**ORİMPEX TEXTILE**

**PERSONAL DATA PROTECTION AND PROCESSING, PERSONAL DATA STORAGE AND DESTRUCTION POLICY**

Effective Date: 15.03.2022

Version: 1.1.

Approved by the Board of Directors.

**CONTENTS**

9.2.2. Information That the Data Controller May Request from the Applicant Personal Data Owner

9.2.3. Data Controller's Right to Reject the Application of the Personal Data Owner

**10. RELATIONSHIP OF THE DATA CONTROLLER PERSONAL DATA PROTECTION AND PROCESSING POLICY WITH OTHER POLICIES**

**ABBREVIATIONS AND CONCEPTS**

| | |
|---|---|
| KVKK Law | Personal Data Protection Law No. 6698 published in the Official Gazette No. 29677 dated April 7, 2016 |
| GDPR | EU (European Union) General Data Protection Regulation |
| Constitution | The Constitution of the Republic of Türkiye, dated 7 November 1982 and numbered 2709, published in the Official Gazette, dated 9 November 1982 and numbered 17863. |
| Data Processor | A person who processes personal data outside the data controller organization and 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 data. |
| Data Owner/Relevant Person | The real person whose personal data is processed, such as the employees, customers, business partners, shareholders, authorities, potential customers, candidate employees, interns, visitors, suppliers, employees of institutions it cooperates with, third parties and other persons, including but not limited to those listed here, with whom the COMPANY and/or its subsidiaries/affiliates have commercial relations. |
| Data Controller | The natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system. |
| Explicit Consent | Consent based on informed consent and expressed freely on a specific subject. |
| Destruction | Deletion, destruction or anonymization of personal data. |
| Recording Environment | Any environment in which personal data is processed by fully or partially automatic means or non-automatic means provided that it is part of any data recording system. |
| Personal Data | Any information relating to an identified or identifiable natural person. |

| | |
|---|---|
| Special Personal Data | Data regarding individuals' race, ethnic origin, political views, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership in associations, foundations or unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data. |
| Processing of Personal Data | Any operation performed on personal data, such as obtaining, recording, storing, preserving, changing, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data, either fully or partially by automatic means or non-automatic means provided that it is part of any data recording system. |
| Anonymization of Personal Data | Making personal data in such a way that it cannot be associated with an identified or identifiable natural person in any way, even by matching it with other data. |
| Deletion of Personal Data | Deletion of personal data; making personal data inaccessible and reusable for the relevant users in any way. |
| Destruction of Personal Data | The process of making personal data inaccessible, irreversible and reusable by anyone. |
| Periodic Destruction | The process of deletion, destruction or anonymization to be carried out ex officio at repeated intervals in case all the processing conditions of personal data specified in the law are eliminated. |
| Regulations | Regulation on the Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette No. 30224 dated 28 October 2017 and entered into force as of 1 January 2018. |
| KVK Board / Board | Personal Data Protection Board |
| Personal Data Protection Authority | Personal Data Protection Authority |
| Policy | Data Controller Personal Data Protection and Processing Policy |
| Turkish Penal Code | Published in the Official Gazette dated 12 October 2004 and numbered 25611; Turkish Penal Code dated 26 September 2004 and numbered 5237. |

## 1. INTRODUCTION

### 1.1. Purpose

As the Data Controller, we are aware of our responsibility regarding the protection and legal safeguarding of personal data, which is regulated as a constitutional right, and we attach importance to the safe use of your personal data.

The purpose of this policy is to regulate the methods and principles to be followed to ensure that the COMPANY's personal data is processed and protected in accordance with the Personal Data Protection Law (KVKK), published in the Official Gazette dated April 7, 2016 and numbered 29677.

In this way, it is aimed to ensure full compliance with the legislation in the processing and protection activities of personal data carried out by the Data Controller and to protect all rights of personal data owners arising from the legislation on personal data.

### 1.2 Scope

This policy is applied to all activities carried out by the COMPANY regarding the processing and protection of personal data.

This policy; It covers the real persons whose personal data are processed by the Data Controller, primarily Employee, Shareholder/Partner, Supplier Official, Product or Service Recipient, Parent/Guardian/Representative, Visitor, Supplier Employee, Potential Product or Service Recipient, Person subject to the news, Employee Candidate, Supplier, Public Official, Corporate Customer Representative/Official, Manager (Not Shareholder/Partner), Company Official, Cargo Officer, Customer - Official - Employee, Approver, Customs Consultant, Customer - Official - Employee, Organizer, Authorized, Exporter, Manufacturer, Distributor, Bank Official, Data Controller Official, Potential Product or Service Recipient (Natural Person), Food Engineer, Doctor, Employee Candidate Reference, Employee Relative, Legal Counsel, Employer Representative, Occupational Health and Safety Specialist, Workplace Physician, Website Visitor, Preparer, Sought Persons, Auditor, through automatic or non-automatic means provided that they are part of any data recording system. This Policy shall not apply in any way to legal entities or legal entity data.

This policy is implemented by the COMPANY together with the relevant detailed data procedures in the activities carried out for the processing and protection of all personal data.

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

The relevant legal regulations in force regarding the processing and protection of personal data will primarily be applied. In the event of any inconsistency between the current legislation and the Policy, the Data Controller accepts that the current legislation will be applied.

### 1.4. Enforcement of the Policy

This Policy, issued by the Data Controller, is dated 15.03.2022. In case the entirety or certain articles of the Policy are renewed, the effective date of the Policy will be updated.

The Policy is published on the Data Controller's website www.orimpex.com.tr and made accessible to the relevant persons upon request of personal data owners.

## 2. ISSUES RELATING TO THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the Personal Data Protection Law, the Data Controller takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of personal data it processes, to prevent unlawful access to data and to ensure the preservation of data, and to carry out or have carried out the necessary audits within this scope.

### 2.1. Ensuring the Security of Personal Data

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

The Data Controller takes technical and administrative measures, in accordance with technological possibilities and implementation costs, to ensure that personal data is processed lawfully, to prevent unlawful access to these data and to store them in secure environments.

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

The main technical measures taken by the Data Controller to ensure that personal data is processed lawfully, to prevent unlawful access to these data and to store them in secure environments are listed below:

- Network security and application security are provided
- Key management is implemented
- Security measures are taken within the scope of information technology systems supply, development and maintenance.
- 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 system is implemented and these are also monitored.
- Log records are kept without user intervention.
- Secure encryption / cryptographic keys are used for sensitive personal data and are managed by different units.

- Intrusion detection and prevention systems are used
- Cyber security measures have been taken and their implementation is constantly monitored.
- Encryption is being done
- Data loss prevention software is used

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

The main administrative measures taken by the Data Controller to ensure that personal data is processed lawfully, to prevent unlawful access to these data and to store them in secure environments are listed below.

- There are disciplinary regulations for employees that include data security provisions.
- Training and awareness activities are carried out for employees on data security at regular intervals.
- An authority matrix has been created for employees.
- Confidentiality commitments are made
- The authority of employees who change their duties or leave their jobs is removed in this area.
- Signed contracts include data security provisions
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported quickly
- Personal data security is monitored.
- Necessary security measures are taken regarding entry and exit 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 reduced as much as possible
- Current risks and threats have been identified
- Protocols and procedures for the security of special personal data have been determined and implemented.

### 2.1.2. Audit of Measures Taken for the Protection of Personal Data

The Data Controller conducts or has conducted the necessary audits within its own organization in accordance with Article 12 of the Personal Data Protection Law. The results of these audits are reported to the relevant department within the scope of the internal operations of the Data Controller and the necessary activities are carried out to improve the measures taken.

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

The Data Controller operates a system that ensures that, in the event that personal data processed in accordance with Article 12 of the PDP Law is obtained by others through illegal means, this situation is reported to the relevant personal data owner and the PDP Board as soon as possible.

### 2.2. Observing the Rights of the Data Owner; Creating Channels to Communicate These Rights to the Data Controller and Evaluating the Requests of the Data Owners

As the Data Controller, it carries out the necessary channels, internal operations, administrative and technical arrangements in accordance with Article 13 of the Personal Data Protection Law in order to evaluate the rights of personal data owners and to provide the necessary information to personal data owners.

If personal data owners submit their requests regarding their rights listed below to the Data Controller in writing, the Data Controller will finalize the request free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires an additional cost, the Data Controller will charge the fee in the tariff determined by the Personal Data Protection Board. Personal data owners;

- Learning whether personal data is being processed,
- To request information regarding the processing of personal data,
- To learn the purpose of processing personal data and whether they are used in accordance with their purpose,
- To know the third parties to whom personal data is transferred, either domestically or abroad,
- To request correction of personal data if it is processed incompletely or incorrectly and to request notification of the action taken to third parties to whom personal data is transferred,
- Requesting the deletion or destruction of personal data in case the reasons requiring processing are eliminated, even though it has been processed in accordance with the provisions of the Personal Data Protection Law and other relevant laws, and requesting that the action taken within this scope be notified to third parties to whom personal data has been transferred,
- To object to a result that is to the detriment of the person himself/herself, as a result of the analysis of the processed data exclusively through automatic systems,
- In case of damage caused by unlawful processing of personal data, the person has the right to demand compensation for the damage.

More detailed information on the rights of data owners is included in Section 10 of this Policy.

**2.3. Protection of Special Personal Data**

With the Personal Data Protection Law, special importance is given to certain personal data due to the risk of causing victimization or discrimination in the event of unlawful processing of such data.

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

The Data Controller acts with sensitivity in protecting special personal data determined as "special nature" by the Personal Data Protection Law and processed in accordance with the law. In this context, the technical and administrative measures taken by the Data Controller to protect personal data are meticulously implemented in terms of special personal data and the necessary controls are provided within the COMPANY.

In the processing of Special Personal Data, as set out in Article 6 of the Law, the Data Controller, in accordance with the Board's decision dated 31.01.2018 and numbered 2018/10, takes the following measures as the data controller:

- This systematic, manageable and sustainable Policy has been established for the security of special personal data, with clear rules.
- For employees involved in the processing of special personal data,
    - Regular training is provided on the law and related regulations and on the security of Special Personal Data.
    - Confidentiality agreements are made,
    - The scope and duration of authorization of users with access to data are clearly defined,
    - Authorization checks are carried out periodically,
    - The authorizations of Employees who change their duties or leave their jobs are immediately revoked in this area. In this context, they receive the inventory allocated to them by the Data Controller.
- The environments where Special Personal Data is processed, stored and/or accessed are electronic environments,
    - Personal Data is stored using cryptographic methods,
    - Cryptographic keys are kept in secure and separate environments,
    - Transaction records of all transactions performed on Personal Data are securely logged,
    - Security updates for the environments where Personal Data is located are constantly monitored, necessary security tests are regularly performed, and test results are recorded.

- If Personal Data is accessed through software, user authorizations for this software are made, security tests of this software are regularly performed/commissioned, and test results are recorded.
- If remote access to Personal Data is required, at least a two-stage authentication system is provided.

- The physical environment where Special Personal Data is processed, stored and/or accessed is;
  - Adequate security measures are taken (against electrical leakage, fire, flood, theft, etc.) depending on the nature of the environment where the Special Personal Data is located.
  - By ensuring the physical security of these environments, unauthorized entry and exit are prevented.

- If Special Personal Data is to be transferred
  - If Personal Data needs to be transferred via e-mail, it is transferred in encrypted form using a corporate e-mail address or a Registered Electronic Mail (KEP) account.
  - If it needs to be transferred via media such as Portable Memory, CD, DVD, it is encrypted with cryptographic methods and the cryptographic key is kept in a different medium,
  - If transfer is made between servers in different physical environments, data transfer is carried out by establishing a VPN between the servers or by using the SFTP method.
  - If it is necessary to transfer Personal Data via paper, necessary precautions are taken against risks such as theft, loss or viewing of documents by unauthorized persons, and the documents are sent in “Confidential” format.
  - In addition to the measures mentioned above, technical and administrative measures to ensure the appropriate level of security specified in the Personal Data Security Guide published on the Personal Data Protection Authority's website should also be taken into account.

**2.4. Increasing Awareness and Supervision 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 increase awareness on preventing the unlawful processing of personal data, unlawful access to data, and ensuring the preservation of data.

Necessary systems are established to raise awareness of the current employees of the Data Controller's business units and newly recruited employees on the protection of personal data, and professional people are employed when necessary.

The results of the training conducted to increase awareness of the business units of the Data Controller on the protection and processing of personal data are reported to the Data Controller. In this regard, the Data Controller evaluates the participation in the relevant trainings, seminars and information sessions and carries out or has the necessary audits carried out. As the Data Controller, we update and renew our trainings in parallel with the updating of the relevant legislation.

## 3. ISSUES RELATING TO THE PROCESSING OF PERSONAL DATA

In accordance with Article 20 of the Constitution and Article 4 of the Personal Data Protection Law, the Data Controller carries out personal data processing activities in accordance with the law and rules of honesty; accurately and, if necessary, up-to-date; for specific, clear and legitimate purposes; in a purpose-related, limited and proportionate manner. The Data Controller retains personal data for the period stipulated by law or required by the purpose of processing personal data.

In accordance with Article 20 of the Constitution and Article 5 of the Personal Data Protection Law, the Data Controller processes personal data based on one or more of the conditions in Article 5 of the Personal Data Protection Law regarding the processing of personal data.

In accordance with Article 20 of the Constitution and Article 10 of the Personal Data Protection Law, the Data Controller informs personal data owners and provides the necessary information in case personal data owners request information.

The Data Controller acts in accordance with the regulations regarding the processing of special personal data in accordance with Article 6 of the Personal Data Protection Law.

In accordance with Articles 8 and 9 of the Personal Data Protection Law, the Data Controller acts in accordance with the regulations stipulated in the law and set forth by the Personal Data Protection Board regarding the transfer of personal data.

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

#### 3.1.1. Processing in Accordance with Law and Fairness

The Data Controller acts in accordance with the principles set forth by legal regulations and the general rule 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 its intended purpose.

#### 3.1.2. Ensuring Personal Data is Accurate and Up-to-Date Where Necessary

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

#### 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 in connection with the service it provides and to the extent necessary for these. The purpose for which personal data will be processed by the Data Controller is determined before the personal data processing activity begins.

#### 3.1.4. Being Relevant, Limited and Proportionate to the Purpose of Processing

The Data Controller processes personal data in a manner suitable for the achievement of the specified purposes and avoids the processing of personal data that is not relevant or needed to achieve the purpose.

### 3.1.5. Storage for the Period Stipulated in the Relevant Legislation or Necessary for the Purpose for which they are Processed

The Data Controller stores personal data only for the period specified in the relevant legislation or required for the purpose for which they are processed. In this context, the Data Controller first determines whether a period is specified in the relevant legislation for the storage of personal data, if a period is specified, it complies with this period, and if no period is specified, it stores personal data for the period required for the purpose for which they are processed. In the event that the period expires or the reasons requiring processing cease to exist, personal data are deleted, destroyed or anonymized by the Data Controller. Personal data are not stored by the Data Controller for the possibility of future use. Detailed information on this subject is provided in Section 9 of this Policy.

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

Protection of personal data is a constitutional right. Fundamental rights and freedoms can only be restricted by law, without affecting their essence, based on the reasons specified in the relevant articles of the Constitution. According to the third paragraph of Article 20 of the Constitution, personal data can only be processed in cases stipulated by law or with the express consent of the person. In this context and in accordance with the Constitution, the Data Controller processes personal data only in cases stipulated by law or with the express consent of the person. Detailed information on this subject is provided in Section 7 of this Policy.

### 3.3. Enlightening and Informing the Personal Data Owner

The Data Controller, in accordance with Article 10 of the Personal Data Protection Law, informs personal data owners during the collection of personal data. In this context, the Data Controller and, if any, their representative are informed about the identity, the purpose for which personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method and legal reason for collecting personal data, and the rights of the personal data owner. Detailed information on this subject is provided in Section 10 of this Policy.

Article 20 of the Constitution stipulates that everyone has the right to be informed about personal data relating to them. Accordingly, Article 11 of the Personal Data Protection Law lists “requesting information” among the rights of personal data owners. In this context, the Data Controller provides the necessary information in case the personal data owner requests information in accordance with Articles 20 of the Constitution and 11 of the Personal Data Protection Law. Detailed information on this subject is provided in Section 10 of this Policy.

### 3.4. Processing of Special Personal Data

The Data Controller strictly complies with the regulations set forth in the PDP Law when processing personal data determined as “special” by the PDP Law.

In Article 6 of the Personal Data Protection Law, certain personal data that poses a risk of causing victimization or discrimination when processed unlawfully are designated as “special data”. These data include data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership in associations, foundations or unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

In accordance with the PDP Law, the Data Controller processes special personal data in the following cases, provided that adequate measures are taken, as determined by the PDP Board:

- If the personal data owner has given explicit consent, or

- If there is no explicit consent of the personal data owner;
    - Special personal data, other than the health and sexual life of the personal data owner, in cases prescribed by law,
    - Personal data of a personal data owner, which is of a special nature, regarding his/her health and sexual life, can only be processed by persons or authorized institutions and organizations that are under a confidentiality obligation for the purposes of protecting public health, providing preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and their financing.

**3.5. Transfer of Personal Data**

The Data Controller may transfer the personal data and special personal data of the personal data owner to third parties by taking the necessary security measures (See 2.1.) in line with the legal personal data processing purposes. In this regard, the Data Controller acts in accordance with the regulations stipulated in Article 8 of the Personal Data Protection Law. 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 in line with legitimate and lawful personal data processing purposes, based on and limited to one or more of the personal data processing conditions specified in Article 5 of the Law listed below:

- If the personal data owner has explicit consent;
- If there is a clear regulation in the laws regarding the transfer of personal data,
- If it is necessary to protect the life or physical integrity of the personal data owner or someone else and the personal data owner is unable to give his/her consent due to a de facto impossibility or if his/her consent is not legally valid;
- If it is necessary to transfer personal data of the parties to a contract, provided that it is directly related to the establishment or execution of a contract,
- If personal data transfer is mandatory for the Data Controller to fulfill its legal obligations,
- If personal data has been made public by the personal data owner,
- If personal data transfer is mandatory for the establishment, exercise or protection of a right,
- If the transfer of personal data is mandatory for the legitimate interests of the Data Controller, provided that it does not harm the fundamental rights and freedoms of the personal data owner.

**3.5.2. Transfer of Special Personal Data**

The Data Controller may transfer the personal data owner's special data to third parties in the following cases, in line with legitimate and lawful personal data processing purposes, by showing due care, taking the necessary security measures (See 2.1) and taking the sufficient measures prescribed by the Personal Data Protection Board.

- If the personal data owner has given explicit consent, or
- If there is no explicit consent of the personal data owner;
    - Personal data of a special nature other than the health and sexual life of the personal data owner (data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, appearance and dress, association, foundation or union membership, criminal conviction and security measures, and biometric and genetic data), in cases prescribed by law,
    - Sensitive personal data regarding the health and sexual life of the personal data owner may only be disclosed by persons or authorized institutions and organizations that are under a confidentiality obligation for the purposes of protecting public health, providing preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and their financing.

**3.6. Transfer of Personal Data Abroad**

The Data Controller may transfer the personal data and special personal data of the personal data owner to third parties by taking the necessary security measures (See 2.1) in line with the lawful personal data processing purposes.

It is shared with companies that provide IT services through instant messaging or online communication channels that are widely used today, and with your express consent, outside of countries that are declared safe, as these are platforms and applications of foreign origin for the purpose of providing services.

Personal data is transferred by the Data Controller to foreign countries declared by the PDP Board to have sufficient protection or, in the absence of sufficient protection, to foreign countries where the data controllers in Türkiye and the relevant foreign country have undertaken in writing to provide sufficient protection and where the PDP Board has granted its permission ("Foreign Country Where the Data Controller Who Undertakes to Provide Sufficient Protection Is Located"). In this regard, the Data Controller acts in accordance with the regulations set forth in Article 9 of the PDP Law.

**3.6.1. Transfer of Personal Data Abroad**

The Data Controller may transfer personal data to Foreign Countries Where the Data Controller Has Sufficient Protection or Promises Sufficient Protection, in line with legitimate and lawful personal data processing purposes, if the personal data owner has explicit consent or if the personal data owner does not have explicit consent, in the event of one of the following situations:

- If there is a clear regulation in the laws regarding the transfer of personal data,
- If it is necessary to protect the life or physical integrity of the personal data owner or someone else and the personal data owner is unable to give his/her consent due to a de facto impossibility or if his/her consent is not legally valid;
- If it is necessary to transfer personal data of the parties to a contract, provided that it is directly related to the establishment or execution of a contract,

- If personal data transfer is mandatory for the Data Controller to fulfill its legal obligations,

**3.6.2. Transfer of Special Personal Data Abroad**

The Data Controller may transfer the personal data owner's special data to Foreign Countries Where the Data Controller Has Sufficient Protection or Promises Sufficient Protection, in line with legitimate and lawful personal data processing purposes, by showing due care, taking the necessary security measures (See 2.1) and taking the sufficient measures prescribed by the Personal Data Protection Board, in the following cases.

- If the personal data owner has given explicit consent, or
- If there is no explicit consent of the personal data owner;
    - Personal data of a special nature other than the health and sexual life of the personal data owner (data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, appearance and dress, association, foundation or union membership, criminal conviction and security measures, and biometric and genetic data), in cases prescribed by law,
    - The personal data of a personal data owner, which is of a special nature, regarding his/her health and sexual life, can only be transferred within the scope of processing by persons or authorized institutions and organizations under a confidentiality obligation for the purposes of protecting public health, carrying out preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and their financing.

**4. CATEGORIZATION OF PERSONAL DATA PROCESSED BY OUR COMPANY, PROCESSING PURPOSES AND STORAGE PERIOD**

In accordance with Article 10 of the Personal Data Protection Law, the Data Controller informs the personal data owner of which personal data owner groups' personal data it processes, the purposes of processing the personal data of the personal data owner, and the storage periods.

**4.1. Categorization of Personal Data**

In accordance with Article 10 of the PDP Law, the Data Controller processes personal data in the following categories, limited to the subjects covered by this Policy, based on one or more of the personal data processing conditions specified in Article 5 of the PDP Law and in line with the legitimate and lawful personal data processing purposes, and in compliance with the general principles specified in the PDP Law, especially the principles specified in Article 4 of the PDP Law regarding the processing of personal data, and all obligations regulated in the PDP Law. The data subjects to whom the personal data processed in these categories are related are also specified in Section 5 of this Policy.

| **Personal Data Categorization** | **Explanation** |
|---|---|

| | |
|---|---|
| Legal Process and Compliance Information | Data processed within the scope of the Company's legal processes, determination and follow-up of receivables and rights, and fulfillment of debts and legal obligations, information in correspondence with judicial authorities, incoming and outgoing documents, and case files. |
| Identity 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; containing information about the person's identity; documents such as driver's license, identity card and passport containing information such as name-surname, Turkish identity number, nationality information, mother's name-father's name, place of birth, date of birth, gender, and tax number, SSI number, signature information, vehicle license plate, etc. |
| Personal Information | Any personal 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; processed to obtain information that will form the basis for the establishment of personal rights of natural persons who have a working relationship with our Company. |
| Criminal Conviction and Security Measures 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; obtained within the scope of operations carried out by the Company's business units or in order to carry out business processes of natural persons who have a working relationship with the Company or to protect the legal and other interests of the Company and the Personal Data Owner, such as the Personal Data Owner's criminal record. |
| Contact Information | Information 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 telephone number, address, e-mail address, fax number, IP address. |
| Risk Management 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; processed to manage all kinds of commercial, technical and administrative risks created according to the type of legal relationship established between the Company and the Personal Data Owner. |
| Transaction Security Information | While the Company is carrying out its activities, personal data such as IP Address information, Website login and logout information, password and passcode information processed for the technical, administrative, legal and commercial security of both the Personal Data Owner and the Company. |
| Financial Information | Personal data processed regarding information, documents and records showing all kinds of financial results created according to the type of legal relationship our Company has established with the personal data owner, which are clearly related to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of |

| | |
|---|---|
| | the data recording system, and data such as bank account number, IBAN number, credit card information, financial profile, asset data, income information. |
| Customer Transaction Information | Information that clearly belongs to an identified or identifiable natural person, processed partially or fully automatically or non-automatically as part of the data recording system; Information obtained and produced about the relevant person as a result of the Company's commercial activities and operations carried out by its business units, such as call center records, invoices, promissory note check information, order information, request information, offers, service numbers. |
| Professional Experience Information | Data that clearly belongs to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of the data recording system, depending on the type of legal relationship established between the Company and the Personal Data Owner; such as diploma information, courses attended, in-service training information, certificates, candidate application forms, reference interview information, job interview information, transcript information. |
| Audio/Visual Information | Data contained in documents that are clearly of a natural person with a known or identifiable identity, such as photographs and camera recordings (excluding records falling within the scope of Physical Location Security Information), voice recordings, and copies of documents containing personal data. |
| Physical Space Security Information | Personal data relating to records and documents taken at the entrance to the physical location, during the stay in the physical location, which are clearly related to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of a data recording system; camera recordings, recordings taken at the security point, etc. |
| Health Information | Health data such as Health Report, Disability tax exemption certificates, insurance documents, military status certificate of the Personal Data Owner and/or their family members, which are clearly related to an identified or identifiable natural person; processed partially or fully automatically or non-automatically as part of the data recording system; within the scope of operations carried out by the Company's business units; in relation to the products and services offered or in order to carry out the business processes of natural persons who have a business relationship with the Company or to protect the legal and other interests of the Company and the Personal Data Owner. |
| Marketing Knowledge | 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; Data obtained and produced about the relevant person as a result of the Company's commercial activities and operations carried out by its business units, such as shopping history information, surveys, cookie records, and campaign work. |

| | |
|---|---|
| Location Data | Information 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; information that determines the location of the personal data owner within the scope of operations carried out by business units, during the use of products and services or while employees are using their vehicles; GPS location, travel data, etc. |
| Other – Vehicle Information | Vehicle Plate, Claimed Vehicle Information |
| Other – Employee Family Member and Relative Information | Employee 1st Degree Relative Information, Employee Family Members Identity and Address Information |

**4.2. Purposes of Processing Personal Data**

The Data Controller processes personal data limited to the purposes and conditions set out in the personal data processing conditions specified in the second paragraph of Article 5 and the third paragraph of Article 6 of the Personal Data Protection Law. These purposes and conditions are;

- The Data Controller's relevant activity regarding the processing of your personal data is clearly prescribed by law.
- The processing of your personal data by the Data Controller is directly related to and necessary for the establishment or performance of a contract.
- The processing of your personal data is mandatory for the Data Controller to fulfill its legal obligations.
- Provided that your personal data is made public by you; it is processed by the Data Controller for the limited purpose of making it public.
- The processing of your personal data by the Data Controller is necessary for the establishment, exercise or protection of the rights of the Data Controller or you or third parties.
- It is necessary to process personal data for the legitimate interests of the Data Controller, provided that it does not harm your fundamental rights and freedoms.
- If the processing of personal data by the Data Controller is necessary to protect the life or physical integrity of the personal data owner or someone else, and in this case the personal data owner is unable to express his/her consent due to actual or legal invalidity.
- It is foreseen in the laws for special personal data other than the health and sexual life of the personal data owner.
- In terms of personal data of a personal data owner's special nature regarding his/her health and sexual life, it is the processing of such data by persons or authorized institutions and organizations that are under a confidentiality obligation for the purposes of protecting public health, carrying out preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and their financing.

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

| **PROCESSING PURPOSES** |
| --- |
| Monitoring and Execution of Legal Affairs |
| Carrying out activities to ensure business continuity |
| Providing Information to Authorized Persons, Institutions and Organizations |
| Execution of Risk Management Processes |
| Execution of Finance and Accounting Affairs |
| Execution of Information Security Processes |
| Conducting Internal Audit/Investigation/Intelligence Activities |
| Carrying out management activities |
| Carrying out activities in accordance with legislation |
| Conducting Audit / Ethics Activities |
| Carrying out the purchasing processes of goods / services |
| Execution of Goods / Services Sales Processes |
| Execution of Customer Relationship Management Processes |
| Ensuring Physical Space Security |
| Conducting/Supervising Business Activities |
| Fulfillment of Employment Contract and Legislative Obligations for Employees |

| |
|---|
| Conducting Employee Benefits and Side Benefits Processes |
| Other – Carrying out environmental management activities |
| Conducting Occupational Health / Safety Activities |
| Ensuring the Security of Movable Goods and Resources |
| Planning Human Resources Processes |
| Execution of Contract Processes |
| Execution of Emergency Management Processes |
| Carrying out logistics activities |
| Obtaining and Evaluating Suggestions for Improving Business Processes |
| Conducting Communication Activities |
| Conducting Assignment Processes |
| Execution of Goods / Services Production and Operation Processes |
| Carrying out After-Sales Support Services for Goods/Services |
| Carrying out marketing processes for products/services |
| Carrying out storage and archive activities |
| Carrying out activities aimed at customer satisfaction |
| Tracking of Requests / Complaints |

| |
|---|
| Organization and Event Management |
| Carrying out advertising / campaign / promotion processes |
| Carrying out social responsibility and civil society activities |
| Conducting Marketing Analysis Studies |
| Execution of Supply Chain Management Processes |
| Implementation of the Wage Policy |
| Implementation of Employee Satisfaction and Loyalty Processes |
| Conducting the Selection and Placement Processes of Employee Candidates / Interns / Students |
| Conducting the Application Process of Employee Candidates |
| Other – Execution of Termination Procedures |
| Conducting Training Activities |
| Conducting Performance Evaluation Processes |
| Conducting Talent / Career Development Activities |
| Execution of Access Permissions |
| Creating and Tracking Visitor Records |
| Execution of Loyalty Processes to Company / Products / Services |
| Ensuring the Security of Data Controller Operations |

| |
|---|
| Conducting Strategic Planning Activities |

If the processing activity carried out for the aforementioned purposes does not meet any of the conditions stipulated under the PDP Law, your explicit consent is obtained by the Data Controller for the relevant processing process.

**4.3. Storage of Personal Data**

**4.3.1. Storage Periods of Personal Data**

The Data Controller stores personal data for the period specified in the relevant laws and legislation, if required by these regulations. The storage, destruction and periodic destruction periods determined by the Data Controller are as follows:

| **Activity** | **Storage Period** | **Destruction Time** |
|---|---|---|
| Litigation and Enforcement Proceedings Process | Other – 15 Years from the Termination of the Business Relationship<br>Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>within 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data.<br>Within 30 days of the request for deletion. |
| Following up on legal processes and representing the company | Other – 15 Years from the Termination of the Business Relationship<br>Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>within 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data.<br>Within 30 days of the request for deletion. |
| Official Institution and Organization Procedures | Other – 15 Years from the Termination of the Business Relationship<br>Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |

| | | |
|---|---|---|
| Legal Risk Analysis | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Conducting Legal Procedures | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 15 Years from the Termination of the Business Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Representation of the Company Before Third Parties | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 15 Years from the Termination of the Business Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Audit Activities | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Processing Purpose<br>Other – 10 Years from the End of the Activity<br>Other – 10 Years from the End of the Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Conducting Financial Activities | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Activity<br>Other – 15 Years from the End of the Employment Contract | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>within 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data.<br>Within 30 days of the request for deletion. |

| | | |
|---|---|---|
| | Other – 10 Years from the End of the Purpose of Processing | |
| Carrying out administrative affairs and activities | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 10 Years from the Termination of the Purpose of Data Processing<br>Other – 15 Years from the Termination of the Employment Contract<br>Other – 15 Years from the Termination of the Employment Relationship<br>Other – 10 Years from the Termination of the Ownership | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Trade Registry Registration Processes | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Data Processing<br>Other – 15 Years from the End of the Business Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Notary Procedures | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Trade Registry Procedures | Other – 10 Years from the End of Data Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| Conducting Commercial Activities | Other – 10 Years from the End of the Purpose of Data Processing<br>Other – 10 Years from the End of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Carrying out environmental management activities | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Support for Administrative Affairs Process | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from Termination of Employment Contract<br>Other – 10 Years from Termination of Legal Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Process of Conducting Business Activities | Other – 15 Years from the Termination of the Business Relationship<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Travel Process | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |

| | | |
|---|---|---|
| | Termination of Employment Contract | |
| Process of Carrying Out Activities in Accordance with Legislation | Other – 15 Years from the Termination of the Employment Relationship<br>Other – 10 Years from the Termination of the Legal Relationship<br>Other – 10 Years from the Termination-Dissolution-Liquidation of the Company<br>Other – 10 Years from the Termination of the Purpose of Processing<br>Other – 15 Years from the Termination of the Employment Contract | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Security Management | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 days<br>Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Service Organization | Other – 15 Years from the Termination of the Employment Relationship<br>Other – 15 Years from the | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| | Termination of the Legal Relationship | |
| Waste Management | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Vehicle Allocation Tracking Process | Other – 10 Years from Termination of Legal Relationship<br>Other – 15 Years from Termination of Employment Contract<br>Other – 10 Years from Termination of Ownership | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Rental Transactions | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Ensuring Building Security | Other – 15 days | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Facility Security Activities | Other – 15 days | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Vehicle Tracking System Processes | Other – 15 Years from Termination of Employment Contract<br>Other – 10 Years from Termination of Legal Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |

| | | |
|---|---|---|
| | Other – 10 Years from Termination of Processing Purpose | |
| Embezzlement Delivery/Return Process | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Postal – Cargo Shipments | Other – 2 Years from the End of the Processing Purpose<br>Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| The Process of Carrying Out Communication Activities | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing<br>Other – 15 Years from the End of the Business Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| International Cargo Shipments | Other – 10 Years from the End of the Legal Relationship<br>Other – 2 Years from the End of the Processing Purpose | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Domestic Cargo Shipments | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage |

| | | |
|---|---|---|
| | | Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Fixed Assets and Embezzlement Transactions Regarding Personnel | Other – 15 Years from Termination of Employment Contract<br>Other – 10 Years from Termination of Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Conducting Company and Partnership Relations | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Company General Assembly Procedures | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Company Legal Entity Legal Documents Process | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 10 Years from the Termination-Termination-Liquidation of the Company | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Sending E-Bulletin | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Maintenance Repair Process | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period, |

| | | |
|---|---|---|
| | | at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Carrying out After Sales Service Activities | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Business Operation | Other – 10 Years from the End of the Purpose of Processing<br>Other – 15 Years from the End of the Business Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Periodic Maintenance and Repair Activities | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Routine Maintenance Inspection | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Obtaining Customer Feedback | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Request and Complaint Management | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Providing Customer Communication | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| Preparing a Customer List | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Carrying out marketing activities | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Order Process | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Marketing Process of Products and Services | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Customer Communication Management | Other – 10 Years from the End of the Legal Relationship<br>Other – 2 Years from the End of the Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Customer Visit Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Corporate Website Management | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |

| | | |
|---|---|---|
| Customer Complaint Management | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Web page management | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Social Media Management | Other – 2 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Customer Interview Process | Other – 2 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Export Operation | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Carrying out sales and marketing activities | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Conducting Correspondence with Institutions and Organizations | Other – 10 Years from the Termination of the Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage |

| | | |
|---|---|---|
| | Other – 10 Years from the Termination of the Legal Relationship | Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Fair Visits – Event Management | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Distributor Order Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Vehicle Allocation Usage and Tracking System | Other – 10 Years from the Termination of the Purpose of Processing<br>Other – 15 Years from the Termination of the Employment Contract<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Expense and Advance Tracking | Other – 10 Years from the End of the Purpose of Processing<br>Other – 15 Years from the End of the Legal Relationship<br>Other – 15 Years from the End of the Business Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| After Sales Support Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage |

| | | |
|---|---|---|
| | | Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Creating a Route Plan | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Customer Management | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Sales Management | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 15 Years from the Termination of the Employment Contract | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Management of Sales Made with Brokerage Firms | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Management of Online Sales | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Factory Visit Tracking | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |

| | | |
|---|---|---|
| Price Quotation Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Sales-Stock Management | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Order Management | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Survey Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Payment, Collection Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Tracking and delivery of shipments | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing | At the end of the Storage Period at the time of the first Periodic Destruction |
| Shipping Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |

| | | |
|---|---|---|
| Warehouse Process | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>within 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data.<br>Within 30 days of the request for deletion. |
| Goods Receiving Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Providing Materials for Production | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Process of Executing Product/Service Activities | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Counting Process | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Warehouse Counting Process | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Procurement Activity | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |

| | | |
|---|---|---|
| Finished Goods Acceptance Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data, at the time of the first Periodic Destruction, after the Deletion Request. |
| Periodic Control of Deterioration/Deformation in Products in Storage Areas | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Periodic Control | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Storage and Shipping Process | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Warehouse Temperature Management | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Receiving Materials Arriving by Cargo – Control Activity | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Operation Reporting Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage |

| | | |
|---|---|---|
| | | Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Stock Management | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Purchasing and Supply Activities | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Purchasing Specification Process | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Creating Supplier Records | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Purchasing Management | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |

| | | |
|---|---|---|
| Quotation Collection Process | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Creating an Approved Supplier List | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Supplier Introduction Information Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Contract Management | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Order Management Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Creating an Order Form | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Collecting Offers | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| New Product/Supplier Research | Other – 10 Years from the Termination of the Processing Purpose<br>Other – 10 Years from the | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |

| | | |
|---|---|---|
| | Termination of the Legal Relationship | |
| Service Purchase Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Creating a Tender File | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Tender Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Individual Retirement System (BES) Process | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from Termination of Employment Contract | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Banking and Payment Transactions | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 15 Years from the Termination of the Employment Contract<br>Other – 15 Years from the Termination of the Employment Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction, it will be deleted and destroyed immediately with a Deletion/Destruction Request<br>within 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data. Within 30 days of the response period after the Deletion Request. |

| | | |
|---|---|---|
| Declaration Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Accounting Procedures | Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction, it will be deleted and destroyed immediately with a Deletion/Destruction Request within 30 days at the latest as of the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Outsourced Audit Process | Other – 10 Years from Termination of Activity<br>Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Preparation of Financial Statements and Sending to Relevant Institutions | Other – 10 Years from the End of the Activity<br>Other – 10 Years from the End of the Purpose of Processing | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Customer Relationship Management Process | Other – 10 Years from Termination of Activity | At the end of the Storage Period at the time of the first Periodic Destruction |
| Preparation of Payroll and Salary File | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>within 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data.<br>Within 30 days of the request for deletion. |
| Conducting Human Resources Activities | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| | Relationship<br>1 Year | |
| Salary Payment Process | Other – 15 Years from Termination of Employment Contract<br>Other – 10 Years from Termination of Legal Relationship<br>Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Making Accounting Records | Other – 15 Years from Termination of Employment Contract | At the end of the Storage Period at the time of the first Periodic Destruction |
| SSI-Accrual Transactions | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Credit Card Transaction Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Current Account Reconciliations | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |

| | | |
|---|---|---|
| Monitoring and responding to documents and correspondence coming to the accounting department | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Insurance Process | Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| General Payment and Advance Transactions | Other – 10 Years from the Termination of the Legal Relationship<br>Other – 15 Years from the Termination of the Employment Contract | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Payment Transactions | Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Personnel Expense Tracking and Payment | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Reconciliation Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Invoice Process | Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |

| | | |
|---|---|---|
| Payment Process (General) | Other – 10 Years from the Termination of the Legal Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Check Transactions | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Current Registration Procedures | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Tax Processes | Other – 10 Years from the End of the Legal Relationship<br>Other – 10 Years from the End of the Purpose of Processing | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Ba/Bs Declaration – Reconciliation Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Bank Transactions | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Ba/Bs Declaration Process | Other – 10 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Cashier Operation Process | Other – 15 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| Payment Process | Other – 15 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Insurance Payments | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Bes Process | Other – 15 Years from Termination of Employment Contract | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Billing | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Staff Meal Organization | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| The Meal Menu Process | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Work Accident / Occupational Disease Processes | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |

| | | |
|---|---|---|
| Notification of Work Accidents and Occupational Diseases | Other – 15 Years from Termination of Employment Contract | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Occupational Health and Safety Process Management | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship<br>Other – 10 Years from Termination of Legal Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Disciplinary Management Process | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Termination Procedures | Other – 15 Years from Termination of Employment Contract<br>Other – 15 Years from Termination of Employment Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Personnel Payment and Advance Transactions | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| The Process of Carrying Out Workplace Health Activities | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from Termination of Employment Contract | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Employee Employment | Other – 15 Years 1 Year from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Job Application Management | 1 Year | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Conducting Job Application Activities | 1 Year | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Job Entry Process | Other – 15 Years 1 Year from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Creation of Employee Personnel File | Other – 15 Years from Termination of Employment Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Educational Activities | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |

| | | |
|---|---|---|
| Family Status Notification Process | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| The Process of Starting a Job and Creating a Personal File | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Process of Creating a Personnel File | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Private Health Insurance Process | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Conducting Occupational Health and Safety Activities | Other – 15 Years from Termination of Employment Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>within 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data.<br>Within 30 days of the request for deletion. |
| Execution of Permit Procedures | Other – 15 Years from Termination of Employment Relationship | As of the end of the Storage Period, at the time of the first Periodic Destruction,<br>no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| In-Service Training Planning | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Conducting Occupational Health and Safety Training and Activities | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from | As of the end of the Storage Period, at the time of the first Periodic Destruction, |

| | | |
|---|---|---|
| | Termination of Employment Contract | no later than 30 days from the notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Employee Monitoring and Guidance Process | Other – 15 Years from Termination of Employment Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Preparation of relevant procedures and regulations | Other – 15 Years from Termination of Employment Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Human Resources Process | Other – 15 Years from Termination of Employment Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Creation of Personnel Name List | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Job Entry Notifications | Other – 15 Years from Termination of Employment Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Monitoring and Procedures of Personnel Leaves | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |

| | | |
|---|---|---|
| The Process of Leaving the Job | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Movable and Immovable Management | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Rest Reports and Follow-up | Other – 15 Years from Termination of Employment Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Payroll Process | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Employment/Periodic Inspection Process | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from Termination of Employment Contract | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| PDKS System Management – Personnel Entry/Exit Records | Other – 15 Years from Termination of Employment Relationship<br>Other – 15 Years from Termination of Employment Contract | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Staff Daily Overtime Tracking | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| Personnel Working Hours Control Activity | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Work Accident Processes | Other – 15 Years from Termination of Employment Contract | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Emergency Management | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| SGK Accrual and ISKUR Transactions | Other – 15 Years from the Termination of the Business Relationship<br>Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Integrated System Document Management Process | Other – 10 Years from the Termination of the Legal Relationship | At the end of the Storage Period at the time of the first Periodic Destruction |
| Integrated System Management | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Netsis Software Program Management | Other – 10 Years from the End of Processing Purpose | At the end of the Storage Period at the time of the first Periodic Destruction |
| Fault Notification and Remedy Process | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |

| | | |
|---|---|---|
| Database Management | Other – 10 Years from the End of Processing Purpose | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Access Management – User Authorization (Ex: AD, Erp, Sap, Netsis etc.) | Other – 10 Years from the End of the Processing Purpose<br>Other – 5 Years from the End of the Processing Purpose<br>Other – 2 Years from the End of the Processing Purpose<br>Other – 10 Years from the End of the Legal Relationship | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Control of Technical Infrastructure and Business Activities | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Process 5651 – Internet Access Logs | Other – 10 Years 2 Years from the End of Processing Purpose | Within 30 days of the reply period after the end of the Storage Period of 30 days at the latest as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data,<br>at the time of the first Periodic Destruction,<br>after the Deletion Request. |
| Collection of requests and complaints | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| CCTV (Closed Circuit Camera System) | Other – 15 days | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |

| | | |
|---|---|---|
| Camera Records | Other – 15 days | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Input/Output Control | Other – 15 Years from Termination of Employment Relationship | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Office Equipment Records – Photocopier, Fax, Printer etc. Usage Information Logging | Other – 5 Years from the End of Processing Purpose<br>Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Card System Control (PDKS) | Other – 15 Years from the Termination of the Employment Relationship<br>Other – 15 Years from the Termination of the Legal Relationship | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |
| Logging Management | Other – 5 Years from the End of Processing Purpose<br>Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Internal Audit Process | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request as of the end of the Storage Period,<br>at the latest 30 days from the Notification of the Personal Data Protection Board's Decision on the Destruction of Personal Data. |

| | | |
|---|---|---|
| Project Management | Other – 5 Years from the End of the Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Backup | Other – 10 Years from the End of Processing Purpose | Within 30 days of response time after the first Periodic Destruction Request at the end of the Storage Period. |
| Forensic Analysis, Cyber Incident Analysis and Intervention | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| IT Risk Management | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Determination and supply of the company's labor, machinery, equipment and material needs | Other – 10 Years from the End of Processing Purpose | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Firewall Access Logs | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |
| Authentication – Opening/Closing User Account (Ex: Ad, Erp, Sap, Netsis etc.) | Other – 10 Years from the Termination of the Legal Relationship | At the end of the first Periodic Destruction at the latest of the 30-day Storage Period as of the Notification of the Decision of the Personal Data Protection Board Regarding the Destruction of Personal Data |

In this context, personal data is stored for the minimum retention periods stipulated in the Law:

If there is no regulation in the legislation regarding the period for which personal data should be stored, Personal Data is processed for the period required by the Data Controller's practices and commercial practices, depending on the activity carried out by the Data Controller while processing that data, and then deleted, destroyed or made anonymous. Detailed information on this subject is provided in Section 9 of this Policy.

If the purpose of processing personal data has ended; if the storage periods determined by the relevant legislation and the Data Controller have also expired; personal data may only be stored as evidence in possible legal disputes or for the purpose of asserting the relevant right related to personal data or establishing a defense. In establishing the periods herein, the storage periods are determined based on the limitation periods for asserting the said right and the examples of previous requests directed to the Data Controller on the same issues despite the expiration of the limitation periods. In this case, the stored personal data is not accessed for any other purpose and access is provided to the relevant personal data only when it is necessary to be used in the relevant legal dispute. Here too, after the mentioned period has expired, the personal data is deleted, destroyed or anonymized.

**4.3.2. Distribution of Responsibilities and Duties**

All units and employees of the Data Controller actively support the responsible units in taking technical and administrative measures to ensure data security in all environments where personal data is processed, in order to ensure the proper implementation of technical and administrative measures taken by the responsible units within the scope of the Policy, to train and raise awareness of the unit employees, to monitor and continuously audit them, and to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure that personal data is stored in accordance with the law.

**4.3.3. Recording Media**

Personal data of data owners are securely stored by the Data Controller in the environments listed in the table below in accordance with the relevant legislation, especially the provisions of the KVKK:

| **Storage Environments** |
| --- |
| Archive Cabinet |
| Paper |
| Domestic Server |
| Computer |
| Domestic Email Server |
| Flash Memory |

| |
|---|
| Hard Disk |
| Business Server |
| Locked Archive Cabinet |
| Server |
| Excel Program |
| Access Restricted File |
| Software Program – Domestic |
| Archive Room |
| Encrypted File |
| International Email Server |
| Foreign Server |
| Folder |
| Hard Disk |
| Notebook |
| Server Located in the Company |
| Online Backup Location |
| Internal Memory |

**5. CATEGORIZATION OF THE OWNERS OF PERSONAL DATA PROCESSED BY THE COMPANY**

| Personal Data Owner Category | Explanation |
|---|---|
| Worker | Natural persons who have an employment contract with the company |
| Shareholder/Partner | Real persons are shareholders of the company |
| Supplier Representative | Natural persons authorized to represent the company who are bound to the company through a supply contract. |
| Person Purchasing Product or Service | Natural persons whose personal data are obtained through the Company's business relations within the scope of operations carried out by the Company's business units, regardless of whether they have any contractual relationship with the Company. |
| Parent / Guardian / Representative | Person/persons authorized to act on behalf of a natural or legal entity that has a legal relationship with the Company. |
| Visitor | Natural persons who have entered the physical premises owned by the Company for various purposes or visited our websites. |
| Supplier Employee | Real persons who have an employment contract with the company and are bound to the company through a supply contract. |
| Potential Product or Service Buyer | Natural persons whose personal data are obtained through the Company's business relations within the scope of operations carried out by the Company's business units, as a basis for the future legal relationship with the Company. |
| Person in question | The person about whom the news was made |
| Employee Candidate | Natural persons who have applied for a job in the company by any means or have made their CV and related information available for review by our company. |
| Supplier | Supplier |
| Public Official | Public Official |
| Corporate Customer Representative/Authorized | Corporate Customer Representative/Authorized |
| Director (Non-Shareholder/Partner) | Director (Non-Shareholder/Partner) |

| | |
|---|---|
| Company Official | Company Official |
| Cargo Officer | Cargo Officer |
| Customer – Representative – Employee | Customer – Representative – Employee |
| Approved by | Approved by |
| Customs Consultant | Customs Consultant |
| Customer – Representative – Employee | Customer – Representative – Employee |
| Edited by | Edited by |
| Official | Official |
| Exporter | Exporter |
| Manufacturer | Manufacturer |
| Distributor | Distributor |
| Bank Officer | Bank Officer |
| Data Controller Officer | Data Controller Officer |
| Potential Product or Service Buyer (Natural Person) | Potential Product or Service Buyer (Natural Person) |
| Food Engineer | Food Engineer |
| Doctor | Doctor |

| | |
|---|---|
| Candidate Reference | Candidate Reference |
| Employee Relative | Employee Relative |
| Legal Advisor | Legal Advisor |
| Employer Representative | Employer Representative |
| Occupational Health and Safety Specialist | Occupational Health and Safety Specialist |
| Workplace Physician | Workplace Physician |
| Website Visitors | Website Visitors |
| Preparer | Preparer |
| Wanted People | Wanted People |
| Supervised by | Supervised by |

The table below details the above-mentioned categories of personal data owners and the types of personal data processed for those within these categories.

| **Personal Data Categorization** | **Data Subject Category to Which the Relevant Personal Data is Associated** |
|---|---|
| Information in correspondence with judicial authorities | Employee<br>Shareholder/Partner<br>Supplier Authorized<br>Person Purchasing Product or Service<br>Other – Supplier |
| Name-Surname | Employee<br>Shareholder/Partner<br>Supplier Authorized<br>Person Receiving Product or Service |

| | |
|---|---|
| | Other – Supplier<br>Parent/Guardian/Representative<br>Other – Public Official<br>Other – Corporate Customer Representative/Authorized<br>Other – Manager (Not Shareholder/Partner)<br>Other – Company Authorized<br>Supplier Employee<br>Other – Cargo Officer<br>Other – Customer – Authorized – Employee<br>Potential Product or Service Recipient<br>Other – Approving<br>Visitor<br>Person Subject to the News<br>Other – Customs Consultant<br>Other – Customer – Authorized – Employee<br>Other – Organizer<br>Other – Authorized<br>Other – Exporter<br>Other – Manufacturer<br>Other – Distributor<br>Other – Bank Authorized<br>Other – Data Controller Authorized<br>Other – Potential Product or Service Recipient (Natural Person)<br>Other – Food Engineer<br>Other – Doctor<br>Candidate Employee<br>Other – Candidate Employee Reference<br>Other – Employee Relative<br>Other – Legal Advisor<br>Other – Employer Representative<br>Other – Occupational Health and Safety Specialist<br>Other – Workplace Physician<br>Other – Preparer<br>Other – Auditor |

| | |
|---|---|
| Parents Name | Employee<br>Shareholder/Partner<br>Other – Manager (Non-Shareholder/Partner)<br>Other – Company Official<br>Supplier Employee<br>Supplier Official<br>Product or Service Purchaser Employee<br>Candidate<br>Other – Employee Relative |
| Payroll information | Worker |
| Information in the case file etc. | Employee<br>Shareholder/Partner<br>Supplier Authorized<br>Person Purchasing Product or Service<br>Other – Supplier<br>Employee Candidate |
| Date of birth | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative<br>Other – Company Official<br>Supplier Employee<br>Supplier Official<br>Product or Service Purchaser Employee<br>Candidate<br>Other – Employee Relative |
| Birthplace | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative<br>Other – Company Official<br>Supplier Employee<br>Supplier Official |

| | |
|---|---|
| | Product or Service Purchaser Employee<br>Candidate<br>Other – Employee Relative |
| Information on safety precautions etc. | Employee<br>Candidate |
| Contact address | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative<br>Product or Service Recipient<br>Other – Supplier<br>Supplier Official<br>Other – Company Official<br>Supplier Employee<br>Other – Customer – Official – Employee<br>Potential Product or Service Recipient<br>Person in the news<br>Visitor<br>Other – Customer – Official – Employee<br>Other – Customs Consultant<br>Other – Organizer<br>Other – Official Other<br>– Manufacturer<br>Other – Distributor<br>Other – Cargo Officer<br>Other – Bank Official<br>Employee Candidate<br>Other – Employee Candidate Reference<br>Other – Employee Relative<br>Other – Occupational Health and Safety Specialist |
| Signature | Employee<br>Shareholder/Partner<br>Other – Public Official |

| | |
|---|---|
| | Other – Manager (Not Shareholder/Partner)<br>Supplier Authorized<br>Person Receiving Product or Service<br>Other – Company Authorized Other<br>– Cargo Officer<br>Other – Approving<br>Parent/Guardian/Representative<br>Supplier Employee<br>Potential Product or Service Recipient<br>Other – Customs Consultant<br>Other – Organizer Other<br>– Authorized Other – Manufacturer Other – Distributor Other – Customer – Authorized – Employee Other – Supplier Other – Bank Authorized Other – Data Controller Authorized Other – Food Engineer Other – Doctor Candidate Other – Legal Advisor Other – Employer Representative Other – Occupational Health and Safety Specialist Other – Workplace Physician Other – Preparer Other – Auditor |
| Employment entry and exit document records | Worker |
| Marital status | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative |

| | |
|---|---|
| | Other – Company Official<br>Employee Candidate |
| National identity card serial number | Employee<br>Parent/Guardian/Representative<br>Supplier Official<br>Product or Service Purchaser<br>Shareholder/Partner<br>Other – Director (Non-Shareholder/Partner)<br>Other – Company Official |
| Turkish identity number etc. | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative<br>Other – Supplier<br>Supplier Official<br>Product or Service Purchaser<br>Other – Company Official<br>Supplier Employee<br>Other – Exporter<br>Other – Potential Product or Service Purchaser (Natural Person)<br>Employee Candidate<br>Other – Employee Relative<br>Potential Product or Service Purchaser |
| Phone number etc. | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative<br>Supplier Authorized<br>Other – Corporate Customer Representative/Authorized<br>Person Receiving Product or Service<br>Other – Supplier<br>Supplier Employee<br>Other – Customer – Authorized – Employee<br>Potential Product or Service Purchaser |

| | |
|---|---|
| | Visitor<br>Other – Exporter<br>Other – Authorized<br>Other – Bank Authorized<br>Employee Candidate<br>Other – Employee Candidate Reference |
| Information processed to manage commercial, technical, administrative risks, etc. | Employee<br>Shareholder/Partner<br>Supplier Authorized<br>Person Receiving Product or Service<br>Other – Supplier<br>Other – Potential Product or Service Receiver (Natural Person) |
| Address number | Employee<br>Shareholder/Partner<br>Parent/Guardian/Representative<br>Supplier Authorized<br>Person Receiving Product or Service<br>Other – Company Authorized<br>Supplier Employee<br>Other – Customer – Authorized – Employee<br>Potential Product or Service Purchaser<br>Visitor<br>Other – Organizer<br>Other – Authorized<br>Other – Exporter<br>Other – Manufacturer<br>Other – Distributor<br>Candidate Employee<br>Other – Legal Counsel |
| Email address | Parent / Guardian / Representative<br>Employee<br>Shareholder / Partner |

| | |
|---|---|
| | Supplier Authorized<br>Other - Corporate Customer Representative / Authorized<br>Person Receiving Product or Service<br>Other - Supplier<br>Other - Customer - Authorized - Employee<br>Potential Product or Service Recipient<br>Supplier Employee<br>Visitor<br>Other - Organizer<br>Other - Authorized<br>Other - Manufacturer<br>Other - Distributor<br>Other - Bank Authorized<br>Employee Candidate |
| IP address information | Employee<br>Shareholder/Partner<br>Visitor<br>Supplier Employee<br>Potential Product or Service Buyer<br>Other – Website Visitor |
| Digital Signature | Employee<br>Shareholder/Partner<br>Other – Public Official |
| Fee Information | Worker |
| His duty | Employee<br>Other – Approving<br>Shareholder/Partner<br>Potential Product or Service Buyer<br>Other – Public Official<br>Other – Customs Consultant<br>Product or Service Buyer |

| | |
|---|---|
| | Other – Authorized<br>Supplier Official<br>Other – Food Engineer<br>Other – Preparer<br>Other – Auditor |
| Current Account Records | Shareholder/Partner<br>Supplier Authorized<br>Person Purchasing Product or Service |
| Check Information | Person Receiving Product or Service<br>Supplier Authorized<br>Other – Supplier |
| Invoice | Person Receiving Product or Service<br>Other – Supplier<br>Supplier Authorized Person<br>Other – Potential Product or Service Receiver (Natural Person) |
| Promissory note | Person Purchasing Product or Service<br>Other – Supplier |
| Order information | Person Purchasing Product or Service<br>Potential Purchaser of Product or Service<br>Other – Supplier |
| Current Account Information | Other – Supplier<br>Product or Service Recipient<br>Shareholder/Partner<br>Supplier Officer |
| Bank Account IBAN Information | Employee<br>Supplier Officer<br>Product or Service Recipient<br>Other – Supplier |

| | |
|---|---|
| | Shareholder/Partner<br>Parent/Guardian/Representative<br>Potential Product or Service Recipient<br>Supplier Employee |
| Invoice Information (Finance) | Employee<br>Supplier Authorized Person<br>Other – Supplier<br>Product or Service Recipient<br>Parent / Guardian / Representative |
| Credit and risk information | Person Receiving Product or Service<br>Other – Supplier<br>Shareholder/Partner |
| Financial performance information | Shareholder/Partner |
| Asset information etc. | Shareholder/Partner |
| Registered e-mail address (KEP) | Supplier Authorized<br>Person Receiving Product or Service<br>Other – Customer – Authorized Person – Employee<br>Potential Product or Service Receiver<br>Employee |
| Information on criminal convictions | Employee<br>Candidate |
| Title | Other – Public Official<br>Shareholder/Partner<br>Other – Approver<br>Employee<br>Other – Customs Consultant<br>Other – Exporter<br>Other – Manufacturer |

| | |
|---|---|
| | Other – Distributor<br>Product or Service Purchaser<br>Other – Authorized<br>Supplier Official<br>Other – Auditor |
| Gender | Shareholder/Collaborator<br>Other<br>– Employee Relative<br>Employee Candidate |
| Date of birth | Shareholder/Partner<br>Other – Director (Non-Shareholder/Partner)<br>Employee |
| Birthplace | Shareholder/<br>Collaborator |
| Photograph | Shareholder/Partner<br>Other – Director (Non-Shareholder/Partner)<br>Employee<br>Visitor<br>Subject of the news<br>Potential Product or Service Buyer<br>Supplier Employee<br>Supplier Official |
| Passport Number | Shareholder/Partner |
| Nationality Information (Identity Information in Passport) | Shareholder/Partner |
| Religious Information (Religious Information in the Identity Card) | Shareholder/<br>Collaborator |

| | |
|---|---|
| Registered Province-District Information | Shareholder/<br>Collaborator |
| Camera recordings etc. | Employee<br>Visitor<br>Product or Service Purchaser Employee<br>Candidate<br>Shareholder/Partner<br>Potential Product or Service Purchaser<br>Supplier Employee<br>Supplier Representative |
| Phone Number | Supplier Officer<br>Shareholder/Collaborator<br>Supplier<br>Employee<br>Other – Supplier<br>Other – Occupational Health and Safety Specialist<br>Other – Wanted Persons |
| Disciplinary investigation | Employee<br>Candidate |
| The license plate number was | Working<br>Shareholder/Partner |
| Mother's Maiden Name | Worker |
| Personal health information | Supplier Employee<br>Supplier Officer<br>Employee<br>Employee Candidate |

| | |
|---|---|
| In-service training information | Supplier Employee<br>Supplier Officer<br>Employee Candidate |
| Certificates | Supplier Employee<br>Supplier Officer<br>Employee Candidate |
| Driving License Document Number | Worker |
| Debited Vehicle Information | Worker |
| Blood Group Information on the ID | Shareholder/Partner |
| Share Information | Shareholder/Partner |
| Nationality | Shareholder/Partner |
| Transaction Information | Other – Approving<br>Employee |
| Visual Records | Employee<br>Visitor<br>Shareholder/Partner<br>Person in the news<br>Potential Product or Service Buyer<br>Supplier Employee<br>Supplier Official |
| Request information etc. | Potential Product or Service Buyer<br>Person Who Receives Product or Service |
| Information obtained through campaign work, etc. | Person Purchasing Product or Service<br>Potential Product or Service Purchaser |

| | |
|---|---|
| Purchase history information | Potential Product or Service Buyer<br>Person Who Receives Product or Service |
| Questionnaire | Potential Product or Service Buyer<br>Person Who Receives Product or Service |
| Location information of the place where it is located, etc. | Person Receiving Product or Service Employee<br>Shareholder/Partner<br>Supplier Employee<br>Potential Product or Service Recipient |
| Tax Identification Number | Shareholder/Collaborator<br>Other<br>– Customs Consultant<br>Other – Exporter<br>Other – Manufacturer<br>Other – Distributor<br>Other – Supplier |
| Workplace Address | Other – Customer – Authorized Person – Employee<br>Person Purchasing Product or Service<br>Other – Customer – Authorized Person – Employee<br>Shareholder/<br>Collaborator |
| Vehicle Tracking System Data | Working<br>Shareholder/Partner |
| GPS Data | Worker |
| Bowl | Supplier Representative |

| | |
|---|---|
| Employee Bank Account Information | Worker |
| Date of Employment | Worker |
| Job | Worker |
| Diagnosis of Occupational Disease | Worker |
| Employee 1st Degree Relative Information | Worker |
| Protocol Number | Worker |
| Diploma Registration Number | Other – Doctor<br>Other – Occupational Health and Safety Specialist |
| Military Discharge Information | Employee Candidate<br>Employee |
| Diploma information | Employee Candidate<br>Employee |
| Courses attended | Employee Candidate |
| Information about the School and Department from which he/she graduated | Employee Candidate |
| Net Income and Gross Income Information | Employee Candidate<br>Employee |
| CV information | Employee Candidate |

| | |
|---|---|
| Program Information | Employee Candidate<br>Employee |
| Transcript information etc. | Employee Candidate<br>Employee |
| Foreign Language Knowledge | Employee Candidate |
| Volume No.-Sequence No.-<br>Individual Sequence No. | Worker |
| Graduation Information | Employee<br>Candidate |
| Information regarding disability status | Employee Candidate<br>Employee |
| Candidate's Strengths and Weaknesses | Employee Candidate |
| Body Language | Employee Candidate |
| Knowledge-Skills | Employee Candidate |
| Development Potential | Employee Candidate |
| Goals-Expectations-Achievements | Employee Candidate |
| Personal Development | Employee Candidate |
| Professional Experience | Employee Candidate |
| Self-Confidence (Personality Test) | Employee Candidate |

| | |
|---|---|
| Responsibility (Personality Test) | Employee Candidate |
| Sociability (Personality Test) | Employee Candidate |
| Dates of Entry and Exit from Employment | Worker |
| Employee Entry – Exit Time Information | Worker |
| Blood group information | Employee<br>Candidate |
| Performance evaluation reports etc. | Worker |
| Information about the device and prosthesis used, etc. | Worker |
| Educational Status | Worker |
| Medical Anamnesis | Worker |
| Identity and Address Information of Working Family Members | Worker |
| Entry and exit registration information of employees and visitors | Employee<br>Visitor |
| Physical Space Entry-Exit Information | Worker |
| Business Registration Number Information (SGK) | Worker |

| | |
|---|---|
| Employee Social Security Registration Number | Worker |
| Patient No. | Worker |
| Website login and logout information | Employee<br>Supplier Employee<br>Potential Product or Service Buyer<br>Other – Website Visitor<br>Visitor |
| Password and passcode information etc. | Working<br>Shareholder/Partner |
| Search History | Worker |

**6. THIRD PARTIES TO WHICH PERSONAL DATA IS TRANSFERRED BY THE COMPANY AND THE PURPOSES OF TRANSFER**

The Data Controller notifies the personal data owner about the groups of persons to whom personal data is transferred in accordance with Article 10 of the Personal Data Protection Law.

The Data Controller may transfer the personal data of data owners managed by the Policy, in accordance with Articles 8 and 9 of the Personal Data Protection Law (See Section 3/Heading 3.5), to the following categories of persons:

- Domestic Buyers: Suppliers, Authorized Public Institutions and Organizations, Natural Persons or Private Law Entities, Others
- Foreign Buyers: Natural Persons or Private Law Entities, Suppliers, Others

The scope of the above-mentioned persons to whom the data is transferred and the purposes of data transfer are stated below.

| **Persons to Whom Data Can Be Transferred** | **Definition** | **Purpose of Data Transfer** |
|---|---|---|
| Suppliers | It defines the parties that provide services to the Company on a contractual basis in accordance with the Company's orders and instructions while conducting the Company's commercial activities. | |

| | | |
|---|---|---|
| Authorized Public Institutions and Organizations | Public institutions and organizations authorized to receive information and documents from the Company in accordance with the relevant legislation. | |
| Natural Persons or Private Law Entities | Private legal entities or real persons authorized to receive information and documents from the Company in accordance with the relevant legislation. | |

In the transfers made by the Data Controller, the matters regulated in Sections 2 and 3 of the Policy are acted in accordance with.

**7. PROCESSING OF PERSONAL DATA BASED ON AND LIMITED TO THE PROCESSING CONDITIONS IN THE LAW**

The Data Controller informs the personal data owner about the personal data he processes in accordance with Article 10 of the Personal Data Protection Law.

**7.1. Processing of Personal Data and Special Personal Data**

**7.1.1. Processing of Personal Data**

The explicit consent of the personal data owner 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 present. The basis for the personal data processing activity may be only one of the conditions listed below, or more than one of these conditions may be the basis for the same personal data processing activity. If the processed data is special personal data; the conditions set out in heading 7.1.2. under this section below shall apply.

Although the legal bases for the processing of personal data by the Data Controller vary, all personal data processing activities are carried out in accordance with the general principles set out in Article 4 of the Personal Data Protection Law (See 3.1.).

**7.1.1.1. Explicit Consent of the Personal Data Owner**

One of the conditions for processing personal data is the explicit consent of the owner. The explicit consent of the personal data owner must be related to a specific subject, based on information and expressed with free will.

For personal data processing activities other than the processing purpose (primary processing) for the purposes for which personal data is obtained (secondary processing), at least one of the conditions set out in Articles 7.1.1.2 - 7.1.1.8 of this title is required; if one of these conditions is not present, these personal data processing activities are carried out by the Data Controller based on the explicit consent of the personal data owner for these processing activities.

In order for personal data to be processed based on the explicit consent of the personal data owner, the explicit consent of the personal data owners is obtained through relevant methods.

#### 7.1.1.2. Explicitly Provided in Laws

The data owner's personal data may be processed in accordance with the law if it is clearly provided for in the law.

#### 7.1.1.3. Failure to Obtain the Explicit Consent of the Person Concerned Due to Actual Impossibility

If the processing of personal data is necessary to protect the life or physical integrity of the person or another person who is unable to give his consent due to a de facto impossibility or whose consent cannot be validated, the personal data of the data owner may be processed.

#### 7.1.1.4. Directly Related to the Establishment or Performance of the Contract

Processing of personal data is possible if it is necessary to process personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract.

#### 7.1.1.5. Fulfillment of Legal Obligations by the Data Controller

The Data Controller may process the data subject's personal data if processing is necessary to fulfill its legal obligations as the data controller.

#### 7.1.1.6. Personal Data Owner's Publicization of Personal Data

If the data owner has made his/her personal data public, the relevant personal data may be processed.

#### 7.1.1.7. Data Processing is Necessary for the Establishment or Protection of a Right

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

#### 7.1.1.8. Data Processing is Necessary for the Legitimate Interest of the Data Controller

Data may be processed if it is mandatory for the legitimate interests of the Data Controller, provided that it does not harm the fundamental rights and freedoms of the personal data owner.

### 7.1.2. Processing of Special Personal Data

Special personal data is processed by the Data Controller in the following cases, unless the personal data owner gives explicit consent, provided that sufficient measures are taken, as determined by the Personal Data Protection Board:

- Special personal data, other than the health and sexual life of the personal data owner, in cases prescribed by law,
- Sensitive personal data regarding the health and sexual life of the personal data owner may only be disclosed by persons or authorized institutions and organizations that are under a confidentiality obligation for the purposes of protecting public health, providing preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and their financing.

### 7.2. Personal Data Processing Activities Conducted at Building and Facility Entrances and Within the Building and Facility

Personal data processing activities carried out by the Data Controller at the entrances of buildings and facilities and within the facility are carried out in accordance with the Constitution, the Personal Data Protection Law and other relevant legislation.

In order to ensure security, the Data Controller carries out personal data processing activities in the Data Controller buildings and facilities, such as monitoring with security cameras and monitoring guest entries and exits.

Personal data processing is carried out by the Data Controller by using security cameras and recording guest entries and exits.

The cameras are divided into two groups: indoor and outdoor cameras. Indoor cameras are positioned at an angle that will not directly attract employees or visitors, except for sinks, rooms, changing rooms, and room interiors. The locations of the cameras have been carefully determined to ensure that monitoring activity is maintained at a minimum level and limited to monitoring purposes.

#### 7.2.1 Monitoring Activities with Cameras Conducted at the Entrances and Inside the Building and Facility of the Data Controller

In this section, explanations will be made regarding the camera monitoring system of the Data Controller and information will be provided on how personal data, privacy and fundamental rights of the individual are protected.

Within the scope of the surveillance activity with security cameras, the Data Controller aims to protect the interests of the Data Controller and other persons in ensuring their security.

#### 7.2.2 Conducting Monitoring Activities with Security Cameras in Accordance with the Personal Data Protection Law

The Data Controller complies with the regulations in the PDP Law when conducting camera surveillance activities for security purposes. The Data Controller carries out security camera surveillance activities in order to ensure security in its buildings and facilities, for the purposes stipulated in the relevant legislation in force and in accordance with the personal data processing conditions listed in the PDP Law.

#### 7.2.3 Announcement of Camera Monitoring Activity

The Data Controller informs the personal data owner in accordance with Article 10 of the Personal Data Protection Law. The Data Controller notifies the data owner about the camera monitoring activity by more than one method of informing about general issues (See Section 3/Heading 3.3). In this way, it is aimed to prevent harm to the fundamental rights and freedoms of the personal data owner, to ensure transparency and to inform the personal data owner.

Regarding the camera monitoring activity by the Data Controller; this Policy is published on the Data Controller's website (online policy regulation) and a notification notice regarding the monitoring is hung at the entrances of the areas where monitoring is carried out (on-site lighting).

#### 7.2.4 Purpose of Carrying Out Camera Monitoring Activity and Limitation to Purpose

In accordance with Article 4 of the Personal Data Protection Law, the Data Controller processes personal data in a limited and proportionate manner, in connection with the purpose for which they are processed.

The purpose of the Data Controller's video camera monitoring activity is limited to the purposes listed in this Policy. Accordingly, the monitoring areas, numbers and times of surveillance cameras are implemented in a way that is sufficient and limited to achieve the security purpose. The privacy of the person is not monitored in areas that may result in an intervention that exceeds the security purposes (for example, toilets).

**7.2.5 Ensuring the Security of the Data Obtained**

The Data Controller takes the necessary technical and administrative measures to ensure the security of personal data obtained as a result of camera monitoring activities in accordance with Article 12 of the Personal Data Protection Law. (See 2.1)

**7.2.6 Storage Period of Personal Data Obtained through Camera Surveillance Activities**

Detailed information on the retention period of personal data obtained through camera surveillance by the Data Controller is provided in Article 4.3 of this Policy, titled "Personal Data Retention Periods".

If the footage obtained from the security camera is determined to constitute evidence for a criminal investigation before the deletion period, it is stored until it is submitted to the judicial authority if it constitutes evidence for a criminal investigation.

The images obtained from security cameras are stored for 10 years if it is determined that they constitute evidence for a legal dispute before the deletion period.

**7.2.7 Who Can Access the Information Obtained as a Result of Monitoring and To Whom This Information Is Transferred**

Only a limited number of Data Controller employees have access to the records recorded and stored digitally with live camera images. The limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality commitment.

IF THERE ARE VISITORS IN THE PERSON GROUP

**7.3. Data Controller Monitors Guest Entrances and Exits Conducted at Building and Facility Entrances**

The Data Controller carries out personal data processing activities to ensure security and to monitor guest entries and exits in the Data Controller buildings and facilities for the purposes specified in this Policy.

The personal data owners in question are informed in this context when the names and surnames of the persons who come to the Data Controller buildings as guests are obtained or through texts hung at the Data Controller or made accessible to the guests in other ways. The data obtained for the purpose of monitoring guest entries and exits is processed only for this purpose and the relevant personal data is recorded in the data recording system in a physical environment.

**7.4. Keeping Records Regarding Internet Access Provided to Our Visitors in Data Controller Buildings and Facilities**

In order to ensure security by the Data Controller and for the purposes specified in this Policy; Internet access can be provided to Visitors who request it during their stay in our buildings and facilities by the Data Controller. In this case, log records regarding your Internet access are recorded in accordance with the mandatory provisions of Law No. 5651 and the legislation regulated under this Law; these records are processed only upon request by authorized public institutions and organizations or in order to fulfill our relevant legal obligations in the audit processes to be carried out within the Data Controller.

Within this framework, only a limited number of Data Controller employees have access to the log records obtained. Data Controller employees who have access to the aforementioned records only access these records for the purpose of using them in requests or audit processes from authorized public institutions and organizations and share them with legally authorized persons. A limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality commitment.

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

As regulated in Article 138 of the Turkish Penal Code and Article 7 of the Personal Data Protection Law, if the reasons requiring processing are eliminated, personal data are deleted, destroyed or made anonymous based on the Data Controller's own decision or upon the request of the personal data owner, even though the data has been processed in accordance with the relevant legal provisions.

In this context:

- Change or repeal of legislation,
- Termination or invalidity of the contract underlying the processing,
- Elimination of the purposes and conditions of processing,
- Withdrawal of consent in processing activities based on explicit consent,
- The Data Owner's application for deletion-destruction-anonymization and acceptance of this application,
- The decision that the request to be made by the Personal Data Protection Board as a result of the Data Owner's application and the rejection of this application must be met,
- Expiration of the storage period,
- Periodic destruction operations carried out by the Data Controller,

As a result, the Data Controller deletes, destroys or anonymizes the Personal Data it has collected.

Pursuant to Article 11 of the Regulation, the Data Controller has determined the periodic destruction period as follows. Accordingly,

- At the end of the Storage Period at the time of the first Periodic Destruction
- Within 30 days of the request for deletion to respond.
- Within 30 days at the latest from the notification of the Personal Data Protection Board's decision on the destruction of personal data.
- It is deleted and destroyed immediately with the Deletion/Destruction Request.

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

The Data Controller deletes, destroys or anonymizes the Personal Data it collects, on its own or upon the request of the Data Owner, if the reasons requiring processing are eliminated. According to Article 28 of the Law, personal data that has been anonymized may be processed for purposes such as research, planning and statistics. Such processing after anonymization is outside the scope of the Law, and in this case, the explicit consent of the Personal Data Owner is not required.

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

#### 8.1.1. Destruction of Physical Documents

Personal Data collected by our company and processed by non-automatic means, although they are part of our data recording systems, can also be destroyed by physically destroying the medium (paper, microfiche) on which they are located in a manner that will not allow the subsequent use of the Personal Data on them.

#### 8.1.2. Destruction of Digital Documents

Digital Documents containing Personal Data produced or obtained in digital environments within the Company are permanently deleted in a way that makes them inaccessible and reusable for the Relevant Users.

#### 8.1.3. Deletion from Database

In our company, Personal Data stored in the database is deleted from the relevant database in a way that makes it inaccessible and reusable for the Relevant Users in no way.

Data can be deleted by deleting data by giving a delete command to the electronic recording media we use, such as Commercial Package Programs, Human Resources Programs, SQL databases, by removing the access rights of the Relevant Users to the files located on our central server or to the directory where the files are located, by deleting the relevant lines in the databases with database commands, or by deleting the Personal Data located on portable media (USB, HDD, etc.) using appropriate software.

However, in cases where some Personal Data is deleted and other data is not accessible in the system, the Personal Data subject to deletion may be archived by making it unrelated to the relevant Data Owner; in this case, the relevant Personal Data is deemed to have been deleted. In such cases, our Company takes all necessary technical and administrative measures to ensure that Personal Data is accessed only by authorized persons.

#### 8.1.4. Deletion from Used Software Programs

Personal Data stored in digital environments within our Company is deleted from the relevant software in a way that makes it inaccessible and unusable for the Relevant Users.

Data can be deleted by deleting data by giving a delete command to the electronic recording media we use, such as Commercial Package Programs, Human Resources Programs, SQL databases, by removing the access rights of the Relevant Users to the files located on our central server or to the directory where the files are located, by deleting the relevant lines in the databases with database commands, or by deleting the Personal Data located on portable media (USB, HDD, etc.) using appropriate software.

However, in cases where some Personal Data is deleted and other data is not accessible in the system, the Personal Data subject to deletion may be archived by making it unrelated to the relevant Data Owner; in this case, the relevant Personal Data is deemed to have been deleted. In such cases, our Company takes all necessary technical and administrative measures to ensure that Personal Data is accessed only by authorized persons.

**8.1.5. Deletion from the Cloud System**

Personal Data stored in cloud systems within the Company are permanently deleted from the cloud system in a way that makes them inaccessible and reusable for the Relevant Users.

However, in cases where some Personal Data is deleted and other data is not accessible in the system, the Personal Data subject to deletion may be archived by making it unrelated to the relevant Data Owner; in this case, the relevant Personal Data is deemed to have been deleted. In such cases, our Company takes all necessary technical and administrative measures to ensure that Personal Data is accessed only by authorized persons.

**8.1.6. Overwriting**

The magnetic media and rewritable optical media used in our company are a data destruction method that eliminates the possibility of reading and recovering old data by writing random numerical data through special software. Any reusable magnetic media with Personal Data on it is cleaned irreversibly by using the overwriting method.

**8.1.1 Deletion from Used Software Programs**

Personal Data stored in digital environments within the Data Controller are deleted from the relevant software in a way that makes them inaccessible and unusable for the Relevant Users.

Data can be deleted by deleting data by giving a delete command to the electronic recording media we use, such as Commercial Package Programs, Human Resources Programs, SQL databases, by removing the access rights of the Relevant Users to the files located on our central server or to the directory where the files are located, by deleting the relevant lines in the databases with database commands, or by deleting the Personal Data located on portable media (USB, HDD, etc.) using appropriate software.

However, in cases where some Personal Data is deleted and other data is not accessible in the system, the Personal Data subject to deletion may be archived by making it unrelated to the relevant Data Owner; in such cases, the relevant Personal Data is deemed to have been deleted. In such cases, the Data Controller takes all necessary technical and administrative measures to ensure that only authorized persons can access the Personal Data.

**8.1.2 Obscuration of Personal Data on Paper**

Personal Data collected in paper environment such as physical application forms, contracts, personnel files collected by the Data Controller for the continuation of its commercial activities can also be deleted by making them unreadable in the paper environment they are in. In particular, in order to prevent malicious, non-intended use or to delete Personal Data requested to be deleted, all personal data that is relevant or subject to the request is physically cut off in a part of the document or rendered invisible using fixed ink in a way that cannot be reversed and read by technological solutions.

**8.1.3 Destruction of Physical Document**

Although the Data Controller is a part of our data recording systems, the Personal Data that we process by non-automatic means can also be destroyed by physically destroying the Personal Data on the medium (paper, microfiche) in a way that does not allow it to be used later.

**8.1.4 Overwriting**

Data Controller is a data destruction method that eliminates the possibility of reading and recovering old data by writing random numerical data through magnetic media and rewritable optical media, special software. Any reusable magnetic media that contains Personal Data is irreversibly purged using the overwrite method.

**8.1.5 Masking**

With the masking method, certain areas of Personal Data are made incapable of being associated with the real person who is the Data Owner by crossing out, painting and/or starring method. For example, an identity data belonging to the customer within the Data Controller is removed from our database, making it impossible to identify the Data Owner.

**8.1.6 Data Derivation**

As the Data Controller, it may use some Personal Data stored for marketing activities. In the event that situations arise that require the deletion of such data from our database, the Data Controller creates a more general content than the content of the Personal Data with the data derivation method, making the Personal Data not associated with any real person.

**8.1.7 Anonymization**

The method of generalization of Personal Data is used in order to aggregate many data available in the Data Controller's data base and make them unassociated with any real person, so that the Data Controller can follow some results without storing any Personal Data. In this way, for example, the results of which year range, in which positions, and in which age range employment is more efficient can be tracked without showing the dates of birth and identity information of our employees whose employment contract has been terminated.

**8.1.8 Deletion from the Cloud System**

Personal Data stored/stored in cloud systems within the Data Controller are permanently deleted from the cloud system in a way that makes them inaccessible and unusable in any way for the Relevant Users.

However, in cases where it is not possible to access some data in the system due to the deletion of some Personal Data, the Personal Data subject to deletion can be archived by making it unable to be associated with the relevant Data Owner; in this case, the relevant Personal Data is deemed to have been deleted. In such cases, the Data Controller takes all necessary technical and administrative measures to ensure that Personal Data is accessed only by authorized persons.

**8.1.9 Destruction of Digital Document**

Digital Documents containing Personal Data produced or obtained in digital environments within the Data Controller are permanently deleted in a way that makes them inaccessible and unusable for the Relevant Users in any way.

**8.1.10 Deletion from the Database**

Personal Data stored in the Data Controller database is deleted from the relevant database in a way that makes it inaccessible and unusable for the Relevant Users in any way.

Deletion of data by giving deletion command to electronic recording media such as Commercial Package Programs, Human Resources Programs, SQL databases we use, removal of the access rights of the Relevant Users to the files on our central server or on the directory where the files are located; Data can be deleted by deleting the relevant lines in databases with database commands or by deleting Personal Data on portable media (USB, HDD, etc.) using appropriate software.

However, in cases where it is not possible to access some data in the system due to the deletion of some Personal Data, the Personal Data subject to deletion can be archived by making it unable to be associated with the relevant Data Owner; in this case, the relevant Personal Data is deemed to have been deleted. In such cases, the Data Controller takes all necessary technical and administrative measures to ensure that Personal Data is accessed only by authorized persons.

**9. RIGHTS OF PERSONAL DATA OWNERS; METHODOLOGY OF THE USE AND EVALUATION OF THESE RIGHTS**

**9.1. Rights of the Data Owner and Exercise of These Rights**

**9.1.1. Rights of the Personal Data Owner**

Personal data owners have the following rights:

1. To learn whether personal data is processed or not,
2. If personal data has been processed, requesting information about it,
3. To learn the purpose of processing personal data and whether they are used in accordance with their purpose,
4. To know the third parties to whom personal data is transferred in the country or abroad,
5. Requesting correction of personal data in case of incomplete or incorrect processing and requesting notification of the transaction made within this scope to third parties to whom personal data has been transferred,
6. Although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, to request the deletion or destruction of personal data in the event that the reasons requiring its processing disappear, and to request the notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,
7. Objecting to the occurrence of a result against the person himself by analyzing the processed data exclusively through automated systems,
8. Requesting the compensation of the damage in case of damage due to unlawful processing of personal data.

**9.1.2. Situations in which the Personal Data Owner cannot assert his rights**

Pursuant to Article 28 of the KVK Law, personal data owners cannot assert the rights listed in 10.1.1. on these issues, as the following cases are excluded from the scope of the KVK Law:

1. Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.
2. Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or does not constitute a crime.
3. Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
4. Processing of personal data by judicial authorities or enforcement authorities in relation to investigation, prosecution, trial or execution proceedings.

Pursuant to Article 28/2 of the KVK Law; In the following cases, personal data owners cannot assert their other rights listed in 10.1.1., except for the right to demand compensation for the damage:

1. The processing of personal data is necessary for the prevention of crime or for criminal investigation.
2. Processing of personal data made public by the personal data owner.
3. The processing of personal data is necessary for the execution of supervisory or regulatory duties and disciplinary investigation or prosecution by authorized and authorized public institutions and organizations and professional organizations in the nature of public institutions, based on the authority granted by the law.
4. The 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 issues.

**9.1.3. Exercising the Rights of the Personal Data Owner**

Personal Data Owners are required to submit to Article 9.1.1 of this section. They will be able to submit their requests regarding their rights listed under the heading to the Data Controller free of charge by filling out and signing the Application Form with information and documents that will identify their identities and by the following methods or other methods determined by the Personal Data Protection Board:

- After filling out the form at www.orimpex.com.tr, a wet signed copy of it is sent to AOSB 10040 SOKAK NO:28 ÇİĞLİ/İZMİR by hand or through a notary public

- After filling out the form at the www.orimpex.com.tr address and signing it with your "secure electronic signature" within the scope of the Electronic Signature Law No. 5070, sending the form with a secure electronic signature to the orimpexas@hs01.kep.tr address by registered e-mail

In order for third parties to request an application on behalf of personal data owners, there must be a special power of attorney issued by the data owner through a notary public on behalf of the person who will apply.

**9.1.4. The Right of the Personal Data Owner to File a Complaint with the KVK Board**

In cases where the application is rejected in accordance with Article 14 of the KVK Law, the answer given is insufficient or the application is not answered in due time; It can file a complaint with the KVK Board within thirty days from the date of learning the answer of the Data Controller and in any case within sixty days from the date of application.

**9.2. Data Controller's Response to Applications**

**9.2.1. Procedure and Time of the Data Controller to Respond to Applications**

In the event that the personal data owner submits his/her request to the Data Controller in accordance with the procedure set forth in section 9.1.3 of this section, the Data Controller will conclude the relevant request free of charge within thirty days at the latest, depending on the nature of the request. However, if a fee is stipulated by the KVK Board, the fee in the tariff determined by the KVK Board will be collected from the applicant by the Data Controller.

**9.2.2. Information that the Data Controller may request from the Personal Data Owner who applied**

The Data Controller may request information from the relevant person in order to determine whether the applicant is the owner of personal data. In order to clarify the issues in the application of the personal data owner, the Data Controller may ask the personal data owner about his application.

**9.2.3. Data Controller's Right to Reject the Application of the Personal Data Owner**

The Data Controller may reject the application of the applicant by explaining the reason in the following cases:

1. Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.
2. Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or does not constitute a crime.
3. Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
4. Processing of personal data by judicial authorities or enforcement authorities in relation to investigation, prosecution, trial or execution proceedings.
5. Processing of personal data is necessary for the prevention of crime or criminal investigation.
6. Processing of personal data made public by the personal data owner.

7. The processing of personal data is necessary for the performance of supervisory or regulatory duties or disciplinary investigation or prosecution by authorized public institutions and organizations and professional organizations with the status of public institutions, based on the authority granted by law.

8. The processing of personal data is necessary to protect the economic and financial interests of the State in relation to budgetary, tax and financial matters.

9. The request of the personal data owner may interfere with the rights and freedoms of other persons.

10. Requests have been made that require disproportionate effort.

11. The requested information is publicly available information.

**10. RELATIONSHIP OF THE COMPANY PERSONAL DATA PROTECTION AND PROCESSING POLICY WITH OTHER POLICIES**

The Data Controller may also create sub-policies for internal use regarding the protection and processing of personal data related to the principles set forth in this Policy, as well as other policies for certain groups of people, particularly employees.

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

ORİMPEX TEXTILE

orimpexas@hs01.kep.tr

AOSB 10040 STREET NO:28 ÇİĞLİ/İZMİR

0 (232) 431-0276

info@orimpex.com.tr

www.orimpex.com.tr

**Orimpex**

Orimpex Organic Textiles

**Communication**

AOSB 10040 street No:28
Çiğli - İZMİR / TURKEY

Tel.: +90 ( 232 ) 431 02 76
Mail: info (@) orimpex.com.tr

Personnel Request/Complaint Form