# TEKSERVİS TEKNİK VE TIBBİ ÜRÜNLERİ PAZARLAMA SAN. VE TİC. LTD. ŞTİ.

# (Data Controller)

# PERSONAL DATA PROTECTION AND PROCESSING, RETENTION AND DESTRUCTION POLICY

# TABLE OF CONTENTS

# ABBREVIATIONS AND CONCEPTS

| | |
|---|---|
| KVKK | Law No. 6698 on the Protection of Personal Data, published in the Official Gazette No. 29677 on April 7, 2016 |
| GDPR | EU (European Union) General Data Protection Regulation |
| Constitution | The Constitution No. 2709 of the Republic of Turkey, dated November 7, 1982, published in the Official Gazette No. 17863 on November 9, 1982 |
| Data Processor | A person or unit outside the data controller's organization, responsible for the technical storage, protection, and backup of data, who processes personal data in accordance with the authorization and instructions received from the data controller. |
| Data Subject | Employees, customers, business partners, shareholders, officials, potential |

| | |
|---|---|
| | customers, job applicants, interns, visitors and suppliers of Data Controller and/or its subsidiaries as well as employees of institutions with which they cooperate, third parties, and other persons whose personal data is processed, including but not limited to those listed here. |
| 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. |
| Explicit Consent | Consent that is specific to a particular subject, freely given based on the information provided. |
| Destruction | The deletion, annihilation or anonymization of personal data. |
| Recording Medium | Any medium containing personal data that is processed automatically, either in whole or in part, or by non-automated means as part of a data recording system. |
| Personal Data | Any information relating to an identified or identifiable natural person. |
| Special Categories of Personal Data | Data related to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire, membership in associations, foundations or unions, health, sexual life, criminal convictions and imposed security measures, as well as biometric and genetic data. |
| Processing of Personal Data | Any operation performed on personal data, such as the collection, recording, storage, retention, alteration, reorganization, disclosure, transfer, acquisition, making available, classification, or restriction of use of such data, by fully or partially automated means or non-automated means, provided it is part of a data recording system. |
| Anonymization of Personal Data | The process of rendering personal data unidentifiable, such that it cannot be associated with any identified or identifiable natural person, even when combined with other data. |
| Deletion of Personal Data | The process of rendering personal data inaccessible and unusable to relevant users. |
| Destruction of Personal Data | The process of rendering personal data inaccessible, unrecoverable, and unusable by anyone. |
| Periodic Destruction | The ex officio process of deleting, destroying, or anonymizing personal data at regular intervals when all conditions for processing personal data specified in the law no longer apply. |
| Regulation | The Regulation on the Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette No. 30224 dated October 28, 2017, and effective as of January 1, 2018. |
| KVK Board / Board | Personal Data Protection Board |
| KVK Institution | Personal Data Protection Institution |
| Policy | Data Controller's Personal Data Protection and Processing Policy |
| Data Controller | TEKSERVİS TEKNİK VE TIBBİ ÜRÜNLERİ PAZARLAMA SAN. VE TİC. LTD. ŞTİ. |
| Turkish Penal Code | The Law No. 5237 dated September 26, 2004, published in the Official Gazette No. 25611 on October 12, 2004. |

# 1. INTRODUCTION

## 1.1. Purpose

As the Data Controller, we are aware of our responsibility to protect and legally safeguard personal data, which is regulated as a constitutional right, and we attach great importance to the secure use of your personal data.

The purpose of this policy is to establish the methods and principles to be followed to ensure that the Data Controller processes and protects personal data in compliance with the Personal Data Protection Law (KVKK) published in the Official Gazette No. 29677 on April 7, 2016.

The idea is to ensure full compliance with the legislation in the processing and protection of personal data by the Data Controller and to protect all rights of the data subjects regarding personal data arising from the legislation.

## 1.2. Scope

This Policy applies to all activities carried out by the DATA CONTROLLER for the processing and protection of personal data.

It covers real persons whose personal data is processed by the Data Controller, either automatically or by non-automatic means as part of a data recording system. This Policy shall in no way apply to legal entities and their data.

This policy is implemented by the DATA CONTROLLER in conjunction with detailed data procedures in all activities related to the processing and protection of personal data.

## 1.3. Implementation of the Policy and the Relevant Legislation

The applicable regulations regarding the processing and protection of personal data shall be implemented. The Data Controller accepts that in the event of any inconsistency between the applicable legislation and the Policy, the applicable legislation shall take precedence.

## 1.4. Force of the Policy

In the event of a revision of the entire Policy or specific articles thereof, the effective date of the Policy shall be updated. The Policy is published on the Data Controller's website at www.tekservis.com and is made available to data subjects upon request.

# 2. MATTERS CONCERNING PROTECTION OF PERSONAL DATA

The Data Controller takes the necessary technical and administrative measures to ensure an appropriate level of security in order to prevent the unlawful processing of personal data, prevent unlawful access to data and ensure the protection of data, in accordance with Article 12 of the KVKK, and conducts or commissions the necessary audits within this scope.

## 2.1. Security of Personal Data

### 2.1.1. Technical and Administrative Measures Taken to Ensure the Lawful Processing of Personal Data, Prevent Unlawful Access and Store Data in Secure Environments

The Data Controller takes technical and administrative measures, depending on its technological capabilities and application costs, to ensure the lawful processing of personal data, prevent unlawful access to such data and store it in secure environments.

#### 2.1.1.1. Technical Measures Taken to Ensure the Lawful Processing of Personal Data, Prevent Unlawful Access and Store Data in Secure Environments

The main technical measures taken by the Data Controller to ensure the lawful processing of personal data, prevent unlawful access to such data, and store it in secure environments are listed below:

- Network security and application security are provided;
- Key management is implemented;
- Closed system networks are used for personal data transfers via the network;
- Security measures are taken for the procurement, development and maintenance of information technology systems;
- Security of personal data stored in the cloud is ensured;
- Access logs are kept regularly;
- Up-to-date anti-virus systems are used;
- Firewalls are used;
- Personal data is backed up and the security of the backed-up personal data is also ensured;
- User account management and authorization control systems are implemented and monitored;
- Log records are kept without user intervention;
- Intrusion detection and prevention systems are used.

#### 2.1.1.2. Administrative Measures Taken to Ensure the Lawful Processing of Personal Data, Prevent Unlawful Access and Store Data in Secure Environments

The main administrative measures taken by the Data Controller to ensure that personal data is processed in accordance with the law, to prevent unlawful access to such data and to store it in secure environments are listed below:

- disciplinary measures related to data security are in place for employees;
- confidentiality agreements are concluded;
- disciplinary regulations containing data security provisions for employees are in place;
- training and awareness-raising activities on data security are conducted at regular intervals for employees;
- an authorization matrix is in place for employees;
- corporate policies on access, information security, use, storage, and destruction have been formulated and implemented;
- the authorizations of employees who have switched to other positions or left the company are revoked;
- signed contracts include data security provisions;
- extra security measures are taken for personal data transferred on paper, and the relevant documents are sent in a confidential document format.

- personal data security policies and procedures have been formulated;
- personal data security issues are reported quickly;
- personal data security is monitored;
- the necessary security measures are taken regarding access to physical environments containing personal data;
- the security of physical environments containing personal data is ensured against external risks (fire, flood, etc.);
- the security of environments containing personal data is ensured;
- personal data is minimized as much as possible;
- periodic and/or random internal audits are conducted and commissioned;
- current risks and threats have been identified;
- protocols and procedures for the security of special categories of personal data have been determined and are being implemented;
- data processing service providers are audited at regular intervals regarding data security;
- data processing service providers are made aware of data security issues;

### 2.1.2. Inspection of Measures for Protection of Personal Data

The Data Controller conducts or commissions the necessary audits within its own organization in accordance with Article 12 of the KVKK. The results of the audits are reported to the relevant department within the Data Controller's internal operations, and the necessary activities are carried out to improve the measures taken.

### 2.1.3. Measures Taken in Case of Unauthorized Disclosure of Personal Data

The Data Controller operates a system that ensures that, in accordance with Article 12 of the KVKK, the Data Controller notifies the Data Subject and the KVK Board as soon as possible in the event that personal data processed by the Data Controller is obtained by others through unlawful means.

### 2.2. Safeguarding the Rights of Data Subjects, Creating Channels for Data Subjects to Communicate Their Rights to the Data Controller and Evaluating Data Subjects' Requests

The Data Controller implements the necessary channels, internal procedures, administrative and technical regulations in accordance with Article 13 of the KVKK to evaluate the rights of data subjects and provide them with the necessary information.

If the data subjects submit their requests regarding their rights listed below in writing to the Data Controller, the Data Controller will respond to the request free of charge as soon as possible and no later than thirty days, depending on the nature of the request. However, if the process entails additional costs, the Data Controller will charge the fee determined by the KVK Board. Data subjects have the right to:

- learn whether their personal data is being processed;
- seek information on how their personal data has been processed;
- learn the purpose of processing personal data and whether it is used in accordance with that purpose;

- know the third parties to whom their personal data is transferred domestically or abroad;
- request correction of their personal data in case of incomplete or incorrect processing, and demand that the action taken in this regard be communicated to the third persons to which their personal data was transferred;
- request deletion or destruction of their personal data although it was processed in accordance with the provisions of the KVKK and other laws in case of disappearance of the reasons for processings, and demand that the action taken in this regard be communicated to the third persons to which their personal data was transferred;
- challenge any result to their detriment upon analysis of their processed personal data exclusively through automated systems;
- claim compensation for their damages arising from unlawful processing of their personal data.

Detailed information regarding the rights of data subjects is provided in Section 10 of this Policy.

**2.3. Protection of Special Categories of Personal Data**

KVKK attaches special importance to certain personal data due to the risk of causing harm or discrimination to individuals if processed unlawfully.

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

The Data Controller handles the protection of special categories of personal data, defined by the KVKK and processed in accordance with the law, with the utmost care. In this context, the technical and administrative measures taken by the Data Controller to protect personal data are carefully implemented, paying attention to the protection of special categories of personal data, and the necessary inspections are done within the Data Controller.

Pursuant to the Board's Decision No. 2018/10 dated January 31, 2018, the Data Controller takes the following measures regarding the processing of Special Categories Personal Data, as specified in Article 6 of the Law:

- A systematic, clearly defined, manageable, and sustainable policy has been formulated for the security of special categories of personal data.
- A policy has been formulated for employees involved in the processing of special categories of personal data.
- A policy has been formulated for the protection and processing of special categories of personal data in electronic media where such data is processed, stored and/or accessed.
- A policy has been formulated for the necessary protection of special categories of personal data in physical environments where such data is processed, stored and/or accessed.
- If Special Categories of Personal Data are to be transferred, this will be done in accordance with the respective Policies.

### 2.4. Raising Awareness Among and Inspection of Business Units Regarding the Protection and Processing of Personal Data

The Data Controller ensures that the necessary training is provided to business units to raise awareness about the prevention of unlawful processing of personal data, unlawful access to data and the protection of data.

The Data Controller establishes the necessary systems to raise awareness among current employees and new employees who have recently joined the business units regarding the protection of personal data, and works with professionals when necessary.

The Data Controller is informed of the results of training conducted to raise awareness about the protection and processing of personal data within the business units. In this regard, the Data Controller evaluates participation in relevant training sessions, seminars and information sessions, and conducts or commissions the necessary audits. The Data Controller updates and renews its training in line with the revisions to the relevant legislation.

## 3. MATTERS RELATED TO THE PROCESSING OF PERSONAL DATA

In accordance with Article 20 of the Constitution and Article 4 of the KVKK, the Data Controller processes personal data in a manner that is lawful and fair, accurately and, where necessary, in an up-to-date fashion, for specific, explicit and legitimate purposes, and in a manner that is relevant, limited, and proportionate to the purpose. The Data Controller retains personal data for the period specified by law or as required by the purpose of processing personal data.

The Data Controller processes personal data in accordance with Article 20 of the Constitution and Article 5 of the KVKK, based on one or more of the conditions set forth in Article 5 of the KVKK regarding the processing of personal data.

The Data Controller informs the data subjects in accordance with Article 20 of the Constitution and Article 10 of the KVKK and provides the necessary information when requested by the data subjects.

The Data Controller acts in accordance with the regulations for the processing of special categories of personal data in accordance with Article 6 of the KVKK.

The Data Controller acts in accordance with the provisions of the law and regulations by the KVK Board regarding the transfer of personal data, in accordance with Articles 8 and 9 of the KVKK.

### 3.1. Processing of Personal Data in Accordance with the Principles Set Forth in the Legislation

#### 3.1.1. Processing in Compliance with the Law and Rules of Good Faith

The Data Controller acts in accordance with the principles established by regulations and the general rules of trust and honesty in the processing of personal data. In this context, the Data

Controller takes into account the requirements of proportionality in the processing of personal data and does not use personal data for purposes other than those specified.

### 3.1.2. Ensuring Accuracy and, Where Necessary, Up-to-dateness of Personal Data

The Data Controller ensures that the personal data it processes is accurate and up-to-date, taking into account the fundamental rights of the data subjects and its own legitimate interests. It takes the necessary measures in this regard.

### 3.1.3. Processing for Specific, Clear and Legitimate Purposes

The Data Controller clearly and precisely determines the legitimate and lawful purpose of processing personal data. The Data Controller processes personal data to the extent necessary for and associated with the services it provides. The purpose for which personal data will be processed by the Data Controller is determined before the processing of personal data begins.

### 3.1.4. Processing in a Manner That Is Relevant, Limited and Proportionate to the Purpose for Which the Data is Processed

The Data Controller processes personal data in a manner that is appropriate for achieving the specified purposes and avoids processing personal data that is not relevant or necessary for achieving the purposes.

### 3.1.5. Retention for the Period Required by Applicable Legislation or Necessary for the Purpose for Which the Data is Processed

The Data Controller retains personal data only for as long as specified in the applicable legislation or as necessary for the purpose for which it is processed. In this context, the Data Controller first determines whether the applicable legislation specifies a period for the storage of personal data, and if so, acts in accordance with that time requirement. If no period is specified, the Data Controller retains personal data for as long as necessary for the purpose for which it is processed. Upon the expiration of the period or the cessation of the reasons for processing, personal data is deleted, destroyed or anonymized by the Data Controller. Personal data is not retained by the Data Controller for future use. Detailed information on this subject is provided in Section 9 of this Policy.

## 3.2. Processing Personal Data Based on and Limited to One or More of the Conditions for Processing Specified in Article 5 of the KVKK

The protection of personal data is a constitutional right. Fundamental rights and freedoms may only be restricted by law for the reasons specified in the relevant articles of the Constitution, without affecting their essence. Pursuant to the third paragraph of Article 20 of the Constitution, personal data may only be processed in cases provided for by law or with the explicit consent of the individual. The Data Controller processes personal data in accordance with this principle and in compliance with the Constitution, only in cases provided for by law or with the explicit consent of the individual. Detailed information on this subject is provided in Section 7 of this Policy.

## 3.3. Informing the Data Subject

The Data Controller informs the data subjects during the collection of personal data in accordance with Article 10 of the KVKK In this context, the Data Controller and, if applicable, its representative provide information about their identity, the purpose for which personal data will be processed, to whom and for what purpose the processed personal data may be transferred, the method of and the legal basis for collecting personal data, and the rights of the data subject. Detailed information on this subject is provided in Section 10 of this Policy.

Article 20 of the Constitution provides that everyone has the right to be informed about personal data concerning themselves. In this regard, Article 11 of the KVKK lists "requesting information" among the rights of the Data Subject. Within this scope, the Data Controller provides the necessary information when the Data Subject requests information in accordance with Article 20 of the Constitution and Article 11 of the KVKK. Detailed information on this subject is provided in Section 10 of this Policy.

### 3.4. Processing of Special Categories of Personal Data

When processing personal data classified as "special category" under the KVKK, the Data Controller acts in strict compliance with the provisions of the KVKK.

Article 6 of the KVKK defines certain personal data that, when processed unlawfully, may cause harm or discrimination to individuals as "special categories of personal data." These types of data include race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire and clothing, membership in associations, foundations or unions, health, sexual life, criminal convictions and imposed security measures, as well as biometric and genetic data.

Subject to the implementation of sufficient measures determined by the KVK Board, special categories of personal data are processed by the Data Controller in compliance with the KVKK:

- If the Data Subject has given explicit consent; or
- In case the Data Subject has not given explicit consent:
    - Special categories of personal data other than those relating to the health and sexual life of the Data Subject are processed in cases provided for by the laws;
    - Special categories of personal data relating to the health and sexual life of the Data Subject may only be processed by persons or authorized institutions and agencies subject to confidentiality obligations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of health services and their financing.

### 3.5. Transfer of Personal Data

The Data Controller may transfer the Special Categories of Personal Data obtained in accordance with the law to third parties in line with the purposes of data processing, after taking the necessary security measures (see 2.1). The Data Controller acts in accordance with the provisions of Article 8 of the KVKK. Detailed information on this subject is provided in Section 6 of this Policy.

### 3.5.1. Transfer of Personal Data

The Data Controller may transfer personal data to third parties based on and limited to one or more of the personal data processing conditions specified in Article 5 of the Law and given below, in accordance with legitimate and lawful purposes of processing personal data:

- If the Data Subject has given explicit consent;
- If there is an explicit provision in the law regarding the transfer ofpersonal data;
- If it is necessary to protect the life or physical integrity of the Data Subject or another person, and the Data Subject is unable to express their consent due to actual impossibility or their consent is not legally valid;
- If the transfer of personal data belonging to the parties to a contract is necessary for the establishment or performance of the contract;
- If the Data Controller is legally obligated to transfer personal data;
- If the Personal Data has been made public by the Data Subject;
- If the transfer of personal data is necessary for the establishment, exercise or protection of a right;
- If the transfer of personal data is necessary for the legitimate interests of the Data Controller, provided that it does not harm the fundamental rights and freedoms of the Data Subject.

### 3.5.2. Transfer of Special Categories of Personal Data

The Data Controller may transfer the Data Subject's special categories of personal data to third parties, in accordance with legitimate and lawful purposes of processing Personal Data, by exercising due care and after taking the necessary security measures (see 2.1), and implementing the adequate safeguards prescribed by the KVK Board, in the following circumstances:

- If the Data Subject has given explicit consent; or
- In case the Data Subject has not given explicit consent:
    - Special categories of personal data other than the Data Subject's health and sexual life (race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire and clothing, membership in associations, foundations or trade unions, criminal convictions and imposed security measures, as well as biometric and genetic data), in cases provided for by law;
    - Special categories of personal data relating to the health and sexual life of the Data Subject may only be processed by persons or authorized institutions and agencies subject to confidentiality obligations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of health services and their financing.

### 3.6. Transfer of Personal Data Abroad

The Data Controller may transfer the Data Subject's personal data and special categories of personal data obtained in accordance with the law to third parties in line with the purposes of data processing, after taking the necessary security measures (see 2.1).

Personal data is transferred by the Data Controller to foreign countries that have been declared by the KVK Board to have adequate protection, or to foreign countries where adequate protection is not available, provided that the data controllers in Turkey and the relevant foreign country have made a written commitment to provide adequate protection and the KVK Board has given its permission ("Foreign Country Where the Data Controller Commits to Adequate Protection"). The Data Controller acts in accordance with the provisions of Article 9 of the KVK in this regard.

### 3.6.1. Transfer of Personal Data Abroad

The Data Controller may transfer personal data to Foreign Countries with Adequate Protection or Foreign Countries with Data Controllers Committing to Adequate Protection in accordance with the legitimate and lawful purposes of processing personal data if the Data Subject has given their explicit consent or, in the event of one of the following circumstances if the Data Subject has not given their explicit consent:

- If there is an explicit provision in the law regarding the transfer ofpersonal data;
- If it is necessary to protect the life or physical integrity of the Data Subject or another person, and the Data Subject is unable to express their consent due to actual impossibility or their consent is not legally valid;
- If the transfer of personal data belonging to the parties to a contract is necessary for the establishment or performance of the contract;
- If the Data Controller is legally obligated to transfer personal data;

### 3.6.2. Transfer of Special Categories of Personal Data Abroad

The Data Controller may transfer the Data Subject's special categories of personal data to Foreign Countries with Adequate Protection or Foreign Countries with Data Controllers Committing to Adequate Protection, in accordance with legitimate and lawful purposes of processing Personal Data, by exercising due care and after taking the necessary security measures (see 2.1), and implementing the adequate safeguards prescribed by the KVK Board, in the following circumstances:

- If the Data Subject has given explicit consent; or
- In case the Data Subject has not given explicit consent:
    - Special categories of personal data other than the Data Subject's health and sexual life (race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire and clothing, membership in associations, foundations or trade unions, criminal convictions and imposed security measures, as well as biometric and genetic data), in cases provided for by law;
    - Special categories of personal data relating to the health and sexual life of the Data Subject may only be transferred for processing by persons or authorized institutions and agencies subject to confidentiality obligations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of health services and their financing.

## 4. CATEGORIZATION, PROCESSING PURPOSES AND RETENTION PERIODS OF PERSONAL DATA PROCESSED BY THE DATA CONTROLLER

The Data Controller informs the Data Subject of which Data Subject groups' personal data it processes, the purposes of processing the Data Subject's personal data, and the retention periods, in accordance with the obligation to inform under Article 10 of the KVKK.

### 4.1. Categorization of Personal Data

In accordance with Article 10 of the KVKK, the Data Controller informs the data subjects and processes the following categories of personal data in accordance with the legitimate and lawful purposes of the Data Controller, based on one or more of the conditions for processing personal data specified in Article 5 of the KVKK and limited to the KVKK, in compliance with the principles specified in Article 4 of the KVKK regarding the processing of personal data, the general principles specified in the KVKK, all obligations provided for by the KVKK, and the time limits specified herein. The data subjects to whom such categories of personal data processed are related hereunder are also specified in Section 5 of this Policy.

| Categorization of Personal Data | Description |
|---|---|
| Identity Information | Data that clearly belongs to an identified or identifiable natural person, processed partially or entirely automatically or non-automatically as part of a data recording system, containing information about the person's identity, including documents such as driver's licenses, identity cards and passports containing information such as name, surname, ID number, nationality, mother's name, father's name, place of birth, date of birth, gender, as well as information such as tax number, social security number, signature, vehicle license plate, etc. |
| Contact Information | Data that clearly belongs to an identified or identifiable natural person, processed partially or fully automatically or non-automatically as part of a data recording system, such as phone number, address, email address, fax number, IP address, etc. |
| Financial Information | Personal data processed in a manner that is fully or partially automated or non-automated as part of a data recording system, which clearly belongs to an identified or identifiable natural person, including any information, documents and records related to financial outcomes created based on the type of legal relationship established between our Company and the data subject, as well as bank account numbers, IBAN number, credit card information, financial profile, asset data, income information, etc. |
| Personnel Information | Personal data that is clearly attributable to an identified or identifiable natural person, processed partially or entirely automatically or non-automatically as part of a data recording system for the purpose of obtaining information that will form |

| | |
|---|---|
| | the basis of the personal rights of natural persons who have an employment relationship with our company |
| Security of Physical Spaces | Personal data belonging to an identified or identifiable natural person, processed partially or entirely automatically or non-automatically as part of a data recording system, including personal data related to records and documents obtained before entry into a physical location and during stay within the physical location as well as camera footage, recordings obtained at security checkpoints, etc. |
| Action Security Information | Personal data such as IP address information, website access information, and password information processed for the technical, administrative, legal and commercial security of both the Data Subject and the Data Controller while the Data Controller carries out its activities |
| Professional Experience Information | Data that clearly belongs to an identified or identifiable natural person, processed partially or entirely automatically or non-automatically as part of a data recording system, depending on the type of legal relationship established between the Company and the Data Subject, such as diploma information, courses attended, professional training information, certificates, candidate application forms, reference interview information, job interview information, and transcript information |
| Health Information | Health data that clearly belongs to an identified or identifiable natural person, processed either partially or entirely automatically or non-automatically as part of a data recording system, obtained in relation to the goods and services offered by the Company within the scope of operations conducted by the Company's business units for the purpose of conducting the business processes of natural persons who are in an employment relationship with the Company or protecting the legal and other interests of the Company and the Data Subject, including health reports, disability tax exemption documents, insurance documents and military status documents of the Data Subject and/or their family members |
| Location Information | Personal data that clearly belongs to an identified or identifiable natural person, processed partially or entirely automatically or non-automatically as part of a data recording system, which determines the location of the data subject while using products and services or while using employee vehicles, within the framework of operations carried out by the data subject's business units, including GPS location, travel data, etc. |
| Other | Personal data that clearly belongs to an identified or identifiable natural person, processed either partially or enitrely automatically or non-automatically as part of a data recording system, and that does not falling into any category. |

**4.2. Purposes of Processing Personal Data**

The Data Controller processes personal data within the scope of the purposes and conditions specified in Article 5, paragraph 2 and Article 6, paragraph 3 of the KVKK. Your personal data will be processed if:

- the processing of your personal data by the Data Controller is explicitly provided for in the laws;
- the processing of your personal data by the Data Controller is necessary for and directly related to the establishment or performance of a contract;
- the processing of your personal data is necessary for the Data Controller to fulfill its legal obligations;
- the processing by the Data Controller is done in a manner limited to the purpose of making it public, provided that it has been made public by you;
- the processing of your personal data by the Data Controller is necessary to establish, exercise or protect the rights of the Data Controller, you or third parties;
- the processing of your personal data is necessary for the legitimate interests of the Data Controller, provided that this does not harm your fundamental rights and freedoms;
- the processing of your personal data by the Data Controller is necessary to protect the life or physical integrity of the Data Subject or another person, and if the Data Subject is unable to give consent due to actual or legal incapacity;
- the processing of special categories of personal data other than those relating to the Data Subject's health and sexual life is provided for by law;
- special categories of personal data relating to the health and sexual life of the Data Subject are processed by persons or authorized institutions and agencies subject to confidentiality obligations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of health services and their financing.

In this context, the Data Controller processes your personal data for the following purposes:

PURPOSES OF PROCESSING
conduct employee candidate/intern/student selection and placement processes;
execute the application processes of job applicants;
manage information security processes;
fulfill the obligations arising from employment contracts and legislation for employees;
conduct the processes related to fringe benefits and interests for employees;
carry out training activities;
conduct finance and accounting operations;
plan human resources processes;
execute/monitor business operations;
carry out occupational health/safety activities;
manage organizations and events;
conduct information security processes;
ensure security of physical premises;
conduct goods/services procurement processes;

conduct goods/services sales processes;
carry out management activities;
monitor and conduct legal affairs;
carry out communication activities;
conduct contract processes;
provide goods/services post-sales support services.

If the processing activity carried out for the aforementioned purposes does not meet any of the conditions specified in the KVKK, the Data Controller will obtain your explicit consent regarding the processing process.

**4.3. Retention of Personal Data**

**4.3.1. Retention Periods of Personal Data**

The Data Controller retains personal data for the periods specified in the relevant laws and regulations, if required by such laws and regulations. The retention, destruction and periodic destruction periods determined by the Data Controller are specified below:

| Activity | Retention Period | Destruction Period |
|---|---|---|
| Carry out job application processes | 6 months | End of retention period |
| Carry out job application processes | 6 months | Within the 30-day response time after a deletion request |
| Carry out job application processes | 6 months | First periodic destruction after the end of retention period |
| Personnel | 15 years from the end of legal relationship | End of retention period |
| Personnel | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Training Activities | 15 years from the end of legal relationship | End of retention period |
| Training Activities | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Training activities | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Timekeeping entry process | 15 years from the end of legal relationship | End of retention period |
| Timekeeping entry process | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Social event | 1 year | End of retention period |
| Social event | 1 year | Within the 30-day response time after a deletion request |
| Social event | 1 year | First periodic destruction after the end of retention period |
| Preparation of payrolls and salary file | 15 years from the end of | End of retention period |

| | | |
|---|---|---|
| | legal relationship | |
| Preparation of payrolls and salary file | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Preparation of payrolls and salary file | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Email generation process | 1 year | End of retention period |
| Email generation process | 1 year | Within the 30-day response time after a deletion request |
| Email generation process | 1 year | First periodic destruction after the end of retention period |
| Camera footage | 1 month | End of retention period |
| Camera footage | 1 month | Within the 30-day response time after a deletion request |
| Camera footage | 1 month | First periodic destruction after the end of retention period |
| Waybill and invoice process | 10 years from the end of legal relationship | End of retention period |
| Waybill and invoice process | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Waybill and invoice process | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Power of attorney process | 1 year | End of retention period |
| Power of attorney process | 1 year | Within the 30-day response time after a deletion request |
| Power of attorney process | 1 year | First periodic destruction after the end of retention period |
| Contract | 10 years from the end of legal relationship | End of retention period |
| Contract | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Contract | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Order and contract | 10 years from the end of legal relationship | End of retention period |
| Order and contract | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Order and contract | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Creation of a current account card | 10 years from the end of legal relationship | End of retention period |
| Creation of a current account card | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Creation of a current account card | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Opening a current account | 10 years from the end of | End of retention period |

| | | |
|---|---|---|
| | legal relationship | |
| Opening a current account | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Opening a current account | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Vehicle and visitor logging | 3 months | End of retention period |
| Vehicle and visitor logging | 3 months | Within the 30-day response time after a deletion request |
| Vehicle and visitor logging | 3 months | First periodic destruction after the end of retention period |
| Receipt of mails and notices | 1 month | End of retention period |
| Receipt of mails and notices | 1 month | Within the 30-day response time after a deletion request |
| Receipt of mails and notices | 1 month | First periodic destruction after the end of retention period |
| Vehicle tracking system processes | 1 month | End of retention period |
| Vehicle tracking system processes | 1 month | Within the 30-day response time after a deletion request |
| Vehicle tracking system processes | 1 month | First periodic destruction after the end of retention period |
| Order and contract process | 10 years from the end of legal relationship | End of retention period |
| Order and contract process | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Order and contract process | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Training organization and event process | 1 year | End of retention period |
| Training organization and event process | 1 year | Within the 30-day response time after a deletion request |
| Training organization and event process | 1 year | First periodic destruction after the end of retention period |
| Check phone lines | 1 year | End of retention period |
| Check phone lines | 1 year | Within the 30-day response time after a deletion request |
| Check phone lines | 1 year | First periodic destruction after the end of retention period |
| Recruitment examination process | 15 years from the end of legal relationship | End of retention period |
| Recruitment examination process | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Recruitment examination process | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Recruitment periodic examination | 15 years from the end of legal relationship | End of retention period |

| | | |
|---|---|---|
| Recruitment periodic examination | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Recruitment periodic examination | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Occupational health and safety training and activities | 15 years from the end of legal relationship | End of retention period |
| Occupational health and safety training and activities | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Occupational health and safety training and activities | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Work accident reporting | 15 years from the end of legal relationship | End of retention period |
| Work accident reporting | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Work accident reporting | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Work accident and occupational disease | 15 years from the end of legal relationship | End of retention period |
| Work accident and occupational disease | 15 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Work accident and occupational disease | 15 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Proposal, order and contract | 10 years from the end of legal relationship | End of retention period |
| Proposal, order and contract | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Proposal, order and contract | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Waybill and invoice process | 10 years from the end of legal relationship | End of retention period |
| Waybill and invoice process | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Waybill and invoice process | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Receipt | 1 year | End of retention period |
| Receipt | 1 year | Within the 30-day response time after a deletion request |
| Receipt | 1 year | First periodic destruction after the end of retention period |
| Insurance/logistics/customs | 10 years from the end of legal relationship | End of retention period |
| Insurance/logistics/customs | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Insurance/logistics/customs | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |

| | | |
|---|---|---|
| Proposal, order and contract | 10 years from the end of legal relationship | End of retention period |
| Proposal, order and contract | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Proposal, order and contract | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Waybill and invoice process | 10 years from the end of legal relationship | End of retention period |
| Waybill and invoice process | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Waybill and invoice process | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Creation of a tender file | 10 years from the end of legal relationship | End of retention period |
| Creation of a tender file | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Creation of a tender file | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |
| Post-sales process | 10 years from the end of legal relationship | End of retention period |
| Post-sales process | 10 years from the end of legal relationship | Within the 30-day response time after a deletion request |
| Post-sales process | 10 years from the end of legal relationship | First periodic destruction after the end of retention period |

In this context, personal data is retained for the minimum retention periods required by law:

If no retention period is specified in the legislation regarding how long personal data must be retained, the Data Controller processes the data for as long as necessary in accordance with its practices and commercial customs related to the activities carried out while processing the data, and then deletes, destroys or anonymizes it. Detailed information on this subject is provided in Section 9 of this Policy.

If the purpose of processing personal data no longer apllies and the retention periods specified by the relevant legislation and the Data Controller have also ended, personal data may only be retained for the purpose of serving as evidence in potential legal disputes or for asserting or defending rights related to personal data. In determining these periods, the limitation periods for asserting the aforementioned right are taken into account, and even if the limitation periods have expired, the retention periods are determined based on examples of previous requests made to the Data Controller on the same issues. In this case, the retained personal data is not accessed for any other purpose and access to the relevant personal data is only provided when it is necessary for the legal dispute. Again, personal data is deleted, destroyed or anonymized after the aforementioned period has expired,.

**4.3.2. Distribution of Responsibilities and Tasks**

All units and employees of the Data Controller provide responsible units with support in taking technical and administrative measures to ensure that the technical and administrative

measures taken by the responsible units under the Policy are implemented as required, that unlawful processing of personal data is prevented by increasing the training and awareness of unit employees as well as monitoring and continuously supervising them, that unlawful access to personal data is prevented, and that personal data is stored lawfully.

### 4.3.3. Storage Environments

Personal data belonging to individuals is stored securely by the Data Controller in the environments listed in the table below, in accordance with the provisions of the KVKK and other relevant legislation:

| Storage Environments |
|---|
| Hard disk |
| Lockable archive cabinet |
| Company server |

## 5. CATEGORIZATION CONCERNING OWNERS OF PERSONAL DATA PROCESSED BY THE DATA CONTROLLER

| Data Subject Category | Description |
|---|---|
| Full Name | Potential Employee<br>Employee<br>Customer<br>Supplier Official<br>Visitor<br>Supplier Personnel<br>Potential Customer |
| ID No | Potential Employee<br>Employee<br>CUSTOMER<br>Supplier Official |
| Date of Birth | Potential Employee<br>Employee |
| Place of Birth | Potential Employee<br>Employee |
| Gender | Potential Employee<br>Employee |
| Marital Status | Potential Employee<br>Employee |
| Identity Details | Potential Employee<br>Employee<br>Customer<br>Supplier Official |
| Email | Potential Employee<br>Employee<br>Customer |

| | |
|---|---|
| Telephone Number | Supplier Official<br>Supplier Personnel<br>Potential Customer<br>Potential Employee<br>Employee<br>Customer<br>Supplier Official<br>Visitor<br>Supplier Personnel<br>Potential Customer |
| Address | Potential Employee<br>Employee<br>Customer<br>Supplier Official |
| Occupation | Potential Employee<br>Employee |
| CV Details | Potential Employee<br>Employee |
| Educational Background Details | Potential Employee<br>Employee |
| Diploma and Certificate Details | Potential Employee<br>Employee |
| Visual Record | Potential Employee<br>Employee |
| Diploma Details | Potential Employee |
| Courses Attended | Potential Employee |
| On-the-job Training Details | Potential Employee |
| Certificates | Potential Employee<br>Employee |
| Photograph | Potential Employee<br>Employee |
| Signature | Employee<br>Customer<br>Supplier Official<br>Supplier Personnel |
| Social Security Registration Number | Employee |
| Residence Certificate | Employee |
| GPS Vehicle Record | Employee |
| Reference Information | Employee |
| Recruitment/Termination Records | Employee |
| Performance Evaluation Reports | Employee |
| Timekeeping Information | Employee |
| Proceedings and Execution File Information | Employee |

| | |
|---|---|
| Military Service Status | Employee |
| Number of Children | Employee |
| Bank Account Details | Employee<br>Customer<br>Supplier Official |
| Personal Health Information | Employee |
| Title | Employee<br>Customer<br>Supplier Official |
| Imagery Data | Employee |
| Payroll Details | Employee |
| Password Information | Employee |
| Tax Office | Customer<br>Supplier Official |
| Contact Address | Customer<br>Supplier Official<br>Employee |
| Debt/Credit Information | Customer<br>Supplier Official |
| Vehicle Plate No. | Visitor |
| Location Information | Employee |
| Passport Number | Employee |

## 6. THIRD PARTIES TO WHOM PERSONAL DATA IS TRANSFERRED BY THE DATA CONTROLLER AND THE PURPOSES OF TRANSFER

The Data Controller informs the Data Subject of the groups of persons to whom personal data is transferred in accordance with Article 10 of the KVKK.

The Data Controller may transfer the personal data of data subjects governed by the Policy to the following categories of persons in accordance with Articles 8 and 9 of the KVKK (see Section 3/Heading 3.5):

- Domestic Recipients: Authorized Public Institutions and Agencies
- International Recipients: No transfers are made internationally.

In transfers carried out by the Data Controller, actions are taken in accordance with the provisions set forth in Sections 2 and 3 of the Policy.

## 7. PROCESSING PERSONAL DATA BASED ON AND LIMITED TO THE CONDITIONS FOR PROCESSING SPECIFIED IN THE LAW

The Data Controller informs the Data Subject about the personal data it processes in accordance with Article 10 of the KVKK.

### 7.1. Processing of Personal Data and Special Categories of Personal Data

### 7.1.1. Processing of Personal Data

The Data Subject's explicit consent is only one of the legal bases that enable the lawful processing of personal data. In addition to explicit consent, personal data may also be processed if one of the other conditions listed below is met. The basis for personal data processing activities may be any one of the conditions listed below, or more than one of these conditions may serve as the basis for the same personal data processing activity. If the processed data is among the special categories of personal data, the conditions set out under the heading 7.1.2. in this section will apply.

Although the legal grounds for the processing of personal data by the Data Controller may vary, all personal data processing activities are carried out in accordance with the general principles set out in Article 4 of the KVKK (see 3.1.).

#### 7.1.1.1. Explicit Consent of Data Subject

One of the conditions for processing personal data is the explicit consent of the data subject. The data subject's explicit consent must be specific to a particular matter, based on the information provided, and freely given.

For personal data processing activities outside the scope of the purpose of processing (primary processing) related to the reasons for obtaining personal data (secondary processing), at least one of the conditions set forth in sections 7.1.1.2-7.1.1.8 of this heading must be met. If none of these conditions are met, the Data Controller carries out these personal data processing activities based on the explicit consent of the Data Subject for such processing activities.

For the processing of personal data based on the explicit consent of the Data Subject, the explicit consent is obtained through the relevant methods.

#### 7.1.1.2. Explicit Prescription by Laws

The personal data of the Data Subject can be processed in accordance with the law if explicitly provided for by law.

#### 7.1.1.3. Failure to Obtain Explicit Consent due to Actual Impossibility

If it is impossible to obtain consent due to actual impossibility, or if consent cannot be deemed valid, the personal data of the Data Subject may still be processed in the event that is necessary to protect the life or physical integrity of the Data Subject or another person.

#### 7.1.1.4. Direct Relation to Establishment or Performance of a Contract

Personal data may be processed if it is necessary for the establishment or performance of a contract, provided that it is directly related to the contract.

#### 7.1.1.5. Fulfillment of a Legal Obligation by the Data Controller

The Data Controller may process the personal data of the Data Subject if processing is necessary for the Data Controller to fulfill its legal obligations

#### 7.1.1.6. Data Subject Making Public Their Personal Data

If the Data Subject has made their personal data public, the personal data may be processed.

#### 7.1.1.7. Necessity of Data Processing for the Establishment, Exercise or Protection of a Right

If data processing is necessary for the establishment, exercise or protection of a right, the personal data of the Data Subject may be processed.

#### 7.1.1.8. Necessity of Data Processing for the Legitimate Interest of the Data Controller

If data processing is necessary for the legitimate interests of the Data Controller, the data may be processed, provided that it does not harm the fundamental rights and freedoms of the Data Subject.

### 7.1.2. Processing of Special Categories of Personal Data

Subject to the implementation of sufficient measures determined by the KVK Board, special categories of personal data are processed by the Data Controller in compliance with the KVKK in the following circumstances:

- Special categories of personal data other than those relating to the health and sexual life of the Data Subject are processed in cases provided for by the laws;
- Special categories of personal data relating to the health and sexual life of the Data Subject may only be processed by persons or authorized institutions and agencies subject to confidentiality obligations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of health services and their financing.

## 8. CONDITIONS FOR THE DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

Once the reasons for processing personal data no longer exist, the Data Controller will delete, destroy or anonymize personal data in accordance with the provisions of Article 138 of the Turkish Penal Code and Article 7 of the KVKK, even if such data has been processed in accordance with the relevant legal provisions, at the discretion of the Data Controller or upon the request of the Data Subject.

In this context, the Data Controller deletes, destroys, or anonymizes the personal data it has collected in the event of:

- amendment or repeal of legislation;
- termination or invalidity of the contract on which the processing is based;
- cessation of the purposes and conditions of processing;
- withdrawal of consent for processing activities based on explicit consent;
- the data subject's request for deletion, destruction or anonymization of their personal data and the acceptance of this request;
- the data subject's request and the decision by the Personal Data Protection Board that the request must be fulfilled upon rejection of this request;

- the expiration of the retention period;
- periodic destruction procedures carried out within the Data Controller.

In accordance with Article 11 of the Regulation, the Data Controller has determined the periodic destruction period as follows. Accordingly:

- at the end of the retention period
- within the 30-day response time after a deletion request
- first periodic destruction after the end of retention period

### 8.1. Techniques for Deletion, Destruction and Anonymization of Personal Data

The Data Controller wiill delete, destroy or anonymize the Personal Data it has collected upon the request of the Data Subject or automatically when the reasons for processing such data no longer exist. In accordance with Article 28 of the Law, anonymized personal data may be processed for purposes such as research, planning and statistics. Such processing carried out after anonymization is outside the scope of the Law, and in such cases, the explicit consent of the Data Subject is not required.

In this context, the Data Controller selects one or more of the following methods of deletion, destruction or anonymization to follow the most appropriate method for the purpose:

#### 8.1.1. Destruction of Physical Documents

Personal Data collected by the Data Controller and processed through non-automated means as part of our data recording systems may also be destroyed by physically eliminating the Personal Data from its medium (paper, microfiche) in a manner that prevents its subsequent use.

#### 8.1.2. Deletion from the Database

Personal Data stored in a database by the Data Controller is deleted from the database in such a way that it cannot be accessed or reused by the Data Users.

Data is deleted by issuing a delete command to electronic recording media such as commercial package programs, human resources programs and SQL databases, by removing the Data Users' right of access to the files located on our central server or the directory where the files are located, by deleting the relevant rows in databases using database commands, or by deleting Personal Data stored on portable media (USB, HDD, etc.) using appropriate software.

However, in cases where the deletion of certain Personal Data renders access to other data in the system impossible, the Personal Data subject to deletion may be archived in a manner that prevents it from being associated with the Data Subject, in which case the Personal Data is considered to have been deleted. In such cases, the Data Controller takes all necessary technical and administrative measures to ensure that Personal Data is only accessible to authorized persons.

### 8.1.3. Deletion from the Software Programs Used

Personal Data stored in digital media by the Data Controller is deleted from the software in such a way that it cannot be accessed or reused by the Data Users.

Data is deleted by issuing a delete command to electronic recording media such as commercial package programs, human resources programs and SQL databases, by removing the Data Users' right of access to the files located on our central server or the directory where the files are located, by deleting the relevant rows in databases using database commands, or by deleting Personal Data stored on portable media (USB, HDD, etc.) using appropriate software.

However, in cases where the deletion of certain Personal Data renders access to other data in the system impossible, the Personal Data subject to deletion may be archived in a manner that prevents it from being associated with the Data Subject, in which case the Personal Data is considered to have been deleted. In such cases, the Data Controller takes all necessary technical and administrative measures to ensure that Personal Data is only accessible to authorized persons.

## 9. RIGHTS OF DATA SUBJECTS AND METHODS OF EXERCISING AND EVALUATING SUCH RIGHTS

### 9.1. Rights of Data Subjects and Exercise of Such Rights

### 9.1.1. Rights of Data Subjects

Data subjects have the right to:

- learn whether their personal data is being processed;
- seek information on how their personal data has been processed;
- learn the purpose of processing personal data and whether it is used in accordance with that purpose;
- know the third parties to whom their personal data is transferred domestically or abroad;
- request correction of their personal data in case of incomplete or incorrect processing, and demand that the action taken in this regard be communicated to the third persons to which their personal data was transferred;
- request deletion or destruction of their personal data although it was processed in accordance with the provisions of the KVKK and other laws in case of disappearance of the reasons for processings, and demand that the action taken in this regard be communicated to the third persons to which their personal data was transferred;
- challenge any result to their detriment upon analysis of their processed personal data exclusively through automated systems;
- claim compensation for their damages arising from unlawful processing of their personal data.

### 9.1.2. Cases where Data Subjects Cannot Exercise Their Rights

Pursuant to Article 28 of the KVKK, the following cases are excluded from the scope of the KVKK, and therefore, data subjects cannot exercise their rights listed in 10.1.1 in these cases:

- Processing of personal data for purposes such as research, planning and statistics by rendering them anonymous through compilation of official statistics;
- Processing of personal data for artistic, historical, literary or scientific purposes, or within the scope of freedom of expression, provided that such processing does not violate national defense, national security, public safety, public order, economic security, privacy of individuals or human rights, or constitute a crime.
- Processing of personal data as part of preventive, protective and intelligence activities carried out by public institutions and agencies authorized by law to ensure national defense, national security, public safety, public order or economic security.
- Processing of personal data by judicial authorities or enforcement authorities in connection with investigation, prosecution, trial or enforcement proceedings.

Pursuant to Article 28/2 of the KVKK, data subjects may not exercise their other rights listed in 10.1.1 in the following cases, except for the right to request compensation for damages:

- If the processing of personal data is necessary for the prevention of crime or for criminal investigation;
- The personal data that has been made public by the data subject themselves will be processed;
- Processing of personal data is necessary for the performance of supervisory or regulatory tasks by public institutions and agencies authorized by law, as well as professional organizations with public institution status, or for disciplinary investigations or prosecutions.
- Processing of personal data is necessary for the protection of the economic and financial interests of the State in relation to budget, tax, and financial matters.

**9.1.3. Data Subjects Exercising Their Rights**

Data subjects may submit their requests regarding their rights listed under Section 9.1.1 to the Data Controller free of charge by filling out and signing the Application Form with the information and documents that will identify them and using the methods specified below or other methods determined by the Personal Data Protection Board:

- They can submit this form or their own petition, signed in ink, to the address “Hüseyin Rahmi Sk. No: 7/7 06680 Çankaya, ANKARA” in person or through their representatives. Identity authentication is mandatory in the application process. In applications made through a representative, an original copy of the power of attorney authorizing the request for personal data must be submitted.
- They can send the application form or their own petition, signed in ink, to the address specified in the first paragraph by writing “Request for Information under the KVKK” on the envelope. The applicant's representative may also submit an application by mail, accompanied by a certified copy of the power of attorney authorizing the request for personal data.
- They can apply through a notary public. The above address will also be used for applications made through a notary public. The subject line of the notification must read “Request for Information under the KVKK.”
- Applications via email can be submitted to ..... If this method is used, the subject line of the email must include the phrase “Request for Information under the KVKK.”

In order for third parties to submit applications on behalf of data subjects, a special power of attorney drawn up by a notary public on behalf of the person who will submit the application must be available.

### 9.1.4. Data Subject's Right to File a Complaint with the KVK Board

Pursuant to Article 14 of the KVKK, the Data Subject may file a complaint with the KVK Board within thirty days from the date of receiving the Data Controller's response, and in any case within sixty days from the date of the application, in cases where the application is rejected, the response is found to be insufficient, or no response is provided within the specified timeframe.

## 9.2. Data Controller's Response to Applications

### 9.2.1. Data Controller's Procedure and Time Limit for Responding to Applications

If the Data Subject submits their request to the Data Controller in accordance with the procedure set out in section 9.1.3, the Data Controller will process the request free of charge within thirty days at the latest, depending on the nature of the request. However, if the Personal Data Protection Board has set a fee, the Data Controller will collect the fee specified by the Personal Data Protection Board from the applicant.

### 9.2.2. Information the Data Controller May Request from the Data Subject Making the Application

The Data Controller may request information from the applicant to determine whether they are a Data Subject. The Data Controller may ask the Data Subject questions regarding their application to clarify the matters contained therein.

### 9.2.3. The Data Controller's Right to Reject the Data Subject's Request

The Data Controller may reject the applicant's application in the following cases, explaining the reasons for the rejection:

- Processing of personal data for purposes such as research, planning and statistics by rendering them anonymous through compilation of official statistics;
- Processing of personal data for artistic, historical, literary or scientific purposes, or within the scope of freedom of expression, provided that such processing does not violate national defense, national security, public safety, public order, economic security, privacy of individuals or human rights, or constitute a crime.
- Processing of personal data as part of preventive, protective and intelligence activities carried out by public institutions and agencies authorized by law to ensure national defense, national security, public safety, public order or economic security.
- Processing of personal data by judicial authorities or enforcement authorities in connection with investigation, prosecution, trial or enforcement proceedings.
- If the processing of personal data is necessary for the prevention of crime or for criminal investigation;
- The personal data that has been made public by the data subject themselves will be processed;

- Processing of personal data is necessary for the performance of supervisory or regulatory tasks by public institutions and agencies authorized by law, as well as professional organizations with public institution status, or for disciplinary investigations or prosecutions.
- Processing of personal data is necessary for the protection of the economic and financial interests of the State in relation to budget, tax, and financial matters.
- The request of the Data Subject may interfere with the rights and freedoms of other individuals.
- The request requires disproportionate effort.
- The requested information is publicly available.

## 10. RELATIONSHIP BETWEEN THE DATA CONTROLLER'S PERSONAL DATA PROTECTION AND PROCESSING POLICY AND OTHER POLICIES

The Data Controller may formulate sub-policies for internal use related to the principles set forth in this Policy regarding the protection and processing of personal data, as well as additional policies targeting specific groups of individuals, primarily employees.

The principles of the Data Controller's internal policies are reflected in public policies to the extent that they are relevant, with the aim of informing interested parties within this framework and ensuring transparency and accountability regarding the personal data processing activities carried out by the Data Controller.