contact Person."

DEFINITIONS

Abbreviations	Definition
Explicit Consent	Consent that is informed, specific to a particular topic, and given freely.
GDPR	General Data Protection Regulation, European Union General Data Protection Regulation (Regulation (EU) 2016/679)
Data Subject	These are individuals who process personal data within the organization of the data controller, or in accordance with the authority and instructions received from the data controller, excluding those responsible for the technical storage, protection, and backup of the data.
Destruction	The deletion, destruction, or anonymization of personal data.
Law/KVKK	Law No. 6698 on the Protection of Personal Data.
Data Recording Environment	Any environment where personal data processed by automated means or non-automated means, provided that it forms part of a data filing system, is stored.
Personal Data	Any information relating to an identified or identifiable natural person.

Processing of Personal Data	Any operation performed on personal data, whether or not by automated means, including the collection, recording, storage, preservation, modification, reorganization, disclosure, transfer, acquisition, retrieval, classification, or prevention of use of the data.

Deletion of Personal Data	The act of making personal data completely inaccessible and unusable for the data subjects.
Anonymization of Personal Data	The process of making personal data so that it cannot be related to an identified or identifiable natural person, even when combined with other data.
Destruction of Personal Data	The process of making personal data completely inaccessible, irretrievable, and unusable b anyone.
Board	Personal Data Protection Board.
Special Categories of Personal Data	Data related to a person's race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
Periodic Destruction	The act of deleting, destroying, or anonymizing personal data at regular intervals, as specified in the data retention and destruction policy, once all processing conditions specified in the Law have ceased to apply.
Data Subject/Relevant Person	A natural person whose personal data is being 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 filing system.
Regulation	The Regulation on the Deletion, Destruction, or Anonymization of Personal Data publishe in the Official Gazette on October 28, 2017.

RULES

Feedback4e Yazılım Danışmanlık A.Ş. adheres to the following principles in the retention and destruction of personal data:

a) The deletion, destruction, and anonymization of personal data are carried out in full compliance with the principles listed in Article 4 of the Law, the measures required under Article 12 of the Law, the technical and administrative measures specified in Article 6.2 of this Policy, relevant legislative provisions, Board decisions, and this Policy.

b) All operations related to the deletion, destruction, and anonymization of personal data are recorded by Feedback4e Yazılım Danışmanlık A.Ş., and these records are kept for at least 6 months, excluding other legal obligations.

c) Unless otherwise decided by the Board, the appropriate method for the deletion, destruction, or anonymization of personal data is selected by us. However, if requested by the Data Subject, the rationale for the selected method will be explained.

d) When all conditions for the processing of personal data specified in Articles 5 and 6 of the Law have ceased to apply, and in accordance with the application basis under GDPR, personal data will be deleted, destroyed, or anonymized by Feedback4e Yazılım Danışmanlık A.Ş. either ex officio or upon request by the Data Subject. In such cases, if the Data Subject applies to Feedback4e Yazılım Danışmanlık A.Ş.;

- Requests are concluded and the relevant person is informed within a maximum of 30 (thirty) days,
- If the data subject to the request has been transferred to third parties, this situation is communicated to the third parties, and necessary actions are ensured to be taken by those third parties.

[1] a) Compliance with the principles of legality and fairness, b) Accuracy and, where necessary, up-to-dateness, c) Processing for specified, explicit, and legitimate purposes, d) Relevant, limited, and adequate to the purposes for which they are processed, e) Retention for the period prescribed by relevant legislation or necessary for the purposes for which they are processed.

EXPLANATIONS REGARDING REASONS FOR RETENTION AND DESTRUCTION

Personal data belonging to data subjects is securely stored by Feedback4e Yazılım Danışmanlık A.Ş. in physical or electronic environments, in accordance with the limits specified by the KVKK and other relevant legislation, particularly for the following reasons: (i) to sustain service activities, (ii) to fulfill legal obligations, (iii) to plan and administer employee rights and benefits, (iv) to manage customer relations, and (v) to comply with legal requirements and the purposes outlined in the inventory.

The reasons for retention are as follows:

- Retention of personal data due to its direct relevance to the establishment and performance of contracts,
- Retention of personal data for the establishment, exercise, or protection of a right,
- Retention of personal data as necessary for the legitimate interests of Feedback4e Yazılım Danışmanlık A.Ş., provided that it does not infringe on individuals' fundamental rights and freedoms,
- Retention of personal data for the purpose of fulfilling any legal obligations of Feedback4e Yazılım Danışmanlık A.Ş.,
- Explicit provision in the legislation for the retention of personal data,
- Retention activities that require obtaining explicit consent from data subjects, provided that such consent is obtained.
- According to the Regulation, personal data of data subjects will be deleted, destroyed, or anonymized by Feedback4e Yazılım Danışmanlık A.Ş. either ex officio or upon request in the following cases:
- Amendment or repeal of the legal provisions that form the basis for the processing or retention of personal data,
- The cessation of the purpose for which the personal data was processed or retained,
- The cessation of the conditions required for the processing of personal data as specified in Articles 5 and 6 of the Law.
- Where the processing of personal data was based solely on explicit consent and the data subject withdraws their consent,
- If the data subject’s request for the deletion, destruction, or anonymization of their personal data, made under Article 11(e) and (f) of the Law, is accepted by the data controller.
- Under GDPR, if the data subject’s request for withdrawal of consent or right to erasure is found to be valid, and there are no compelling legitimate grounds that override the data subject's interests, rights, and freedoms or are necessary for the establishment, exercise, or defense of legal claims, the data must not be processed.
- These rights under GDPR or national laws may be limited; for example, if fulfilling your request would result in the disclosure of personal data about another person, violate the rights of a third party (including our rights), or if you request the deletion of information that we are required to retain by law or have compelling legitimate interests to protect.
- If the data controller rejects a request by the data subject for the deletion, destruction, or anonymization of their personal data, provides an inadequate response, or fails to respond within the time frame specified by the Law, a complaint can be lodged with the Board, and if the request is found to be valid by the Board,
- If the maximum retention period for personal data has passed and there are no conditions justifying the retention of the data for a longer period.

RETENTION AND DESTRUCTION PERIODS

The retention and destruction periods for your personal data obtained by Feedback4e Yazılım Danışmanlık A.Ş. in compliance with KVKK and other relevant regulations are determined based on the following criteria:

a) If the legislation prescribes a retention period for the personal data, this period will be observed. After the expiration of this period, the data will be processed as described in section b.

b) If the retention period specified in the legislation has expired or if no retention period is specified in the relevant legislation, then;

c) Personal data will be classified based on the definitions in Article 6 of KVKK into personal data and sensitive personal data. All personal data identified as sensitive will be destroyed. The method of destruction for such data will be determined based on the nature of the data and its importance to Feedback4e Yazılım Danışmanlık A.Ş.

- The compliance of data storage with the principles outlined in Article 4 of KVKK is examined, for instance, whether Feedback4e Yazılım Danışmanlık A.Ş. has a legitimate purpose for storing the data. Data found to violate the principles in Article 4 of KVKK will be deleted, destroyed, or anonymized.
- It is determined which exceptions specified in Articles 5 and 6 of KVKK apply to the data storage. Reasonable retention periods are established based on the identified exceptions. Upon the expiration of these periods, the data will be deleted, destroyed, or anonymized.

You can access the storage, destruction, and periodic destruction periods identified by Feedback4e Yazılım Danışmanlık A.Ş. from the "Personal Data Processing Inventory" attached to this Policy.

Personal data whose retention period has expired will be destroyed in accordance with the procedures specified in the Policy and within 6-month intervals, as outlined in the attachment.

All actions related to the deletion, destruction, and anonymization of personal data are recorded, and these records are retained for at least 6 months, excluding other legal obligations.

RETENTION AND DESTRUCTION METHODS FOR PERSONAL DATA RECORDING ENVIRONMENTS

Personal data of data subjects are securely stored by Feedback4e Yazılım Danışmanlık A.Ş. in the environments listed below, in accordance with KVKK regulations and other relevant legislation, as well as international data security principles:

a) Electronic Environments:

- Servers (domain, backup, email, database, web, file sharing, etc.)
- Software (office software, portals, government applications, VERBİS)
- Information Security Devices (firewalls, intrusion detection and prevention systems, antivirus software, etc.)
- Personal Computers (desktop computers, laptops)
- Removable Storage Devices (USB drives, memory cards, etc.)
- Printers, Scanners, Photocopiers

b) Physical Environments:

- Paper
- Written, Printed Materials, forms, contracts, visual materials

TECHNICAL AND ADMINISTRATIVE MEASURES

To ensure the secure storage of your personal data, prevent unlawful processing, prevent unauthorized access, and ensure the lawful destruction of data, Feedback4e Yazılım Danışmanlık A.Ş. has implemented the following administrative and technical measures in accordance with the principles set out in Article 12 of KVKK:

a) Administrative Measures:

Feedback4e Yazılım Danışmanlık A.Ş., within the scope of administrative measures;

Feedback4e Yazılım Danışmanlık A.Ş implements necessary administrative measures to ensure the security of personal data and monitors employees to ensure compliance with these measures. Access and authorization levels are defined according to the legal compliance requirements specific to each business unit, without disrupting business processes. Employees are informed that they must not disclose or use personal data beyond its intended purpose and that this obligation continues even after their departure from the company. Continuous training is provided on Information Security, Personal Data Security, GDPR, and the Law No. 6698 on Personal Data Protection, with necessary commitments obtained from employees. Framework agreements or contract clauses are established with third parties for data sharing to ensure data security. Third parties are required to take necessary security measures and ensure compliance within their organizations. If personal data is unlawfully obtained by others despite these measures, the data subject and the KVK Board are notified, and the method of unauthorized acquisition is investigated. Feedback4e Yazılım Danışmanlık A.Ş applies necessary administrative measures to address identified vulnerabilities and takes technical measures if needed.

b) Technical Measures:

Under its technical measures, Feedback4e Yazılım Danışmanlık A.Ş;

Feedback4E Yazılım Danışmanlık A.Ş ensures data security by employing knowledgeable and experienced personnel and providing training in compliance with KVKK, ISMS, and GDPR. Additionally, the company establishes and maintains ISO 27001 Information Security Management System and ISO 27701 Personal Data Management System, undergoing independent audits annually. Necessary internal controls are implemented for these systems. In accordance with Article 32 of GDPR, it ensures that the necessary audits are conducted for GDPR compliance, guarantees the legality of data processing activities through internal policies and procedures, and enforces stricter measures for accessing special categories of personal data,

Under the established systems, Feedback4E Yazılım Danışmanlık A.Ş implements processes for risk analysis, data classification, information security, personal data management risk assessment, and business continuity analysis. Technical measures are taken in line with technological advancements. The company invests in infrastructure that aligns with emerging technologies, installs necessary software and hardware for virus protection and data security in cloud environments, and ensures that systems use updated versions with necessary security measures against known vulnerabilities. Regular penetration testing and vulnerability scanning are conducted. Access to personal data by employees is monitored, with access rights and authorizations defined based on legal compliance requirements for business units. Compliance with authorization guidelines is checked, and security findings are reported to relevant parties. Risks are identified, and appropriate technical measures are implemented. The organization promotes awareness of continuous technical measures as part of its corporate culture to ensure ongoing data security and ensures that precautions are maintained through regular controls.

PERSONNEL

You can obtain information about the titles, departments, and job descriptions of the personnel involved in the personal data storage and destruction processes from our organization.

METHODS OF DESTRUCTION OF PERSONAL DATA

Personal data obtained by Feedback4e Yazılım Danışmanlık A.Ş, in accordance with KVKK and other relevant regulations, will be destroyed by Feedback4e Yazılım Danışmanlık A.Ş either ex officio or upon the request of the data subject, once the purposes for processing the personal data listed in the Law and Regulation are no longer applicable. This destruction will be carried out using the technical methods specified below, in compliance with the Law and relevant regulations.

a) Techniques for Deletion and Destruction of Personal Data:

The procedures and principles regarding the deletion and destruction of personal data by Feedback4e Yazılım Danışmanlık A.Ş are listed below:

Deletion of Personal Data:

Secure Deletion from Software: When deleting data that is processed either fully or partially automatically and stored in digital environments, methods are used to ensure that the data is completely inaccessible and unusable for the relevant users. This includes methods for removing the data from the relevant software.

Deletion of data from a cloud system by issuing a deletion command; removal of access rights for the relevant user on the file or directory containing the file on a central server; deletion of relevant rows in databases using database commands; or deletion of data on portable media such as flash drives using appropriate software, all fall under this scope.

However, if the deletion of personal data results in the inability to access and use other data within the system, the personal data will be considered deleted if the following conditions are met, even if the data is archived in a form that cannot be linked to the relevant person.

- The data must be inaccessible to any other institution, organization, or individual,
- All necessary technical and administrative measures must be taken to ensure that personal data can only be accessed by authorized individuals.

Secure Deletion by an Expert: In certain cases, the organization may engage an expert to delete personal data on its behalf. In this scenario, the personal data will be securely deleted by the expert in a manner that renders it inaccessible and unusable for the relevant users.

Physical Redaction of Personal Data: To prevent the misuse of personal data or to delete data upon request, the physical removal of the data from documents by cutting it out or making it unreadable with non-reversible, technology-resistant ink is used. This method ensures that the personal data cannot be seen or retrieved.

Destruction of Personal Data:

Physical Destruction: Personal data, which may also be processed through non-automated means as part of any data recording system, is physically destroyed to ensure that it cannot be used or accessed again. This method is applied to make the personal data irretrievable and unusable.

Techniques for Anonymizing Personal Data:

Feedback4e Yazılım Danışmanlık A.Ş has outlined the procedures and principles for anonymizing

personal data as follows:

Anonymization of Personal Data is defined as the process by which personal data is made unidentifiable or non-retrievable to any identified or identifiable individual, even when combined with other data.

- Use of appropriate techniques based on the activity area related to the record medium,
- Techniques for anonymization include the use of de-identification techniques or methods for matching data with other data.

According to Article 28 of the KVKK, if personal data is processed for purposes such as research, planning, and statistics by anonymizing it for official statistics, this processing will be outside the scope of the Law and will not require explicit consent.

OTHER MATTERS

In the event of any inconsistency between the KVKK and other relevant legislation and this Policy, the provisions of the KVKK and other relevant legislation shall prevail.

This Policy prepared by Feedback4e has entered into force. In the event of any changes to the Policy, the effective date and relevant provisions of the Policy will be updated accordingly.

RETENTION AND DESTRUCTION PERIODS

The retention and destruction periods for processed data are determined on a process basis in the Personal Data Inventory. Information on retention and destruction periods can be accessed by filling out the KVKK and GDPR Application Form, which can be requested from the data inventory maintained by our institution.

PERSONS RESPONSIBLE FOR RETENTION AND DESTRUCTION PROCESSES

The company appoints a "Personal Data Protection Committee" or responsible person(s) to manage the retention and destruction processes as specified in this policy and other related policies, as well as to ensure the implementation of actions designated by senior management for compliance.

The tasks to be carried out by the relevant person or committee include:

- Preparing, tracking, and submitting documents related to the design of processes for the protection and processing of personal data for approval by relevant parties.
- Ensuring the implementation of documents related to the protection and processing of personal data and conducting necessary audits.
- Monitoring and managing relationships and correspondence with the KVKK Authority and the KVKK Board.

PUBLICATION AND UPDATING OF THE POLICY

This Policy is published on the Company's website (***www.feedback4e.com***) and made available to data subjects upon request.

The Policy will be updated as needed and the changes will come into effect by being published on the website.