Personal Data Protection and Processing Policy

Table of Contents

1. Purpose

This policy aims to describe the methods adopted for the processing and protection of personal data in accordance with the 6698 Personal Data Protection Law (KVKK) and the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") through appropriate technical and administrative measures in all activities conducted by Feedback4e Yazılım Danışmanlık A.Ş. The Personal Data Protection and Processing Policy includes principles applied in the processes of data collection, usage, sharing, storage, and destruction, as well as data security, transparency, individuals' rights over their personal data, and technical, legal, and administrative responsibilities. It is intended to inform individuals whose personal data is processed by the company, including ongoing clients of Feedback4e Yazılım Danışmanlık A.Ş., company employees, visitors, employees of partner organizations, and third parties.

2. Scope

This Policy covers all personal data processed in the processes of our organization, whether through automated means or as part of any data recording system, for ongoing clients, employees, visitors, employees of partner organizations, and third parties.

3. Authority 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, Regulation, and Policy. Each department is responsible for storing and protecting the data it produces in its own business processes.

Decisions on data destruction that could affect business processes, cause data integrity issues, result in data loss, or lead to non-compliance with legal regulations will be made by the relevant information systems department, considering the type of personal data, the systems involved, and the business unit performing the data processing.

Responsibility for acknowledging or accepting notifications or correspondence with the Data Protection Authority and for registering them in the official records lies with the designated contact person for data protection.

4. Definitions and Abbreviations

Explicit Consent; Consent that is based on being informed about a specific matter and is given freely and voluntarily.

GDPR: General Data Protection Regulation ((AB) 2016/679)

Authorized User; Individuals within the data controller organization or those who process personal data in accordance with the authority and instructions received from the data controller, excluding the person or unit responsible for the technical storage, protection, and backup of the data.

Destruction; The process of deleting, destroying, or anonymizing personal data.

Law; Personal Data Protection Law No. 6698 (KVKK).

Recording Medium; Any environment where personal data is processed, whether fully or partially automated, or through non-automated means as part of any data recording system.

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

Processing of Personal Data; Any operation performed on personal data, whether by automated means or as part of a data recording system, including collection, recording, storage, retention, alteration, rearrangement, disclosure, transmission, acquisition, accessibility, classification, or restriction of use.

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.

Deletion of Personal Data; The process of making personal data irretrievable and unusable for Authorized Users, ensuring that it cannot be accessed or reused in any way.

Destruction of Personal Data; The process of making personal data completely inaccessible, irretrievable, and unusable by anyone in any manner.

Board; Personal Data Protection Board.

Special Categories of Personal Data; Data relating to an individual's race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance, 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 process of automatically deleting, destroying, or anonymizing personal data at regular intervals specified in the data retention and destruction policy, once all conditions for processing personal data specified in the law have ceased to apply.

Veri Sahibi/İlgili Kişi; Kişisel verisi işlenen gerçek kişi.

Data Subject; The natural person whose personal data is being processed.

Data Processor; A 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; A 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.

Data Controller Contact Person and Assistants; Since the data controller is a legal entity established in Turkey, a data controller contact person has been appointed. Therefore, the primary duty of the contact person and their assistants is to be responsible for determining the purposes and means of processing personal data and 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 on October 28, 2017.

5. Personal Data Protection and Processing Policy

Our organization outlines the necessary measures and processes for the protection and processing of personal data in a concrete manner through this policy. In cases where there is a discrepancy between relevant laws, regulations, and this policy, or if the policy is not up-to-date with newly updated legislation, Feedback4E Yazılım Danışmanlık A.Ş acknowledges its commitment to comply with the applicable laws. This policy will be updated according to changes in laws, regulations, and legislation, and revised to ensure that Feedback4E Yazılım Danışmanlık A.Ş meets its legal requirements.

5.1. Ensuring the Security of Personal Data

Feedback4e Yazılım Danışmanlık A.Ş. implements all necessary technical and administrative measures to ensure an adequate level of security for the protection of personal data.

As required by Article 12(1) of the KVKK (Personal Data Protection Law);

- Preventing the unlawful processing of personal data,
- Preventing unauthorized access to personal data,
- Ensuring the protection of personal data.

It takes the necessary measures.

Our organization has detailed the measures it implements to ensure the security of personal data in the following subsections.

5.1.1. Technical Measures

Feedback4E Yazılım Danışmanlık A.Ş. employs knowledgeable and experienced personnel to ensure data security and provides training to its staff on compliance with KVKK, ISMS, and GDPR, as well as information security. Additionally, the

company establishes and maintains an ISO 27001 Information Security Management System and an ISO 27701 Personal Data Management System, undergoing independent audits annually. Internal controls are conducted for the established systems. The company ensures the implementation of GDPR provisions in accordance with Article 32 of the GDPR, ensures the legality of data processing activities through internal policies and procedures, and applies stricter measures for access to special categories of personal data.

The processes include risk analysis, data classification, information security, personal data management risk assessment, and business continuity analysis. Technical measures are taken in line with technological advancements, and infrastructure investments are made to keep up with evolving technology. The company ensures the installation of necessary software and hardware for virus protection and data security in cloud environments. Systems are maintained with updated versions that address known vulnerabilities, and regular penetration and vulnerability scanning tests are conducted. Access to personal data is controlled, and access and authorization definitions are made according to legal compliance requirements on a departmental basis. Compliance with authorization requirements is monitored, and findings from system security checks are reported to relevant parties. Risk areas are identified, and necessary technical measures are taken. To maintain the security of personal data, technical measures are integrated into the organizational culture and awareness is promoted. The implemented measures are continuously monitored through controls.

5.1.2. Administrative Measures

Feedback4E Yazılım Danışmanlık A.Ş. takes the necessary administrative measures to ensure the security of personal data and monitors employees' adherence to these measures. Access and authorizations are defined at the departmental level in accordance with legal compliance requirements, ensuring they do not disrupt business processes. Employees are informed that they must not disclose personal data they learn in violation of the KVKK (Personal Data Protection Law), cannot use it for purposes other than those for which it was processed, and that this obligation continues even after their departure from the organization.

Employees receive ongoing training in information security, personal data security, GDPR (General Data Protection Regulation), and the 6698 Personal Data Protection Law, covering technical, administrative, and legal aspects. Employees are required to make necessary commitments in this regard. Agreements are signed with third parties regarding the sharing of personal data to ensure data security, either through framework agreements or by adding relevant provisions to contracts. Third parties who receive personal data agree to implement the necessary security measures and ensure compliance with these measures within their own organizations.

In the event that personal data is found to be unlawfully obtained by others despite the measures taken, the data representative will notify the relevant party and the KVKK Board. The method by which personal data was obtained by others will be investigated. Feedback4E Yazılım Danışmanlık A.Ş. will apply the necessary administrative measures to address any identified vulnerabilities and will take technical measures if needed

5.1.3. Storage of Personal Data in a Secure Environment

Feedback4E Yazılım Danışmanlık A.Ş. takes necessary technical and administrative measures based on technological capabilities and application costs to store the personal data it collects in secure environments. The rules and methods for storing data in a secure environment are detailed in our 'Data Retention and Destruction Policy.

5.1.4. Audits Conducted for the Sustainability of Personal Data Protection

Feedback4E Yazılım Danışmanlık A.Ş., in accordance with Article 12 of the KVKK (Personal Data Protection Law), conducts and commissions necessary audits.

To ensure the sustainability of the Information Security Management System and Personal Data Protection Management Systems, both internal and external audits are carried out. Regular penetration tests are performed to identify potential technical vulnerabilities in the systems. The systems are continuously monitored by the organization. Additionally, system logs are reviewed to ensure security against cyber-attacks. After identifying findings from management system audits, alert system data, and system monitoring, necessary technical and administrative measures are taken. If unlawful access to or

processing of personal data is detected during the audits, it is reported to the Personal Data Protection Committee. The organization's management is then informed by the committee.

5.1.5. Measures Taken in the Event of Unauthorized Disclosure of Personal Data

Feedback4E Yazılım Danışmanlık A.Ş., in accordance with Article 12 of the KVKK (Personal Data Protection Law), notifies the relevant data subject and the KVKK Board in the event of unauthorized disclosure of processed personal data.

If deemed necessary by the KVKK Board, this situation may be announced on the KVKK Board's website or through other methods.

5.1.6. Measures Implemented to Ensure the Protection of Personal Data by Third Parties

Feedback4E Yazılım Danışmanlık A.Ş. includes provisions in its contracts with third parties to prevent the unlawful processing of personal data, prevent unauthorized access to data, and ensure the protection of data. Confidentiality agreements are signed before sharing information with third parties. Necessary notifications are made to third parties to increase their awareness.

5.1.7. Measures Implemented to Protect Special Categories of Personal Data

Special categories of personal data require sufficient measures due to their nature and the potential to cause harm or discrimination to individuals. Article 6 of the KVKK (Personal Data Protection Law) designates certain personal data as 'special categories' due to the risk of causing harm or discrimination if processed unlawfully.

These data include race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and attire, membership in associations, foundations, or unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

Feedback4E Yazılım Danışmanlık A.Ş. takes the necessary measures to protect special categories of personal data as defined by the KVKK and processed lawfully. Special attention is given to these sensitive personal data in both technical and administrative measures.

Feedback4E Yazılım Danışmanlık A.Ş. processes special categories of personal data in accordance with the sufficient measures determined by the KVKK Board. Before processing such data, the explicit consent of the data subject is obtained. If explicit consent is not available, the processing is carried out based on the authority granted by the laws, in compliance with the criteria specified below.

- Special categories of personal data other than the health and sexual life of the data subject may be processed in cases specified by the law,
- Special categories of personal data related to the health and sexual life of the data subject may only be processed for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and their financing. Such data may only be transferred to individuals or authorized institutions and organizations that are under an obligation of confidentiality.

5.1.8. Raising Awareness for Ensuring the Protection of Personal Data

To prevent the unlawful processing of personal data, unauthorized access to data, and to ensure the protection of data, necessary information is provided to business units, training sessions are organized, and activities are monitored to increase awareness. The "Personal Data Protection and Processing Policy" and other related policies are published on our institution's website. Our employees have been informed about this policy.

In case of changes to relevant laws, regulations, or legislation, policies are revised and communicated to employees again.

5.2. Principles for Processing Personal Data

Article 4, Paragraph 2 of the KVKK (Personal Data Protection Law) establishes principles for the processing of personal data. Feedback4E Yazılım Danışmanlık A.Ş. processes personal data in accordance with these established principles.

The processing of personal data is carried out in accordance with the following principles;

a) Compliance with the law and principles of fairness.
b) Accuracy and, where necessary, being up-to-date.

c) Processing for specific, explicit, and legitimate purposes.
d) Being relevant, limited, and proportionate to the purposes for which they are processed.
e) Retaining data only for the period specified by the relevant legislation or as necessary for the purposes for which it is processed.

5.3. Conditions for Processing Personal Data

Feedback4E Yazılım Danışmanlık A.Ş. processes most of its data using the powers it is required to use due to legal obligations and for the protection of public order. According to Article 5/2 of the relevant law, the processing of data is permissible under the following conditions:

a) Explicitly provided by laws.
b) Necessary for the protection of the life or bodily integrity of a person who is unable to express consent due to physical impossibility or whose consent is not legally valid.
c) Necessary for the establishment or performance of a contract, provided it is directly related to the contract and the personal data of the parties to the contract.
d) Necessary for the data controller to fulfill its legal obligations.
e) Made public by the data subject.
f) Necessary for the establishment, exercise, or protection of a right.
g) Necessary for the legitimate interests of the data controller, provided it does not harm the fundamental rights and freedoms of the data subject.

For situations not covered by the above conditions, our institution processes personal data only by obtaining the explicit consent of the data subjects.

5.4. Purposes of Processing Personal Data

Our institution has carried out the necessary activities under KVKK & GDPR, and based on the information received from departments, a data inventory has been created, outlining the purposes necessary for business processes and data processing.
Processing personal data to fulfill a contract or take steps related to a contract we have with you. (According to GDPR Article 6(1), Point 1(b)), data is processed in accordance with Articles 5 and 6 of the Turkish Personal Data Protection Law No. 6698. Our organization will provide information to the data subject in accordance with the clarification text, based on the details specified in the KVKK and GDPR application form submitted by the data subject, upon request.

5.5. Disposal of Personal Data

Our organization will dispose of personal data obtained from data subjects upon their request, unless it is required to be used for legal obligations or the maintenance of public order. Personal data of data subjects will be disposed of based on the decision of the organization when the requirements for continuing to provide service to the customer, fulfilling legal obligations, and planning employee rights and benefits are no longer necessary. The rules and methods for the disposal of personal data are detailed in our "Data Retention and Disposal Policy.

5.6. Transfer of Personal Data to Domestic Recipients

Our organization, with respect to the sharing of personal data with third parties, strictly complies with the conditions regulated under the KVKK (Personal Data Protection Law), while taking into account the provisions set forth in other laws. In this context, personal data will not be transferred to third parties without the explicit consent of the data subject. However, personal data may be transferred without obtaining the explicit consent of the data subject if any of the following conditions regulated by KVKK are met:

- Explicitly provided for by laws,
- Necessity for protecting the life or bodily integrity of a person who is unable to express their consent due to physical impossibility or whose consent is not legally valid, or for protecting another person’s life or bodily integrity,
- Necessity for processing personal data of the parties to a contract, provided that it is directly related to the establishment or performance of the contract,
- Necessity for fulfilling the legal obligations of the data controller,
- Disclosure by the data subject himself or herself,
- Processing of data being necessary for the establishment, exercise, or protection of a right,

- Processing of data being necessary for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject.

In the processing of special categories of personal data, it is also required to take sufficient measures as determined by the Board.

The processing of special categories of personal data is prohibited. However, processing of such data is permissible under the following conditions;

- The data subject has given explicit consent,
- It is expressly provided for by laws,
- It is necessary for the protection of the life or physical integrity of the data subject or another person, where the data subject is unable to give consent due to physical impossibility or legal incapacity,
- It concerns personal data made public by the data subject and is in accordance with the will of making it public,
- It is necessary for the establishment, exercise, or protection of a right,
- It is necessary for public health protection, preventive medicine, medical diagnosis, treatment, and care services, and planning, management, and financing of healthcare services by persons or authorized institutions who are under an obligation of secrecy,
- It is necessary for fulfilling legal obligations in employment, occupational health and safety, social security, social services, and social assistance fields,
- It is conducted by non-profit organizations or formations established for political, philosophical, religious, or union purposes, provided that it is in compliance with the relevant legislation and their objectives, limited to their fields of activity, and not disclosed to third parties; directed towards current or former members and affiliates of these organizations or formations, or individuals in regular contact with these organizations or formations.

The transfer of special categories of personal data must also adhere to the conditions specified for the processing of such data.

5.7. Transfer of Personal Data to Foreign Parties

Personal data may be transferred abroad by data controllers and data processors if one of the conditions specified in Articles 5 and 6 is met and if there is an adequacy decision regarding the country to which the data is to be transferred, the sectors within the country, or international organizations.

The adequacy decision is issued by the Board and published in the Official Gazette. The Board may consult with relevant institutions and organizations if needed. The adequacy decision is reviewed at least once every four years. The Board may, as necessary, modify, suspend, or revoke the adequacy decision with effect for the future, based on the results of the evaluation or in other cases deemed necessary.

When issuing an adequacy decision, the following factors are primarily considered:

a) The reciprocity status regarding the transfer of personal data between the country to which the data will be transferred, sectors within that country, or international organizations, and Turkey.
b) The relevant legislation and practices of the country to which personal data will be transferred, as well as the rules applicable to the international organization to which the personal data will be transferred.
c) The existence of an independent and effective data protection authority in the country to which the personal data will be transferred or the international organization to which the personal data will be transferred, along with the availability of administrative and judicial remedies.
d) The status of the country or international organization to which the personal data will be transferred in terms of being a party to international agreements related to the protection of personal data or membership in relevant international organizations.
e) The status of the country or international organization to which the personal data will be transferred in terms of membership in global or regional organizations to which Turkey is a member.
f) The international treaties to which Turkey is a party.

If adequate protection is not available, personal data may be transferred abroad without the explicit consent of the data subject, provided that data controllers in Turkey and the relevant foreign country give a written commitment to ensure adequate protection and obtain permission from the Board.

In the absence of an adequacy decision, personal data may be transferred abroad if one of the conditions specified in Articles 5 and 6 is met, and if the data subject has the opportunity to exercise their rights and access effective legal remedies in the country to which the data is being transferred, provided that one of the appropriate safeguards listed below is ensured by the parties involved:

a) The existence of an international agreement that is not a treaty between public institutions or organizations abroad or international organizations and public institutions or professional organizations with the status of public institutions in Turkey, and authorization for the transfer by the Board.
b) The presence of binding corporate rules within a group of enterprises engaged in joint economic activities, which include provisions related to the protection of personal data and are approved by the Board, as well as a standard contract that includes details such as data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures to be taken by the data recipient, and additional measures for sensitive personal data, as announced by the Board.
c) The presence of a written commitment containing provisions that ensure adequate protection and authorization for the transfer granted by the Board.

The standard contract must be reported to the Authority by the data controller or data processor within five business days from the date of signing.

Personal data can be transferred abroad only with the permission of the Board and after obtaining the opinion of the relevant public institution or organization, in cases where Turkey or the interests of the data subject would be seriously harmed, except for the provisions of international treaties.

5.8. Categorization of Personal Data

Personal data at Feedback4E Yazılım Danışmanlık A.Ş. is categorized into two groups.

Data Subject Group Categories;

Company Employees: Company employees whose personal data is processed in accordance with relevant legislation, primarily the Labor Law and Occupational Safety regulations.

Former Company Employees: Company employees whose personal data must continue to be processed for a certain period after the termination of their employment contract, in accordance with relevant legislation, primarily the Labor Law and Occupational Safety regulations. This applies even though their employment contract has ended.

Company Service Providers, Suppliers, Subcontractors, and Their Employees: Natural persons or their employees from whom the company receives services or products, or who are subcontractors of the company.

Former Company Service Providers, Suppliers, Subcontractors, and Their Employees: Service providers, suppliers, subcontractors, and their employees whose data continues to be processed due to legal obligations, even though their contractual relationship with the company has ended. Once the legal requirement to process this data is no longer applicable, the data will be deleted or anonymized according to the relevant procedures.

Data Type Categories;

Data Category	Explanation of Personal Data Categorization
Identification Information	Driver's licenses, identity cards, residence permits, passports, bar association IDs, and marriage certificates (e.g., TCKN, passport number, ID card serial number, name, photo, place of birth, date of birth, age, place of registration, detailed copy of the identity card).
Contact Information	Information used for contacting the person (e.g., email address, phone number, mobile phone number, address).
Customer Transaction Information	Information related to every transaction performed by the customer benefiting from our services (e.g., requests, instructions, etc.).
Physical Location Security Information	Personal data related to records and documents collected during entry to a physical location and while staying inside the location (e.g., entry and exit logs, visitor information, camera recordings, etc.).

Transaction Security Information	Personal data processed to ensure the technical, administrative, legal, and commercial security of our organization and relevant parties (e.g., information such as website passwords and access credentials used to associate an individual with a specific transaction and to verify their authorization to perform that transaction)
Financial Information	Personal data within the scope of information, documents, and records showing any financial result generated according to the type of existing legal relationship with the data subject (e.g., information showing the financial result of transactions performed by the data subject, tax debt amount, card information, tax payments, payable interest amount and rate, debt balance, credit balance, etc.)
Personal Details	Personal data essential for the formation of the employment rights of the employees of our organization's suppliers (any information and documents required by law to be included in the personnel file)
Legal Transaction and Compliance Information	Personal data processed for the determination and tracking of legal claims and rights, and for the fulfillment of debts and legal obligations (e.g., data included in documents such as court and administrative authority decisions)
Audit and Inspection Information	Personal data processed in compliance with our organization's legal obligations and company policies (e.g., audit and inspection reports, relevant interview records, and similar documentation)
Special Categories of Personal Data	Data related to individuals' race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.
Request/Complaint Management Information	Personal data related to receiving and evaluating any requests or complaints directed to our organization (e.g., requests and complaints made to our organization, and related records and reports)
Visual and Auditory Data	Visual and auditory records associated with the data subject (e.g., photographs, camera recordings, and audio recordings)

5.9. Printed Documents, Camera Recordings, Personal Data of Website Visitors,

5.9.1. Printed Documents

Our company collects personal data in printed document format in certain situations when providing services to customers. This type of data is processed, stored, and disposed of in accordance with the conditions specified in the KVK (Personal Data Protection) Law.

Personnel personal details used in human resources; Refer to any personal data processed to obtain information essential for the establishment of employment rights for our employees or individuals in a working relationship with our organization.

Data collected for Health Services; Personal data is stored for the health services provided to our employees by the company.

5.9.2. Personal Data of Website Visitors and Personal Data Collected for Internet Access Point Services

On the websites owned by our organization, personal data of visitors is collected to ensure that their visits are conducted appropriately and in line with their intended purposes. Technical means (e.g., cookies) are used to record internet activities on the sites.

Detailed explanations regarding the protection and processing of personal data related to these activities are provided in the "Cookie Policy" texts of the respective websites.

Our company provides free internet services to all visitors at open access points. Personal data is collected in compliance with Law No. 5651 (Regulation of Publications Made on the Internet and Combating Crimes Committed Through These Publications) and for verifying access information.

5.9.3. Rights of the Data Subject

The rights of data subjects, as stipulated in Article 11 of the Law on the Protection of Personal Data (KVKK), which can be accessed in full on the KVKK website, are as follows:

Article 11 - (1) Everyone has the right to apply to the data controller and request information regarding;

a) To learn whether their personal data is being processed,

b) To request information about their processed personal data,

c) To learn the purpose of processing their personal data and whether it is being used in accordance with that purpose,

d) To know the third parties to whom their personal data has been transferred, both domestically and internationally,

e) To request correction of their personal data if it is incomplete or inaccurately processed,

Under GDPR, you have the following rights (more information, you can visit **https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights_en**)

a) Right to Withdraw Consent (Article 7 GDPR
b) Right of Access (Article 15 GDPR)
c) Right to Rectification (Article 16 GDPR)
d) Right to Erasure (Article 17 GDPR)
e) Right to Restrict Processing (Article 18 GDPR)
f) Right to Data Portability (Article 20 GDPR)
g) Right to Object (Article 21 GDPR)

Under GDPR or national laws, these rights 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 own rights), or if you request deletion of data that we are legally required to retain or where there are compelling legitimate interests for its retention. Relevant exemptions are detailed in GDPR or applicable national laws.

If the data controller does not act on a data subject's request, the controller must inform the data subject without undue delay and within one month of receiving the request, explaining the reasons for not taking action and providing information on the right to lodge a complaint with a supervisory authority and seek legal remedies.

Your rights mentioned above can be exercised by completing the "KVKK and GDPR Request Form."

The contact details for the data controller, the data controller's representative, and the data controller are as follows:

In accordance with Article 11 of the Personal Data Protection Law titled "Rights of the Data Subject" and Article 12 of the GDPR, you can submit your requests within the scope of these rights by completing the Feedback4e Application Form in accordance with the "Communiqué on the Principles and Procedures of Applications to the Data Controller."

You may send your written request to the following address:

Harbiye Mahallesi Hüsrev Gerede Caddesi, Tozan Apt. No:77 İç Kapı:16 Şişli/İstanbul

Alternatively, you can submit your request by filling out the "KVKK and GDPR Application Form" on our website or by sending an email to ***kvkk@feedback4e.com.***

5.9.4. The Organization's Obligation to Provide Information and Clarification

Under Article 10 of the Personal Data Protection Law (KVKK), data subjects must be informed before or at the time their personal data is collected. The information that must be provided to data subjects under this obligation includes:

- The identity of the data controller and, if applicable, their representative,
- The purpose of processing the personal data,
- The recipients or categories of recipients to whom the personal data may be transferred and the purpose of such transfers,
- The method of collecting personal data and the legal basis for processing,
- Other rights enumerated in Article 11 of KVKK.

Under Article 28(1) of the Personal Data Protection Law (KVKK), there are certain situations where the obligation to inform data subjects does not apply:

- **Personal data processed by individuals solely for themselves or their family members living in the same household, provided that the data is not shared with third parties and data security obligations are adhered to**,

- **Personal data processed for purposes such as research, planning, and statistics, provided it is anonymized and used for official statistics**,
- **Personal data processed for purposes such as art, history, literature, or scientific research, or within the scope of freedom of expression, as long as it does not violate national defense, national security, public safety, public order, economic security, privacy, or personal rights, or constitute a crime**,
- **Personal data processed by public institutions and organizations authorized by law for preventive, protective, and intelligence activities aimed at national defense, national security, public safety, public order, or economic security**.
- **Personal data processed by judicial authorities or enforcement agencies in connection with investigations, prosecutions, trials, or enforcement proceedings**.

To inform data subjects and obtain their explicit consent, an "Explicit Consent and Information Statement" has been prepared.

5.10. Conditions for the Deletion, Destruction, and Anonymization of Personal Data

Our organization deletes, destroys, or anonymizes personal data upon the request of data subjects, when not required for legal obligations or to maintain public order. The rules and methods for the deletion, destruction, and anonymization of personal data are detailed in our "Data Retention and Destruction Policy."

5.11. Working Principles of the Personal Data Protection Committee

Our organization has established a "Personal Data Protection Committee" to fulfill the requirements of KVKK and GDPR and to maintain compliance.

The primary aims and objectives of the Personal Data Protection Committee are:

- To protect the privacy of personal life
- To safeguard individuals' fundamental rights and freedoms
- To regulate the duties and authorities of those processing data

6. Reference Documents

- Law No. 6698 on the Protection of Personal Data,
- General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")
- Regulation on the Deletion, Destruction, or Anonymization of Personal Data
- Explicit Consent and Information Statement

7. Related Documents

- Data Retention and Destruction Policy