

**ACCURIDE WHEELS BİLECİK JANT SANAYİ A.Ş**  
**PERSONAL DATA PROTECTION AND PROCESSING POLICY**

**TABLE OF CONTENTS**

<b>CHAPTER 1: INTRODUCTION</b> .....	<b>3</b>
I. IMPORTANCE OF PERSONAL DATA PROTECTION.....	3
II. THE AIM OF THE POLICY.....	3
III. SCOPE .....	3
IV. IMPLEMENTATION OF THE POLICY AND THE RELEVANT REGULATION .....	4
V. ACCESS AND UPDATING .....	4
<b>CHAPTER 2: PROCESSING OF PERSONAL DATA</b> .....	<b>4</b>
I. PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH THE PRINCIPLES AND RULES STIPULATED IN THE REGULATION .....	5
II. TRANSFER OF PERSONAL DATA .....	7
III. KİŞİSEL VERİ KATEGORİZASYONLARI .....	10
<b>CHAPTER 3: LEGAL GROUNDS AND PURPOSES FOR THE PROCESSING OF THE PERSONAL DATA</b> .....	<b>14</b>
I. LEGAL GROUNDS FOR THE PROCESSING OF THE PERSONAL DATA ....	14
1. <b>General Principles</b> .....	14
2. Reasons for the Compliance with the Law.....	14
3. <b>Processing of the Personal Data of Special Quality and Reasons for the Compliance with the Law</b> .....	15
II. PURPOSES FOR THE PROCESSING OF THE PERSONAL DATA.....	15
<b>CHAPTER 4: RETENTION, DELETION, DESTRUCTION AND ANONYMIZATION OF THE PERSONAL DATA</b> .....	<b>19</b>
I. RETENTION OF THE PERSONAL DATA AND RETENTION PERIODS .....	19
II. DELETION, DESTRUCTION AND ANONYMIZATION OF THE PERSONAL DATA .....	19
1. <b>Deletion of the Personal Data</b> .....	19
2. Destruction of the Personal Data.....	20

<b>3. Anonymization of the Personal Data</b> .....	20
<b>CHAPTER 5: RIGHTS OF THE RELEVANT PERSON</b> .....	21
I. SCOPE OF THE RIGHTS OF THE RELEVANT PERSON AND USE OF THESE RIGHTS .....	21
<b>1. Rights of the Relevant Persons</b> .....	21
<b>2. Use of the Rights by the Relevant Persons</b> .....	21
<b>3. Reply to the Applications</b> .....	23
<b>CHAPTER 6: ENSURING THE SECURITY OF THE PERSONAL DATA</b> .....	23
I. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR ENSURING THE PROCESSING OF THE PERSONAL DATA IN COMPLIANCE WITH THE LAW .....	23
II. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN IN THE PROCESSING OF THE PERSONAL DATA OF SPECIAL QUALITY	24
III. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR PREVENTING THE ACCESS TO THE PERSONAL DATA IN CONTRARY TO THE LAW .....	25
<b>1. Technical Measures Taken For Preventing The Access To The Personal             Data In Contrary To The Law</b> .....	25
<b>2. Administrative Measures Taken For Preventing The Access To The Personal             Data In Contrary To The Law</b>	27
IV. RETENTION OF THE PERSONAL DATA IN SECURE ENVIRONMENTS .....	28
<b>1. Technical Measures taken for the Retention of the Personal Data in Secure             Environments</b> .....	28
<b>2. Administrative Measures taken for the Retention of the Personal Data in             Secure Environments</b> .....	28
V. TRAINING .....	28
VI. INSPECTION .....	29
1. Increase and Inspection of the Awareness of the Business Departments on the Protection and Processing of the Personal Data .....	29
2. Increase and Inspection of the Awareness of the Business Partners and the Suppliers on the Protection and Processing of the Personal Data .....	29
3. Inspection of the Measures taken for the Protection of the Personal Data .....	29

## CHAPTER 1: INTRODUCTION

### I. IMPORTANCE OF PERSONAL DATA PROTECTION

The protection of personal data is a constitutional right and is a priority for our Company. For this purpose, it is aimed to establish a system that is constantly updated in our Company and this policy has been established. Within the scope of the Personal Data Protection Law No. 6698 ("Law"), in order to fulfill the general disclosure obligation of **Accuride Wheels Bilecik Jant Sanayi A.Ş** (the "Company") as a Data Controller and to determine the basic principles of our Company's personal data processing rules, this Personal Data Protection and Processing Policy ("Policy") is made, and in this context, the basic principles are regulated regarding the protection of the personal data of our customers, potential customers, employees, employee candidates, interns and students, supplier / sub-contractor employees and officials, company shareholders and company partners, visitors and other third parties whose data we process.

With regard to the implementation of the issues specified in this Policy, necessary procedures are arranged within the company, the clarification texts are created in accordance with the **Personal Data Processing Inventory** specific to individual categories, the contracts on protection of personal data and confidentiality are made with Company employees and third parties who have access to personal data, the job descriptions are revised, the necessary administrative and technical measures are taken by the Company to protect personal data, and the necessary inspections are or get made in this context. The issue of Protection of Personal Data is also adopted by the senior management, and personal data protection processes are managed by establishing a special Committee on this issue (the **Company's Personal Data Protection Studies Committee**).

### II. THE AIM OF THE POLICY

The main aim of this Policy is to set forth the principles for the personal data processing activities and protection of personal data carried out by the Company in accordance with the law, and to provide transparency by clarifying and informing the persons whose personal data are processed by our company.

### III. SCOPE

This policy is related to all personal data of the persons who we categorized under the following headings *“our customers, potential customers, employees, employee candidates, interns and students, supplier / sub-employer employees and officials, company shareholders and company partners, visitors, product or service purchasers, employee references, employee family and relatives, parents/guardians/representatives and other third parties whose data we process”* that we process either automatically or by non-automatic means provided that they are part of any data recording system.

#### **IV. IMPLEMENTATION OF THE POLICY AND THE RELEVANT REGULATION**

The relevant legal regulations in force regarding the processing and protection of personal data will primarily be applied. In case of inconsistency between the current legislation and the Policy, our Company adopts that the applicable legislation will apply.

#### **V. ACCESS AND UPDATING**

The policy is published on our company's website [[www accuridecorp.com](http://www accuridecorp.com)] and made available to the relevant persons upon the request of personal data owners and updated when necessary.

### **CHAPTER 2: PROCESSING OF PERSONAL DATA**

Our company processes personal data in accordance with Article 20 of the Constitution and Article 4 of the Law, in line with the law and the rules of honesty, accurate and when necessary, in line with specific, explicit and legitimate purposes, in connection with the purpose, in a limited and reasonable manner. Our company keeps personal data for the period stipulated by law or as required by the purpose of processing personal data.

Our company processes personal data in accordance with Articles 20 of the Constitution and Articles 5 of the Law, based on one or more of the conditions in Article 5 of the Law.

Our company processes the personal data of employees and employee candidates based on the purposes of job suitability and performance of the employment contract in accordance with Article 419 of the Code of Obligations, without prejudice to this Law.

Our company clarifies the personal data owners in accordance with the 20th article of the Constitution and the 10th article of the Law and provides the necessary information in case the personal data owners request information and apply to exercise their rights arising from the law, and responds to the applications within the legal period.

Our company acts in accordance with the regulations stipulated in terms of processing of personal data of special nature in accordance with Article 6 of the Law.

In accordance with the 8th and 9th articles of the Law 20th, our company complies with the rules stipulated by the law regarding the transfer of personal data and carries out its activities taking into account the decisions taken and communiqués published by the Personal Data Protection Board ("Board") and the safe country lists.

## I. PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH THE PRINCIPLES AND RULES STIPULATED IN THE REGULATION

### 1. Principles of Processing of Personal Data

#### *A) Processing in accordance with the Law and the Principle of Good Faith*

Our company acts in accordance with the principles of legal regulations and the principle of good faith in the processing of personal data. In this context, our company determines the legal bases that will require the processing of personal data, takes into account the requirements of proportionality, does not use personal data outside the purpose required, and does not perform any processing activities without the knowledge of individuals.

#### *B) Ensuring that Personal Data is Accurate and Up-To-Date*

Our company ensures that the personal data it processes are accurate and up-to-date, taking into account the fundamental rights of personal data owners and their own legitimate interests, and takes necessary measures in this direction. In this context, data on all categories of persons are kept up-to-date. In particular, customer and potential customer data are carefully updated, marketing and promotional e-mails and offers are not sent to individuals out of their consent.

#### *C) Processing with Certain, Clear and Legitimate Purposes*

Our company clearly and precisely determines the purpose of processing personal data that is legitimate and lawful. Our company processes personal data in connection with and to the extent required for the services it provides. The purpose of processing personal data by our company is determined prior to the processing and is also processed in the "**Personal Data Inventory**".

#### *D) Being Connected, Limited, and Proportional to the Purpose of Processing*

Our company processes personal data in a way that is convenient for the achievement of the specified purposes and avoids the processing of personal data that is not needed or not related to the achievement of the purpose. In this context, processes are constantly reviewed and the principle of "**Data Minimization**" is tried to be implemented.

#### *E) Retention As Long As Stipulated in the Applicable Legislation or Required for the Purpose of Processing*

Our Company retains the personal data only for the period specified in the relevant legislation or necessary for the purpose of processing. Within this scope, our Company first of all determines whether any period for keeping the personal data is stipulated in the relevant legislation; if any period has been determined, acts in compliance with this period; takes into account the legal and penal timeout periods within this scope; and retains the personal data for the period necessary for the purpose of processing. In the case of the expiration of the period or in the case that the reasons requiring the processing of the personal data disappear, the personal data is deleted, destroyed or made anonymous in accordance with the "**Retaining and Disposal of Personal Data**" procedure of our Company.

## **2. Rules for the Processing of the Personal Data of General Quality**

The protection of the personal data is a right granted in the Constitution and the fundamental rights and freedoms, save for their essence, can be restricted only depending on the reasons specified in the relevant articles of the Constitution and only by law. In accordance with the third paragraph of the Article 20 of the Constitution, the personal data will be able to be processed only in the cases stipulated in the law or with the explicit consent of the person. The personal data is processed by our Company without requiring the explicit consent of the relevant person only if the following requirements are met in the processing of the personal data;

- a) Expressly stipulated in the Laws,
- b) It is strictly required for the protection of the life or physical body integrity of the person, or someone else, who may not disclose his consent due to actual impossibility or whose consent is not accepted as valid and applicable,
- c) The processing of the personal data of the parties to the contract is strictly necessary, provided that it is directly related to the execution or performance of a contract,
- d) The personal data is obligatory for the Data Supervisor to be able to fulfill its legal liability,
- e) The personal data has been publicized by the relevant person,
- f) The data processing is mandatory for the establishment, use or protection of a right,
- g) The data processing is obligatory for the legitimate interests of the Data Controller without prejudice to the fundamental rights and freedoms of the personal data owner.

If the requirements above are not met, the explicit, free will and information-based consent of the relevant person is applied to by our Company. It is taken as basis that the data is principally based on the reasons of compliance with the law remaining out of the consent by taking into account the dependency relationship of the employee especially in the field of Human Resources and Employment Affairs and only in the event that these reasons do not exist, the explicit consent is applied to. On the contrary, the processing activity is performed by taking as basis the express consent of the relevant person in the activities such as marketing. However, in all cases where the personal data is processed, the data processing activity is performed certainly upon “**clarification**”.

## **3. Rules for the Processing of the Personal Data of Special Quality**

In the processing of the personal data designated as “special quality” by the Law, our Company acts in compliance with the regulations stipulated in the Law. In the Article 6 of the Law, certain personal data which bears the risk of causing the unjust treatment of the persons or discrimination when they are processed in contrary to the law is designated as “special quality” and care and sensitivity must be shown in the processing of such data. This data are the ones related to race, ethnic origin, political thought, philosophical belief, religion, communion or other believes, appearance, association, foundation or union membership, health, sexual life, conviction or security measures and the biometric and genetic data. The personal data of special quality are processed by our Company in compliance with the Law a) Acts the following cases, provided that the necessary measures are taken:

- ✓ The personal data of special quality other than the health and sexual life of the relevant person is processed in the cases stipulated in the laws or based on the explicit consent of the relevant person, if any,
- ✓ The special quality personal data regarding the health and sexual life of the relevant person,

however, is processed by the persons or authorized institutions and organizations under the confidentiality obligation or with the explicit consent of the relevant person only for the purpose of protecting the public health, executing the preventive medicine, medical diagnosis, treatment and care services and planning and managing the health services and their finance.

✓ Regardless of which reason it is based on, the general data processing principles are always taken into account and the compliance with these principles is ensured in the processing courses (PDPL a. 4; see above 2nd Section, I,1). In relation to the protection of the data of special quality, **“Protection of Personal Data of Special Quality Policy”** was put into force in our Company and the actions and the necessary measures are taken in accordance with the provisions of this policy in our business departments.

#### **4. Making Clarification and Giving Information to the Relevant Persons whose Data are Processed**

Our Company makes clarification to the personal data owners during the acquisition of the personal data in compliance with the Article 10 of the Law. Within this scope, the relevant person whose data are processed is clarified on for which purpose the personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method and legal reason of collecting personal data and the rights of the relevant person whose personal data are processed, and the relevant departments of our Company fulfill the necessary proceedings in accordance with our Company’s **“Clarification Principles Procedure”**. In the Article 11 of the Law, **“Information Request”** is also listed among the rights of the relevant person whose personal data are processed and our Company, within this scope, gives the necessary information if the relevant person whose personal data are processed requests them in compliance with the Article 20 of the Constitution and the Article 11 of the Law and our Company performs the proceedings in this matter in line with the **“Relevant Person Application Procedure”**.

## **II. TRANSFER OF PERSONAL DATA**

Our Company can transfer the personal data and the personal data of special quality of the relevant person whose personal data are processed to third persons by taking the necessary security measures in line with the personal data processing purposes. Our Company, accordingly, acts in compliance with the regulations stipulated in the Article 8 of the Law.

### **1. Principles for the Transfer of the Personal Data**

In line with the legitimate and lawful personal data processing purposes, our company may transfer personal data to third parties based on one or more of the personal data processing conditions listed below and specified in Article 5 of the Law, on a limited basis.

If the relevant person whose personal data are processed gives his explicit consent, based on this explicit consent; or

- ✓ If there is a explicit regulation in the laws regarding that the personal data will be transferred,
- ✓ If it is compulsory for the protection of the life or physical body integrity of the relevant person or any other person and if the relevant person cannot disclose his consent due to actual impossibility or if his consent is not legally accepted;
- ✓ If the transfer of the personal data of the parties to the contract is strictly necessary, provided that it is directly related to the execution or performance of a contract,
- ✓ If the personal data transfer is compulsory for our Company to fulfill its legal obligations,
- ✓ If the personal data has been publicized by the relevant person,

- ✓ If the personal data transfer is compulsory for the establishment, use or protection of any right,
- ✓ If the personal data transfer is compulsory for the legitimate interests of our Company, provided that it will not cause damage to the fundamental rights and freedoms of the relevant person whose personal data are processed.

Regardless of which reason it is based on, the general data processing principles are always taken into account and the compliance with these principles is ensured in the transferring courses (Law a. 4; see above 2nd Section, I,1).

## **2. Transferring of the Personal Data of Special Quality**

Our Company may transfer the data of special quality of the relevant person whose personal data are processed to third parties in line with legitimate and lawful personal data processing purposes by showing necessary care, taking necessary security measures and taking sufficient measures stipulated by the Board.

- If the relevant person gives his explicit consent, based on this explicit consent or
- If the relevant person does not give his explicit consent;
  - ✓ The personal data of special quality other than the health and sexual life of the relevant person (data related to race, ethnic origin, political thought, philosophical belief, religion, communion or other believes, appearance, association, foundation or union membership, health, sexual life, conviction or security measures and biometric and genetic data) can be processed in the cases stipulated in the laws,
  - ✓ The special quality personal data regarding the health and sexual life of the personal data owner, however, may be processed by the persons or authorized institutions and organizations under the confidentiality obligation only for the purpose of protecting the public health, executing the preventive medicine, medical diagnosis, treatment and care services and planning and managing the health services and their finance.

In relation to the transferring of the personal data of special quality, the “**Protection of Personal Data of Special Quality Policy**” was put into force in our Company and the actions and the necessary measures are taken in accordance with the provisions of this policy in our business departments. Regardless of which reason it is based on, the general data processing principles are always taken into account and the compliance with these principles is ensured in the transferring courses (Law a. 4; see above 2nd Section, I,1).

## **3. Transfer of Personal Data to Abroad**

Our Company may transfer the personal data and the personal data special quality that it processes to third parties by taking the necessary security measures in line with lawful personal data processing purposes. The personal data will be able to be transferred by our Company to the countries which are announced by the Board to have sufficient protection (“Foreign Country Having Sufficient Protection”) or the foreign countries for which the data controllers in Turkey and the relevant foreign country committed a sufficient protection in written in the event that such countries do not have sufficient protection and for which the Board gives consent (“Foreign Country in which the Data Controller Committing the Sufficient Protection is Present”). Our Company, accordingly, acts in compliance with the regulations stipulated in the Article 9 of the Law.



Our Company will be able to transfer the personal data to the Foreign Countries Having Sufficient Protection or to the countries in which the Data Controller Committing the Sufficient Protection is Present if the relevant person whose personal data are processed gives his explicit consent; or in case presence of any of the following cases if the relevant person whose personal data are processed does not give his explicit consent in line with the legitimate and lawful personal data processing purposes:

- ✓ If there is an explicit regulation in the laws regarding that the personal data will be transferred,
- ✓ If it is compulsory for the protection of the life or physical body integrity of the relevant person whose personal data are processed or any other person, and if the relevant person whose personal data are processed cannot give his consent due to actual impossibility or if his consent is not legally accepted;
- ✓ If the transfer of the personal data of the parties to the contract is strictly necessary, provided that it is directly related to the execution or performance of a contract,
- ✓ If the personal data transfer is compulsory for our Company to fulfill its legal obligations,
- ✓ If the personal data has been publicized by the relevant person,
- ✓ If the personal data transfer is compulsory for the establishment, use or protection of any right,
- ✓ If the personal data transfer is compulsory for the legitimate interests of our Company, provided that it will not cause damage to the fundamental rights and freedoms of the relevant person.

#### **4. Purposes for the Transfer of the Personal Data by our Company and Categories of the Persons to whom the Transfer is made**

##### ***A) Data Transfer Purposes***

The data transfer is made for the purposes such as ensuring that the activities and establishment objectives of our Company are fulfilled, ensuring that the provision to our Company of the necessary services which our Company procures externally from the supplier and which are required for the fulfillment of the commercial activities of the Company, ensuring that the human resources and employment policies of our Company are implemented and ensuring that the obligations of our Company within the framework of our occupational health and safety are fulfilled and the necessary measures are taken.

##### ***B) Persons to whom the Data are transferred***

Our Company may transfer the **personal data** to the person categories specified below in accordance with the Articles 8 and 9 of the Law:

AUTHORIZED PUBLIC INSTITUTIONS	Public institutions and organizations authorized to obtain information and documents from our Company	Data is shared in accordance with the provisions of the relevant legislation.
AUTHORIZED PRIVATE ENTITIES	Private entities authorized to obtain information and documents from our Company	Data is shared in a limited manner for the purpose requested by the relevant private entities within the scope of their legal authority.

AFFILIATES	The companies in which our Company is a shareholder.	Data is shared in a limited manner in order to ensure that commercial activities that also require the participation of our Company's affiliates are carried out.
SHAREHOLDER	Shareholders of our Company	Data is shared in a limited manner in order to design strategies regarding the commercial activities of our Company as well as auditing purposes.
BUSINESS PARTNERS	Parties with which our company establishes business partnerships for purposes such as sales, promotion and marketing of our company's products and services, after-sales support, and execution of joint customer loyalty programs while conducting its commercial activities.	Limited data sharing is carried out in order to ensure the fulfillment of the establishment objectives of the business partnership.
SUPPLIER	Parties that provide services to our Company while our Company is conducting its commercial activities.	Limited data sharing is carried out in order to provide our Company with the services that our company procures externally from the supplier and that are necessary for our Company to fulfill its commercial activities.

In the transfers made by our company, we act in accordance with the principles and rules set out in this Policy.

### III. PERSONAL DATA CATEGORIZATIONS

The persons whose data are processed, and the data processed within this scope are categorized as follows in our Company;

#### PERSON CATEGORIZATION

EMPLOYEE CANDIDATE	Real bodies who have made a job application to our Company by any means or who have opened their
--------------------	--

	curriculum vitae and relevant information to our Company for examination
EMPLOYEE	Real bodies working in our Company
POTENTIAL CUSTOMER	Real bodies who have requested to use our services or who are interested in using our services or who are considered to be interested in using our services in compliance with the commercial customs and good faith rules.
INTERN/STUDENT	Students who carry out their internship in our Company, the students who receive education/make internship subject to CMEK.
SUPPLIER'S PERSONNEL	Real bodies working in the corporations (such as, without limitation, business partnership, supplier) with which our Company is in all kinds of business relationships
SUPPLIER'S AUTHORIZED PERSON	Real bodies who are the shareholders and authorized persons of the corporations with which our Company is in a business relationship
PRODUCT-SERVICE RECEIVER / AUTHORIZED PERSON OF THE PRODUCT-SERVICE RECEIVER	The real bodies who use or have used the products and services offered by our Company (the product or service buyer) or the Legal Entity Authorities who use / have used them, regardless of whether they have any contractual relationship with our company.
CUSTODIAN/GUARDIAN/REPRESENTATIVE	Real bodies whose personal data are processed in the capacity of custodians, guardians or representatives.
VISITOR	Real bodies who have entered into the physical premises owned by our Company for various purposes or who visit our websites
OTHER	Third party real bodies who are related to the person categorizations and data processing processes whose data our Company processes when fulfilling Human Resources, Production and service processes (For example; Family Members and relatives, Employee References)

**DATA CATEGORIZATION**

CREDENTIALS	Information available in the documents such as Driving License, Birth Certificate, Residence Certificate, Passport, Attorneyship Identity, Marriage Certificate, which is obvious to belong to a real person whose credentials are definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
CONTACT DETAILS	Information such as telephone number, address, e-mail, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system
LOCATION DETAILS	Information determining the location of the personal data owner during the use of our services by him or of our employees and the employees of the corporations with which we are in cooperation while they are using the tools of our Company, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
PERSONAL DATA	All kinds of personal data processed for obtaining the information that will form the basis of the formation of the personal rights of the our employees or the real persons who are in an employment relationship with our Company, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
LEGAL TRANSACTIONS AND COMPLIANCE DETAILS	Your personal data processed within the scope of the determination and follow-up of our legal receivables and rights, the settlement of our debts, our legal obligations and the policies of our Company, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
CUSTOMER TRANSACTION DATA	Information such as the records for the use of our services, the instructions necessary for the use of the services by the customer and the requests, which is obvious to belong to a real person whose identity is definite or determinable and which is included in the data recording system.

PHYSICAL SPACE SECURITY DATA	Personal data regarding the records and documents taken at the entry into the physical space and during the stay inside the physical space, which is obvious to belong to a real person whose identity is definite or determinable and which is included in the data recording system.
TRANSACTION SECURITY DATA	Personal data processed for ensuring the technical, administrative, legal and commercial security while the activities are being carried out, which is obvious to belong to a real person whose identity is definite or determinable and which is included in the data recording system
RISK MANAGEMENT DATA	Personal data processed by the methods that are used in compliance with the generally accepted legal, commercial customs and honesty rule in these fields for us to be able to manage our commercial, technical and administrative risks, which is obvious to belong to a real person whose identity is definite or determinable and which is included in the data recording system.
FINANCIAL DATA	Personal data processed with respect to the information, documents and records indicating all kinds of financial result created according to the type of the legal relationship which our Company has established with the personal data owner, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
PERFORMANCE AND CARRIER DEVELOPMENT DATA (OCCUPATIONAL EXPERIENCE DATA)	Personal data processed for the purpose of measuring the performance of our employees or the real persons who are in an employment relationship with our Company and planning and executing their carrier development within the scope of the human resources policy of our Company, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
MARKETING DATA	Personal data processed for customizing and marketing our services in line with the usage habits, taste and needs of the personal data owner and the reports and evaluations created as a result of these processing outcomes, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.
AUDIO-VISUAL DATA	Photographs and camera records (except for the records included within the scope of the Physical Space Security Information), sound records and data included in the documents which are the copies of the documents including personal data, which is obvious to belong to a real person whose identity is definite or determinable; which is processed partially or wholly in an automatic manner or in a non-automatic manner as a part of the data recording system.

EMPLOYEE'S RELATIVES AND FAMILY DATA	Data regarding the relatives and family members of the employees.
REFERENCE DETAILS	Data regarding those who have referenced the employee and employee candidates.
SPECIAL DATA OF SPECIAL QUALITY (HEALTH, SEXUAL LIFE)	Data regarding health and sexual life.
SPECIAL DATA OF SPECIAL QUALITY II	Data related to race, ethnic origin, political thought, philosophical belief, religion, communion or other believes, appearance, association, foundation or union membership, conviction or security measures and the biometric and genetic data.

### **CHAPTER 3: LEGAL GROUNDS AND PURPOSES FOR THE PROCESSING OF THE PERSONAL DATA**

#### **I. LEGAL GROUNDS FOR THE PROCESSING OF THE PERSONAL DATA**

##### **1. General Principles**

Although the legal grounds for the processing of the personal data by our Company differ, the action is taken in compliance with the general principles set forth in the article 4 of the Law in all kinds of personal data processing activities. Accordingly; in all kinds of data processing activities, the following general principles are taken into account:

- a) Compliance with the law and the honesty rules,
- b) Being accurate and current when necessary,
- c) Being processed for certain, express and legitimate purposes,
- d) Being related to, limited to and proportional to the processing purpose,
- e) Being kept for the period stipulated in the relevant legislation or for the period required for the processing purpose.

##### **2. Reasons for the Compliance with the Law**

**A) Personal Data Owner's giving his Explicit Consent**

One of the processing requirements of the personal data is the explicit consent of the data owner. The explicit consent of the personal data owner should be clarified with respect to a specific subject, based on notification and with free will.

**B) Expressly Stipulated in the Laws**

The personal data of the relevant person can be processed in compliance with the law if expressly stipulated in the laws. *For instance, the notification of the identities of our employees to the competent authorities pursuant to the Identity Notification Legislation.*

**C) Inability to obtain the Explicit Consent of the Relevant Person due to Physical Impossibility**

The personal data of the relevant person can be processed if the processing of the personal data is compulsory for protecting the life or physical body integrity of the person who cannot disclose his consent due to the physical impossibility or whose consent is not accepted as valid and applicable or any other person. *For instance, sharing the blood type information of the employee who felt faint with the physician.*

**D) Direct Relation with the Establishment or Performance of the Contract**

It is possible to process the personal data if the processing of the personal data of the parties to the contract is necessary, provided that it is directly related to the establishment or performance of a contract. *For instance, receiving a CV from the candidate for the establishment of the employment contract, obtaining an address for notification under the contract.*

**E) Fulfillment of the Legal Obligation by the Company**

The personal data of the data owner can be processed if the processing is compulsory for the fulfillment of its legal obligations by our Company as the data controller. *For instance, processing the family information in order to have the Employee take advantage from the Minimum Living Allowance.*

**F) Publicization of the Personal Data by the Relevant Person**

If the relevant person, has publicized his personal data by himself, the relevant personal data can be processed. *For instance, if the customers of our Company submit their complaints, requests or suggestions in a platform open to the public on the internet, these customers are deemed to have publicized their relevant information. In this case, it is possible for the data to be processed by the authorized person of our Company, provided that it will be limited to the purpose of answering the complaints, requests or suggestions.*

**G) Compulsory Data Processing for the Establishment or Protection of any right**

If the data processing is compulsory for the establishment, use or protection of any right, the personal data of the data owner can be processed. *For instance, keeping the data which has the characteristic of an evidence (sales contract, invoice) and using it at the time when it is necessary.*

**H) Compulsory Data Processing for the Legitimate Interest of our Company**

If the data processing is compulsory for the legitimate interests of our Company, provided that it will not cause damage to the fundamental rights and freedoms of the personal data owner, the personal data of the data owner can be processed. *For instance, monitoring the critical points of the*

*Company against theft or for occupational safety purpose with security camera.*

### **3. Processing of the Personal Data of Special Quality and Reasons for the Compliance with the Law**

The personal data of special quality may be processed by our Company only in the cases stipulated in the laws, provided that the sufficient measures to be determined by the Board will be taken if the relevant person does not give his explicit consent. The special quality personal data regarding the health and sexual life of the personal data owner, however, may be processed by the persons or authorized institutions and organizations under the confidentiality obligation only for the purpose of protecting the public health, executing the preventive medicine, medical diagnosis, treatment and care services and planning and managing the health services and their finance. Regardless of which reason it is based on, the general data processing principles are always taken into account and the compliance with these principles is ensured in the processing courses (PDPL a. 4; see above 2nd Section, I,1).

## **II. PURPOSES FOR THE PROCESSING OF THE PERSONAL DATA**

Our Company processes personal data as limited to the purposes and conditions included in the personal data processing requirements specified in the second paragraph of the article 5 and the 3rd paragraph of the article 6 of the Personal Data Protection Law. Within the course of data processing, the aforementioned legal grounds are taken into account and, if the other reasons for the compliance with the law are not available, the consent of the relevant person is requested. At this point, the general principles are inspected within the scope of the article 4 and principally it is sought from the data processing activity to comply with the principles for the compliance with the law in general.

The consent of the relevant person, however, is obtained “explicitly, based on notification and free will”. The purposes for the processing of the personal data are specified also in “the **Personal Data Inventory**” of our Company.

The personal data is processed especially for the following purposes in the departments of our Company;

- For the fulfillment of the reciprocal obligations arising from the employment contract as the employer, the personal data of the **EMPLOYEES, STUDENTS AND INTERNS** (in general, the employees) and their **CUSTODIANS/GUARDIANS/REPRESENTATIVES** should be processed. The personal data of the employees is processed and kept in compliance with the law and the good faith rules, accurately and up-to-date when necessary, in line with the certain, express and legitimate purposes, as related to, limited to and proportional to the purpose. Within this scope, the explicit consent which will be requested from the employees in the cases where the data processing is compulsory for the execution of the processes of establishing, performing and terminating the employment contract in compliance with the law, the legitimate interests of the Company, provided that it will not be in contrary to the fundamental rights and freedoms, the cases expressly stipulated in the law, the fulfillment of the legal obligations related to the employment of the employees, the establishment, use and protection of the right in the cases of legal proceedings, which is based on notification and which the employees will disclose with their own free will in line with the purposes necessary for the employment of the employees in compliance with the laws constitute the legal grounds for the processing of the personal data.



- Within the scope of the activities required by the field of business of the Company, the legitimate interests of the employer require the processing of the personal data of the employees. The activity of processing the personal data of the employees can be performed due to the reasons such as preventing the misconducts, preventing the theft, ensuring the general security or the occupational health and safety. However, in this case, a great care is shown not to cause damage to the fundamental rights and freedoms of the employees.
  
- If the employee becomes a union member after obtaining the status of "employee" (not required in the employee candidacy category), union membership can also be processed in accordance with the explicit provisions of the law in order to fulfill the requirements of the legal legislation. Apart from this, the data of the employees in relation to race, ethnic origin, political thought, philosophical belief, religion, communion or other believes, appearance of the employees are not included among the personal data processed unless expressly stipulated in the law, as a rule, and if an exceptional application will be made, the requirements are carefully evaluated before processing the personal data and the express consent of the relevant person is obtained. The Company makes inspection and observations on the information communication means (telephone, mobile telephones, computers and internet). The Law no 5651 and the legitimate interests of our Company constitute the legal bases of the mentioned applications.
  
- In addition to our employees, our visitors and other categories of people who are connected to the internet through our Company's system can also be included in the scope of this processing. The vehicle tracking system can be applied for the reasons of “security, management of the vehicles and the personnel in a more effective manner” in the vehicles of our Company. The mentioned activity is also based on the legitimate interests of our Company and performed, provided that it will not cause damage to the fundamental rights and freedoms of the employees.
  
- ✓ Personal data of **EMPLOYEE RELATIVES AND FAMILY MEMBERS** are also processed in connection with the processes of providing contact and communication during emergency processes (for example, informing in case of an accident), fulfilling legal obligations such as minimum living allowance and employee relations processes.
- ✓ According to the Labor Law No. 4857, Law of Obligations No. 6098, Article 419, Law No. 6698 on the Protection of Personal Data and relevant legislation, our Company may process personal data such as name, address, date of birth, e-mail address, telephone number and other contact information, CV, cover letter, previous or relevant work experience or other experience, educational background, transcript, language test results, or supporting or explanatory documents related to the job application, video conference, telephone, or records of information obtained during the interview in case of face-to-face interviews, and the references stated in the job application of the **EMPLOYEE CANDIDATES** who applied for job. In the context of employee candidacy, it is strongly recommended that the candidate refrain from specifying any personal information and especially sensitive (sensitive) data that are not directly related to their competencies (race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, biometric and genetic data), and if there are relevant parts of the CV and documents submitted in writing, they should be darkened and delivered to the Company. In addition, for the **PERSONAL DATA** (name, surname, telephone, e-mail, etc.) of the **REFERENCE PERSON(S)** included in the candidate's resume and whose data are processed in this process, the candidate must be informed that he/she is responsible for informing the person in question and obtaining their express consent(s) when delivering to the Company.

- Personal data of **SUPPLIERS / SUBCONTRACTOR AUTHORITIES AND EMPLOYEES** can also be processed by our Company. In the Law no 6331, the documents and information required to be controlled in relation to the employees who come from another workplace to the principal employer in relation to the occupational health and safety are specified. Likewise, in the Labor Law no 4857 and the Social Insurances and General Health Insurance Law no 5510, obligations are imposed to the principal employer in relation to the subcontractor workers and the temporary workers and, within this scope, the issues required to be controlled are specified. Accordingly, the processing of the personal data of the workers who work at our workplace as associated to the supplier and another employer is based on the legitimate interests of our enterprise, mainly the mentioned legal regulations. **The data of PRODUCT-SERVICE RECEIVES OR THEIR AUTHORITIES** area also within the scope of the commercial activity and legal relation with the relevant person.
- The personal data is processed in our Relevant Departments also for the purpose of:
  1. carrying out the emergency management processes
  2. carrying out the information security processes
  3. carrying out the Employee Candidate / Intern / Student Selection and Placement Processes
  4. carrying out the Application Processes of the Employee Candidates
  5. carrying out the Employee Satisfaction and Loyalty Processes
  6. fulfilling the Obligations Arising From Employment Contract And Legislation For Employees
  7. carrying out the Fringe Benefits and Benefits Processes for Employees
  8. carrying out the auditing/ethical activities
  9. carrying out the training activities
  10. carrying out the access authorizations
  11. carrying out the activities in compliance with the legislation
  12. carrying out the financing and accounting affairs
  13. carrying out the company/product/service engagement processes
  14. providing the security of the physical spaces
  15. carrying out the assignment processes
  16. following up and carrying out legal affairs,
  17. carrying out the internal audit/investigation/intelligence activities
  18. carrying out the communication activities
  19. planning of human resources processes
  20. carrying out/inspecting business affairs
  21. Carrying out Occupational Health / Safety Activities
  22. Receiving and Evaluating Suggestions for the Improvement of Business Processes
  23. Carrying out Business Continuity Activities
  24. carrying out the logistics activities
  25. Carrying out Goods/Service Purchase Processes
  26. Carrying out Goods/Service After Sales Support Services
  27. Carrying out Goods/Service Sale Processes
  28. Carrying out Goods/Service/Production and Operation Processes
  29. Carrying out Customer Relationship Processes
  30. Conducting Activities for Customer Satisfaction
  31. Organization and Event Management
  32. Conducting Marketing Analysis Studies
  33. Carrying out Performance Evaluation Processes
  34. Carrying out Advertising / Campaign / Promotion Processes

35. Carrying out Risk Management Processes
  36. Carrying out Custody and Archive Activities
  37. Carrying out Social Responsibility and Civil Society Activities
  38. Carrying out the Contract Processes
  39. Carrying out the sponsorship activities
  40. Carrying out Strategic Planning Activities
  41. Tracking Requests/Complaints
  42. Ensuring Security of Movable Goods and Resources
  43. Carrying out the supply chain management processes
  44. Carrying out Wage Policy
  45. Carrying out Marketing Process of Products/Services
  46. Ensuring the Security of Data Supervisor Operations
  47. Work and Residence Permit Procedures of Foreign Personnel
  48. Carrying out Investment Processes
  49. Conducting Talent / Career Development Activities
  50. Informing Authorized Persons, Institutions and Organizations
  51. Carrying out the management activities
  52. Creating and tracking visitor records.
- In our workplaces, **Visitor Records and** camera surveillance are carried out for the purposes of occupational health and safety, general security and product safety by taking into account the legitimate interests of our company, on the condition that it does not harm the fundamental rights and freedoms of our visitors, persons whose data is processed, and especially employees.

#### **CHAPTER 4: RETENTION, DELETION, DESTRUCTION AND ANONYMIZATION OF THE PERSONAL DATA**

If the reasons requiring the processing of the personal data disappear even though they have been processed in compliance with the provisions of the relevant law, the personal data is deleted, destroyed or anonymized based on our Company's own decision or upon the request of the personal data owner as regulated in the article 138 of the Turkish Criminal Law and the article 7 of the Law.

##### **I. RETENTION OF THE PERSONAL DATA AND RETENTION PERIODS**

Our Company retains the personal data if stipulated in the relevant laws and the legislation for the period specified in the relevant legislation. If any period is not regulated in the legislation with respect to how long the personal data is required to be retained, the retention periods are determined by taking into consideration the statute of limitations / limitation periods that may arise within the scope of the legal relationship related to the person concerned. Regarding the Storage of Personal Data, the "**Storage and Destruction of Personal Data**" procedure has been put into effect, and detailed retention periods are specified in the "**Personal Data Inventory**".

##### **II. DELETION, DESTRUCTION AND ANONYMIZATION OF THE PERSONAL DATA**

If the reasons requiring the processing of the personal data disappear even though they have been processed in compliance with the provisions of the relevant law, the personal data is deleted, destroyed or anonymized based on our Company's own decision or upon the request of the personal data owner as regulated in the article 138 of the Turkish Criminal Law and the article 7 of the Law.

In this case, after the expiration of the mentioned period, the personal data is deleted, destroyed or anonymized.

## **1. Deletion of the Personal Data**

### ***A) Procedure of deleting the Personal Data***

Our Company can delete the personal data based on its own decision or upon the request of the relevant person if the reasons requiring the processing of the personal data disappear even though they have been processed in compliance with the provisions of the relevant law. The deletion of the personal data is the procedure of making the personal data inaccessible and un reusable **for the relevant users**. All kinds of technical and administrative measures necessary for the deleted personal data to become inaccessible and un reusable for the relevant users are taken by our Company.

### ***B) Process of deleting the Personal Data***

The process required to be followed in the procedure of deleting the personal data is as follows:

- Determination of the personal data to be subject to the deletion procedure.
- Determination of the relevant users for each personal data by using access authorization and control matrix or a similar system.
- Determination of the authorizations and methods of the relevant users such as access, recovery, reuse etc..
- Closure and elimination of the authorizations and methods of the relevant users such as access, recovery, reuse etc. within the scope of the personal data.

### ***C) Methods of deleting the Personal Data***

As the personal data can be retained in various recording environments, they are deleted by the methods suitable for the recording environments.

## **2. Destruction of the Personal Data**

### ***A) Procedure of destroying the Personal Data***

Our Company may destroy the personal data based on its own decision or upon the request of the relevant person if the reasons requiring the processing of the personal data disappear even though they have been processed in compliance with the provisions of the relevant law. The destruction of the personal data is the **procedure of making the personal data inaccessible, unrecoverable and un reusable by any person**. Our Company takes all kinds of necessary technical and administrative measures related to the destruction of the personal data.

### ***B) Methods of destroying the Personal Data***

For the destruction of the personal data, all copies including the data are determined and the systems including the data are destroyed one by one.

## **3. Anonymization of the Personal Data**

### ***A) Procedure of anonymizing the Personal Data***

The anonymization of the personal data is to make the personal data not to be able to be correlated

with a real person whose identity is definite or determinable by any means even by matching with other data. Our Company may anonymize the personal data when the reasons requiring the processing of the personal data processed in compliance with the law disappear. Our Company takes all kinds of necessary technical and administrative measures related to the anonymization of the personal data.

The personal data which is anonymized may be processed for the purposes such as research, planning and statistics in compliance with the article 28 of the Law. This type of processing is out of the scope of the Law and the explicit consent of the personal data owner shall not be sought.

### ***B) Methods of anonymizing the Personal Data***

Anonymization is the removal or modification of all direct and / or indirect identifiers in a data set, preventing the identification of the relevant person from being identified or losing its distinctiveness within a group or crowd in a way that cannot be associated with a real person. The data which does not point out a specific person as a result of prevention or lose of these characteristics are deemed to have been anonymized. The purpose of anonymization is to disconnect the relation between the data and the person who is identified by that data. The anonymization methods stand for the entire disconnection procedures carried out by the methods such as grouping, masking, derivation, generalization, randomization which are automatic or non-automatic and which are applied to the records available in the data recording system where the personal data is retained.

The data obtained as a result of the application of these methods should not be able to identify a specific person.

## **CHAPTER 5: RIGHTS OF THE RELEVANT PERSONS**

### **I. SCOPE OF THE RIGHTS OF THE RELEVANT PERSONS AND USE OF THESE RIGHTS**

#### **1. Rights of the Relevant Persons**

The persons whose personal data is processed by our Company have the rights set forth below:

- ✓ Learning whether the personal data has been processed or not,
- ✓ Requesting the relevant information if the personal data has been processed,
- ✓ Learning for what purposes personal data relating to them are processed and whether these data are used in line with these purposes,
- ✓ Having information of the third persons to whom personal data relating to them are transferred in the country and overseas,
- ✓ Requesting rectification of personal data relating to them in cases where they are processed incompletely or inaccurately, and to request informing third parties to whom your personal data were transferred about this rectification within this scope,
- ✓ Requesting deletion or destruction of personal data in case the reasons requiring its processing disappear, although it has been processed in accordance with the provisions of the Law and the provisions of other relevant law, and requesting the notification of this transaction to third parties to whom your personal data were transferred,
- ✓ Objecting to the occurrence of a result against the person himself by analyzing the personal data exclusively via automatic systems,

✓ Requesting compensation for damages caused by unlawful processing of personal data.

## 2. Use of the Rights by the Relevant Persons

It is necessary and sufficient for the Relevant Persons to submit their requests regarding the exercise of the above-mentioned rights in accordance with paragraph 1 of Article 13 of the Law, to our Company by choosing one of the following methods and addresses;

<b>Application Method</b>	<b>Application Address</b>	<b>Information Required to be Stated While Applying</b>
<b>Personal Application</b>  (Applicant must come in person and apply with a document certifying his/her identity)	[Genel Müdürlük Binası - Fatih mah. Sanayi Küme Evler Bölgesi No:44, Bayırköy Beldesi Merkez/Bilecik 11120]  [Küçükbakkalköy mah. Dudullu cad. R2 Blok Sit. Brandium apt. No:23-25B/259 Ataşehir/İSTANBUL]	The envelope shall bear the statement:  <u>"Information Request Under the Law on Protection of Personal Data "</u> .
<b>Notification through Notary Public</b>	[Genel Müdürlük Binası - Fatih mah. Sanayi Küme Evler Bölgesi No:44, Bayırköy Beldesi Merkez/Bilecik 11120] [Küçükbakkalköy mah. Dudullu cad. R2 Blok Sit. Brandium apt. No:23-25B/259 Ataşehir/İSTANBUL]	The statement <u>"Information Request Under the Law on Protection of Personal Data"</u> should appear on the service envelope.
Shall be signed with <b>"Secure Digital Signature"</b>  and sent through registered e-mail.	[- <a href="mailto:accuride.kvvk@hs01.kep.tr">accuride.kvvk@hs01.kep.tr</a> ]	The subject of the email shall be:  <u>"Information Request Under the Law on Protection of Personal Data"</u> .

The applications must include name, surname and, if the application is in written, signature, T.R. Identity Number for the Turkish citizens; and for the foreigners: nationality, passport number or identity number, if any, residence or workplace address for notification, electronic mail address, if any, for notification, telephone number and fax number, and subject of the request.

The relevant information and documents shall also be added to the application.

It is not possible for the third persons to make a request on behalf of the relevant person. For any person other than the relevant person to make a request, a special power of attorney must be issued by the relevant person in the name of the person who will make an application with respect to the subject matter. In the application containing the explanations about the right requested to be used as the person concerned; the requested matter must be clear and understandable, the requested subject must be related to the person concerned or if someone is acting on behalf of someone else, this must be specifically authorized and documented, the application must include identity and address information, and documents certifying your identity must be attached to the application.

The Relevant Person Application Form is available at the website of our Company.

### **3. Reply to the Applications**

In the event that the Relevant Person has conveyed his/her request in compliance with the procedure stipulated, our Company shall conclude the relevant request free of charge within the shortest period of time as per the nature of the request and within no later than thirty days. However, if the procedure requires an extra cost, the fee in the tariff determined by the Board shall be collected from the applicant by our Company. Our Company may request information from the relevant person in order to determine whether the applicant is the relevant person. Our Company may ask questions to the relevant person in relation to their application in order to clarify the issues set forth in the application of the relevant person. The applications are managed within our Company in accordance with the “**Relevant Person Application Procedure**” of our Company.

## **CHAPTER 6: ENSURING THE SECURITY OF THE PERSONAL DATA**

### **I. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR ENSURING THE PROCESSING OF THE PERSONAL DATA IN COMPLIANCE WITH THE LAW**

Our Company takes all necessary technical and administrative measures in order to ensure the processing of the personal data in compliance with the law. Within this scope;

- ✓ Within the scope of our Company, the Data Inventory (Data Mapping) compatible with the VERBIS system is issued and the inspections regarding the compliance with the law and the purpose are made herein.
- ✓ For our Company to fulfill its obligation of making clarifications to the relevant persons completely and properly, the “**Procedure for the Clarification Principles in the Processing of the Personal Data**” was put into force.
- ✓ The employees are informed about the personal data protection law and the processing of the personal data in compliance with the law.
- ✓ All activities carried out by our Company are analyzed in detail as specific to each business

department and as a result of this analysis, compliance with the legislation is ensured in personal data processing processes specific to the activities carried out by the relevant business departments.

- ✓ The personal data processing activities carried out by the business departments of our Company and the requirements to be fulfilled for ensuring the compliance with the personal data processing conditions required by the Law no 6698 are determined as specific to each business department and the detail activity carried out by it.
- ✓ The records imposing the obligation not to process, not to disclose and not to use the personal data, except for the exemptions introduced with the instructions of the Company and by the law, are included into the contracts and documents managing the legal relationship between our Company and the employees and the awareness of the employees on this matter is raised and the inspections are carried out.
- ✓ The records imposing the obligation not to process, not to disclose and not to use the personal data, except for the exemptions introduced with the instructions of the Company and by the law, are included into the contracts and documents managing the legal relationship between our Company and the third persons processing the data for which our Company is responsible and the **“Procedure on Confidentiality and Protection of Personal Data with Third Parties”** was put into force on this matter.

## **II. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN IN THE PROCESSING OF THE PERSONAL DATA OF SPECIAL QUALITY**

The law attached special importance to certain personal data due to the risk of causing victimization or discrimination when unlawfully processed. These data are the ones related to race, ethnic origin, political thought, philosophical belief, religion, communion or other believes, appearance, association, foundation or union membership, health, sexual life, conviction or security measures and the biometric and genetic data. Our Company acts with sensitivity in the protection of the personal data of special quality which are designated as “special quality” by the Law and processed in compliance with the law. Within this scope, the technical and administrative measures taken by our Company for the protection of the personal data are applied carefully in terms of the personal data of special quality and the necessary inspections are performed. Within this scope;

- ✓ With respect to the security and the processing principles of the personal data of special quality, the **“Special Quality Personal Data Protection and Processing Policy”** was put into practice.
- ✓ The employees who are involved in the courses of processing the special quality personal data are given regular trainings on the Law and the relevant regulations and the special quality personal data security, the confidentiality contracts are signed, the authorization scope and duration of the users who are authorized to access to the data are clearly determined, the authorization controls are made, the authorizations of the employees whose duty is changed or who quit the job are immediately revoked and, within this scope, the inventory allocated to the employee by the data controller is withdrawn.
- ✓ If the environments where the special quality personal data is processed, maintained and/or accessed are electronic environments, the data is stored by using cryptographic methods. The cryptographic keys are kept in secure and different environments, the transaction records of all actions taken on the data are logged securely, the security updates for the environments where the data is available are followed up, the necessary security tests are performed and the test results are recorded.
- ✓ In the event that the data is accessed via software, the user authorizations for this software are



made, the security tests of this software are regularly performed and the test results are recorded. If the data is required to be accessed remotely, at least two-stage identity authentication system is ensured.

- ✓ If the environments where the special quality personal data is processed, maintained and/or accessed are physical environments, the sufficient security measures are taken (against electricity leakage, fire, flood, theft etc.) as per the nature of the environment where the special quality personal data is available and the unauthorized entries and exits are prevented by ensuring the physical security of these environments.
- ✓ If the special quality personal data will be transferred, it is ensured that the data is transferred with the corporate e-mail address as encoded or by using the Registered Electronic Mail (REM) account if they are required to be transferred by e-mail.
- ✓ If the Special Data is required to be transferred by means of the environments such as Memory, CD, DVD, the data is encoded by the cryptographic methods and the cryptographic key is kept in a different environment.
- ✓ If the special data is transferred between the servers in different physical environments, the data transfer is made by establishing VPN between the servers or by the sFTP method. If the special data is required to be transferred in paper form, the necessary measures are taken against the risks such as that the documents are stolen, the documents are lost or the documents are seen by unauthorized persons and the documents are sent in “**classified document**” format.
- ✓ In addition to the aforementioned measures, the technical and administrative measures for ensuring the appropriate security level specified in the Personal Data Security Guide published at the website of the Personal Data Protection Board are also taken into account.

### **III. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR PREVENTING THE ACCESS TO THE PERSONAL DATA IN CONTRARY TO THE LAW**

Our Company takes the technical and administrative measures in order to prevent the disclosure of, access to and transfer of the personal data in a careless or unauthorized manner or all accesses to the personal data in contrary to the law in other means.

#### **1. Technical Measures Taken For Preventing The Access To The Personal Data In Contrary To The Law**

The main technical measures taken by our Company in order to prevent the access to the personal data in contrary to the law are listed below:

##### ***A) Ensuring the Cyber Security***

For the personal data security to be ensured, primarily the cyber security products are used, but the measures are not limited to this. The measures such as firewall and gateway are taken. The unused software and services are uninstalled from the devices.

##### ***B) Software Updates***

By means of the patch management and software updates, it is regularly controlled that the software and hardware properly function and whether the security measures taken for the systems are sufficient.

##### ***C) Access Restrictions***

Also the access to the systems including personal data is restricted. Within this scope, the employees are granted access authorization to the extent necessary for the works and duties that they are carrying out and for their authorities and responsibilities, and the access to the relevant systems are provided by the use of user name and password. While creating the mentioned user names and passwords, it is ensured that the combinations consisting of capital and small letters, numbers and symbols are preferred instead of the number or letter sequences related to the personal information which are easy to guess. Accordingly, the access authorization and control matrix is created.

#### ***D) Encryption***

In addition to the use of strong codes and passwords, the access is restricted by the methods such as restricting the number of the password-entry trials, ensuring that the passwords are changed at regular intervals, creating the administrator account and admin authority for the use only when required and promptly deleting the account or closing the entries for the employees whose relationship with the data controller is ceased.

#### ***E) Anti-Virus Software***

For the protection from the malicious software, the products such as anti-virus, anti-spam which regularly scan the information system network and identify the threats are also used and the necessary files are regularly scanned by keeping such products up-to-date. If personal data will be provided from different websites and/or mobile application channels, it is ensured that the connections are made by SSL or a more secure way.

#### ***F) Monitoring of the Personal Data Security***

- It is controlled which software and services function in the information networks,
- It is determined whether there is penetration or any action that should not occur in the information networks,
- The records of the actions of all users are regularly kept (such as log records),
- The security problems are reported as fast as possible,

and an official reporting procedure is established for the employees to notify the security gaps in the systems and services or the threats using these security gaps.

In the undesired incidents such as collapse of the information system, the malicious software, the attacks intending to make out of service, the deficient or wrong data entry, the violations distorting the confidentiality and integrity and misuse of the information system, the evidences are collected and kept in a secure manner.

#### ***G) Ensuring the Security of the Environments Including Personal Data***

If the personal data are retained in the devices or papers in the premises of the data controllers, the physical security measures are taken against the threats such as that these devices and papers are stolen or lost. The physical environments containing personal data are protected against the external risks (fire, flood etc.) by the appropriate methods and the entries into / exits from these environments are taken under control.

If the personal data are in electronic environment, the access between the network components can be restricted or the separation of the components is ensured in order to prevent the personal data security violations.

The measures at the same level are taken also for the paper environments, electronic environments and devices (laptop computer, mobile phone, flash memories) which are outside of the Company premises and which include the personal data of the Company. The personal data to be transferred by electronic mail or mail is also sent carefully and by taking the sufficient measures.

In the event that the employees access to the information system network with their personal electronic devices, the sufficient security measures also for these devices are taken.

The method of using the access control authorization and/or encoding methods is applied against the cases such as the devices including personal data are lost or stolen. Within this scope, the code key is kept in the environment to which only the authorized persons can access and the unauthorized access is prevented.

The documents in paper environment including personal data are kept in the environments which are locked and which are accessible only to the authorized persons and the unauthorized access to the mentioned documents is prevented.

#### ***H) Storage of the Personal Data in the Cloud***

The applications for the storage of the personal data in the cloud can be also applied to when necessary. In this case, it should be evaluated by the Company whether the security measures taken by the cloud storage service provider are sufficient and appropriate. Within this scope, the measures specified in the guide and recommendations of the Board are taken into account.

#### ***I) Supply, Development and Maintenance of the Information Technologies Systems***

While determining the needs related to the supply and development of the new systems or the improvement of the existing systems, the security requirements are taken into consideration by the Company.

#### ***J) Back-up of the Personal Data***

In the cases such as that the personal data is damaged, destroyed, stolen or lost for any reason, the Company ensures to proceed with the activity within the shortest period of time by using the backed up data. The backed up personal data is accessible only to the system manager and the data set back-ups are kept out of the network.

## **2. Administrative Measures Taken For Preventing The Access To The Personal Data In Contrary To The Law**

The main administrative measures taken by our Company in order to prevent the access to the personal data in contrary to the law are listed below:

- ✓ The employees are informed and trained on the technical measures to be taken for preventing the access to the personal data in contrary to the law.
- ✓ The employees are informed about that they may not disclose the personal data that they learned to others in contrary to the provisions of the Law, they may not use the personal data for any purpose other than their intended use and this obligation will continue also after their discharge and accordingly, the necessary commitments are obtained from them.
- ✓ The Personal Data Security Policies and Procedures are established, the controls are regularly made, the controls made are documented and the issues required to be developed are determined

within the scope of the policies and procedures. Also, how to manage the risks and security violations that might arise for each personal data category is clearly determined.

- ✓ Reducing the Personal Data as far as possible: The personal data should be accurate and current and should be maintained for the period stipulated in the relevant legislation or necessary for the processing purpose. However, it is evaluated whether the data which is not accurate, which is not current and which does not serve to any purpose is still needed and the personal data which is not needed, however, is deleted, destroyed or anonymized by the personal data retention and disposal policy.
- ✓ Management of the Relations with the Data Processors: When the Company purchases service from the data processors in order to meet its BT need, the action is taken by making sure that the mentioned data processors ensure the security level ensured by them in minimum about the personal data while purchasing service. Within this scope, the protective regulations related to the protection of the personal data are included into the contracts signed with the data processors.

#### **IV. RETENTION OF THE PERSONAL DATA IN SECURE ENVIRONMENTS**

Our Company takes the necessary technical and administrative measures according to the technological opportunities and the application cost in order to ensure that the personal data is retained in secure environments and to prevent the personal data from being destroyed, lost or modified for the purposes in contrary to the law.

##### **1. Technical Measures taken for the Retention of the Personal Data in Secure Environments**

The main technical measures taken by our Company for the retention of the personal data in secure environments are listed below:

- ✓ For the retention of the personal data in secure environments, the systems suitable for the technological developments are used.
- ✓ The technical security systems are established for the retention areas, the technical measures taken are periodically inspected by the inspection mechanism determined by our Company, the issues posing risk are reevaluated and the necessary technological solutions are generated.
- ✓ All necessary infrastructures are used in compliance with the law for ensuring the retention of the personal data in a secure manner.

##### **2. Administrative Measures taken for the Retention of the Personal Data in Secure Environments**

The main administrative measures taken by our Company for the retention of the personal data in secure environments are listed below:

- ✓ The employees are informed about ensuring that the personal data is retained in a secure manner.
- ✓ In the event that any service is purchased from outside due to the technical requirements about the retention of the personal data by our Company, the contracts signed with the relevant companies to which the personal data is transferred in compliance with the law include the provisions regarding that the persons to whom the personal data is transferred will take the necessary security measures for the purpose of protecting the personal data and they will ensure that these measures are complied with in their own corporations and, on this matter, the action is taken in accordance with the provisions set forth in the Policy for the “**Principles for the Protection of the Personal Data in the Relations with the Third Parties**” of the Company.

## V. TRAINING

- ✓ Our Company gives the necessary trainings to its employees on the protection of the Personal Data within the scope of the Policy and the PDP Procedures and the PDPL Regulations.
- ✓ In the trainings, the applications for the definition and protection of the Special Quality Personal Data are specifically mentioned.
- ✓ If an employee of our Company accesses to the Personal Data physically or in computer environment, our Company gives training to the relevant employee as specific to these accesses (for instance, computer program accessed).

## VI. INSPECTION

### 1. Increase and Inspection of the Awareness of the Business Departments on the Protection and Processing of the Personal Data

Our Company ensures that the necessary notifications are made to the business departments for the increase of the awareness for preventing the processing of the personal data in contrary to the law, preventing the data is accessed in contrary to the law and ensuring the maintenance of the data.

### 2. Increase and Inspection of the Awareness of the Business Partners and the Suppliers on the Protection and Processing of the Personal Data

Our Company gives the necessary information to the business partners for the increase of the awareness for preventing the processing of the personal data in contrary to the law, preventing the data is accessed in contrary to the law and ensuring the maintenance of the data.

### 3. Inspection of the Measures taken for the Protection of the Personal Data

Our Company is entitled to inspect all the time and ex officio that all employees, departments and contractors of the Company act in compliance with this Policy and the PDP Regulations without making any preliminary notification and, within this scope, carries out or causes to be carried out the routine inspections. The results of these inspections are evaluated within the scope of the internal functioning of the Company and the necessary activities are carried out for the improvement of the measures taken.

Our Company executes the system which ensures that if the personal data processed in compliance with the Article 12 of the Law is obtained by others by illegal means, this situation is notified to the relevant personal data owner and the Board within the shortest period of time.