**Arzum Elektrikli Ev Aletleri Sanayi ve Ticaret Anonim Şirketi**

PERSONAL DATA

PROTECTION AND PROCESSING POLICY

Prepared exclusively for **ARZUM**. All rights reserved. This document cannot be reproduced, distributed and used without permission.

**Table of Content**

**1. INTRODUCTION**3

2. PURPOSE AND SCOPE OF THE POLICY3

**3. EXECUTION OF THE POLICY AND THE PERSONAL DATA PROTECTION (KVK) ARRANGEMENTS**3

**4. DEFINITIONS**3

**5. ENFORCEMENT OF THE POLICY**5

**6. PRINCIPLES APPLICABLE IN THE PROCESSING OF PERSONAL DATA**5

**7. PROCESSING PERSONAL DATA AND SENSITIVE PERSONAL DATA BASED AND LIMITED TO THE PROCESSING TERMS SPECIFIED IN PERSONAL DATA PROTECTION ARRANGEMENTS** 5

**8. CLASSIFICATION OF PERSONAL DATA PROCESSED BY ARZUM**7

**9. DELETING, DESTRUCTING AND ANONYMIZATION PERSONAL DATA**10

**10. TRANSFERRING PERSONAL AND PROCESSING BY THIRD PARTIES**11

**11. RIGHTS OF THE PERSONAL DATA OWNER AND EXERCISE OF SUCH RIGHTS**12

**12. PURPOSES OF PROCESSING AND TRANSFERRING PERSONAL DATA AND PERSONS WHOM PERSONAL DATA ARE TRANSFERRED TO**14

**13. ISSUES RELATED TO THE PROTECTION OF PERSONAL DATA**15

**1. INTRODUCTION**

For **Arzum Elektrikli Ev Aletleri Sanayi ve Ticaret Anonim Şirketi,** as the data controller, the protection of the personal data of its employees and real persons which the company is in relation with is essential and the company is aware of its responsibility of ensuring the personal data security in form and term as specified in legal regulations; thereby, ARZUM turns this responsibility into a policy.

This policy defines the principles to be followed by the company while ARZUM performs its obligations in respect with protecting personal data and processing personal data in accordance with the KVK (Personal Data Protection) Regulations. In this scope, all required arrangements in order to process and protect personal data are implemented and also the necessary system to raise awareness is established by ARZUM.

ARZUM, acting in the capacity of data controller in terms of the personal data taking place within the company, declares that ARZUM will act in compliance with the policy and the procedures to be applied under this policy.

**2. PURPOSE AND SCOPE OF THE POLICY**

The purpose of this policy is to make statement on the systems which have been adopted by ARZUM in respect with the personal data processing activities and personal data protection carried out by ARZUM in accordance with the KVK Regulations and to define the principles in respect with the processes. For the processes of processing protecting personal data, the purpose of the processes and goals which are managed by this policy and the processes and other written policies within ARZUM is processing and protecting personal data in a legal manner.

This policy has been issued for persons whose personal data are processed by ARZUM automatically or non-automatically provided that the latter shall be part of any data recording system; those persons are mainly company stakeholders, company executives, company business partners, employees, employee candidates, visitors, customers, potential customers and third parties and these personal data shall be executed in scope of these aforementioned real persons.

The rights for any changes in this policy are reserved, if such changes are required by the KVK Regulations or if deemed necessary by ARZUM in scope of any changes to be made in the purposes of processing and transferring and data collection methods.

**3. EXECUTION OF THE POLICY AND THE PERSONAL DATA PROTECTION (KVK) ARRANGEMENTS**

In the course of processing and protecting personal data, the KVK Arrangements shall prevail and in case of any discrepancies between such arrangements and the provisions of the policy the KVK Arrangements shall be applicable.

The update chart is taking place in Appendix 1.

**4. DEFINITIONS**

**Personal Data:** Any information of a real person who is identified or identifiable (In the scope of this policy, the term “Personal Data” does also include “Sensitive Personal Data” to the extent that the term Personal Data is deemed appropriate).

**Sensitive Personal Data:** Any data related to race, ethnic origin, political view, philosophical belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, penal sentence and security measures as well any biometric and genetic data.

**Processing Personal Data:** Any process which may be realized on personal data such as gaining, storing, keeping, changing, rearranging, disclosing, transferring, taking over, making obtainable, classifying or preventing the use of personal data in part or in full automatically or automatically or non-automatically provided that the latter shall be part of any data recording system.

**KVKK:** The Personal Data Protection Act 6698.

**KVK Arrangements:** Any regulation, communique and respective legislation related to the Personal Data Protection Act 6698 and the protection of personal data, decisions of the personal Data Protection Council, court decisions, applicable international treaties in respect with the protection of personal data and any other legislations.

**Data Controller:** A real person or legal entity who defines the purposes and means of personal data processing and who is responsible for the establishment and management of the data recording system.

**Data Processor:** A real person or legal entity who processes data on behalf of the data controller based on the authority given by the data controller.

**Personal Data Subject:** A real person whose personal data are processed by or on behalf of ARZUM.

**Third Party:** Real persons who are not defined in a different manner within the policy and whose personal data are processed in scope of the policy.

**Data Recording System:** A recording system where personal data are structured and processed under certain criteria.

**Explicit Consent:** A consent which has been declared with freewill on a certain matter and which is based on notification.

**Anonymization:** Rendering personal data in such way that they cannot be associated in any way with any identified or identifiable real person even by matching such data with other data.

**Application Form:** An application form which includes the applications to be made by personal data subjects in order to exercise their rights which has been prepared in compliance with the Personal Data Protection Act 6698 and the Communique related to the Principles and Procedures for Applying to the Data Controller issued by the Personal Data Protection Council, in respect with application to be made the respective person (Personal Data Subject) to the Data Controller.

**Company Stakeholder:** Any real person who is the company’s stakeholder.

**The Company’s Real Person Business Partner:** Any real persons who the company is in any kind of business relation.

**The Company’s Business Partners’ Stakeholder, Executive, Employee:** All real persons including employees, stakeholders and executives of real persons and legal entities who the Company is in any kind of business relationship (such as business partner, supplier etc.).

**Company Executive:** The Company’s members of the board of directors and other authorized real persons.

**Employee Candidate:** Any real persons who have made a job application to the company by any means or who have made available their resume and other related information to the company’s review.

**Customer:** Any real person who use or have used the products and services provided by the company regardless of whether there is any contractual relationship between such person and the company or not.

**Potential Customer:** Any real persons who have requested or are interested in the use of the company’s products and services or who are evaluated under business practices and good faith as having the potential to have such interest.

**Visitor:** All real persons who visit the company’s physical sites for various purposes or visiting the company’s websites for any purpose.

**Council:** The Personal Data Protection Council.

**Policy:** The personal data processing and protection policy.

**5. ENFORCEMENT OF THE POLICY**

This policy which has been prepared by the company and has come into effect on September 15, 2020 is published in the company’s website ([www.arzum.com.tr](http://www.arzum.com.tr)) and is made available for access by respective persons who are Data Subjects.

**6. PRINCIPLES APPLICABLE IN THE PROCESSING OF PERSONAL DATA**

**6.1. Processing personal data in compliance with legal rules and good faith**

In the course of processing personal data, ARZUM acts in compliance with the law and good faith principles; takes the principles of proportionality and essentialness into consideration and; processes the personal data at such level so that it shall fall into the data processing purposes.

**6.2. Keeping personal data correctly and, if necessary, updated**

Keeping data in a correct and updated manner is essential in terms of protecting persons’ fundamental rights and freedoms, so ARZUM ensures that any processed personal data are correct and updated and takes any required measures in this respect; in this sense, if the personal data subject should request any changes in his/her personal data, ARZUM updates the respective personal data.

**6.3. Processing personal data for defined, clear and legal purposes**

ARZUM defines its lawful and legitimate personal data processing purposes in a clear and precise manner; processes personal data in connection with its business activities and products and services which the company provides and as necessary as required to do so; the purpose of processing personal data is set forth already before starting the personal data processing activities; in this line, the personal data subject is clarified in scope of the KVK Arrangements and if deemed necessary, the personal data subject’s explicit consent is obtained.

**6.4. Processing personal data in connection, limited to and measured by the processing purpose**

ARZUM processes personal data in a convenient way which allows the realization of the defined purposes and refrains from processing personal data which are not related to the achievement of the purpose or which are not needed. In this scope, personal data processing actions for meeting future needs which may arise later on are not carried out. ARZUM processes personal data only under limited states as specified in the KVK Arrangements (KVKK articles 5.2 and 6.3) or in line with the purpose which is subject to obtaining the personal data subject’s explicit consent (KVKK articles 5.1 and 6.2) and in accordance with the proportionality principle.

**6.5. Keeping personal data for a time period as stipulated in the KVK Arrangements or as long as required by the purpose of processing**

ARZUM keeps personal data only for a time period as stipulated in the KVK Arrangements or as long as required by the purpose of processing; in this scope, ARZUM firstly defines whether a time period is envisaged for keeping personal data in the KVK Arrangements and acts accordingly if a time period is stipulated; if no timer period is defined, ARZUM keeps personal data as long as required by the purpose of processing; upon expiration of the aforementioned time period or upon the removal of the causes which require processing of personal data, ARZUM deletes, destroys or anonymizes the personal data depending on the nature and purpose of use of such personal data according to the obligations in scope of the KVK Arrangements.

**7. PROCESSING PERSONAL DATA AND SENSITIVE PERSONAL DATA BASED AND LIMITED TO THE PROCESSING TERMS SPECIFIED IN PERSONAL DATA PROTECTION ARRANGEMENTS**

**7.1. Processing Personal Data**

According to the KVK Arrangements; ARZUM processes personal databased on one or several of the terms taking place in the KVKK articles 5 and 6 and; clarifies personal data subjects and also makes necessary notifications if personal data subjects should request information according to the KVKK article 10.

**7.1.1. Explicit Consent**

One of the conditions of processing personal data is the explicit consent of the data subject and in cases where the personal data subjects’ explicit consent is required upon the notification to be made in scope of the obligation of clarification, the personal data will be processed if the personal data subjects’ explicit consent is obtained. In scope of the obligation of clarification, the rights of personal data subjects shall be notified to the personal data subjects before obtaining their explicit consents.

**7.1.2. Processing Personal Data without obtaining Explicit Consent**

In cases where the processing of personal data without obtaining explicit consent is stipulated in the Arrangements (KVKK articles 5.2 and 6.3), ARZUM shall be entitled to process personal data without gaining the explicit consent of the personal data subject and in case of processing personal data by this way, the company processes the personal data within the limits specified by the KVK Arrangements. The basis of personal data processing actions may be only one of the following conditions whereas several of these conditions may be the basis for the same personal data processing action as well.

**7.1.2.1.** The personal data of the data subject shall be processed lawfully if clearly stipulated by law.

**7.1.2.2.** For the purpose of the protection of the life or bodily integrity of a personal data subject who cannot declare his/her explicit consent due to actual impracticability or whose consent is not of legal validity or of a person other than such aforementioned personal data owner, personal data may be processed by ARZUM without explicit consent.

**7.1.2.3.** Personal data of contractual parties may be processed by ARZUM without seeking the explicit consent of the personal data subjects provided that they shall be directly related to the establishment, execution, performance or termination of a contract.

**7.1.2.4.** If deemed necessary for ARZUM, in order to carry out its legal obligations in the capacity of the data controller, ARZUM may process personal data without the explicit consent of the personal data subject.

**7.1.2.5.** Any personal data which have been made public by the personal data subject may be processed by ARZUM without seeking explicit consent.

**7.1.2.6.** If the processing of personal data without explicit consent is the only possible way to establish, use or protect any right, ARZUM may process the personal data without seeking explicit consent.

**7.1.2.7.** If the processing of personal data is mandatory for ARZUM’S legitimate interests such personal data may be processed by ARZUM without seeking explicit consent provided that the fundamental rights and freedoms of the personal data subject shall not be harmed.

**7.2. Processing of Sensitive Personal Data**

ARZUM acts in accordance with the regulations stipulated in terms of processing sensitive personal data according to KVKK article 6. According to KVKK article 6; if the explicit consent of the personal data subject is not available, sensitive personal data may be processed only under following conditions provided that adequate measures specified by the Council shall be taken:

**7.2.1.** Personal data subjects’ sensitive personal data other than the personal data subject’s health and sexual life may be processed in cases where stipulated by law.

**7.2.2.** Personal data subjects’ sensitive personal data related to the personal data subject’s health and sexual life may be processed only for the purposes of the protection of public health, performance of preventive medicine, medical diagnosis, treatment and nursing services as well as the planning and management of health services and its financing by persons with confidentiality obligation or authorized institutions and organizations.

**7.2.3.** In this scope; ARUM evaluates whether its personal data processing actions fall into the scope of any of these conditions and stops any personal data actions which are not based on any of the aforementioned conditions. While processing sensitive personal data, the measures defined by the Council are taken.

**7.2.4.** Your sensitive personal data are protected in scope of an exclusively issued policy in accordance with the Council decision.

**8. CLASSIFICATION OF PERSONAL DATA PROCESSED BY ARZUM**

**8.1.** At ARZUM, the personal data shown in the classifications below are processed: in line with ARZUM’s legitimate and lawful personal data processing purposes; based on and limited to one of or several personal data processing conditions specified in KVKK article 5; by complying with the general principles specified in KVKK and all obligations specified in KVKK, mainly with the principles specified in article 4 related to the processing of personal data; being not limited to the chart below and upon notifying respective persons according to KVKK article 10. The relation between the personal data processed under these classes and data subjects who are arranged under this policy is defined in article 8.2 of this policy.

|  |  |
| --- | --- |
| **PERSONAL DATA CLASSIFICATION** | **DESCRIPTION OF THE PERSONAL DATA CLASSIFICATION** |
| **Identity Data** | Any data which: it is clear that it belongs to an identified or identifiable person; is processed in full or in part automatically or non-automatically provided that it shall be part of a data recording system; and where information of the person’s identity is available: name-surname, Turkish Republic identity number, date of birth, social security number and tax identity number. |
| **Communicative Data** | Any information which it is clear that it belongs to an identified or identifiable real person and is processed in full or in part automatically or non-automatically provided that it shall be part of a data recording system, such as: telephone number, home address, workplace address, personal e-mail address, computer number, system user name, fax number, IP number, access URL (web). |
| **Personal Data** | Any personal data which it is clear that it belongs to an identified or identifiable real person and is processed in full or in part automatically or non-automatically provided that it shall be part of a data recording system and; is processed for gaining information which shall base in order to constitute personal benefits of real persons who are in an employment relationship with ARZUM (information such as resume, education, salary and bonus, promotion/warning, employment date, job position(s), the name of the manager who the employee is reporting to, job assignments, working hours, performance, discharge certificate, annual leaves). |
| **Financial Data** | Any personal data which it is clear that it belongs to an identified or identifiable real person and is processed in full or in part automatically or non-automatically provided that it shall be part of a data recording system, of any information, document and records evidencing any financial results created according to the legal relation established between ARZUM and the personal data subject, bank information workplace credit card data (if any), employee’s costs, salary, social security data, credit card information, e-invoice information. |
| **Audiovisual Records** | Any data group including the person’s audiovisual data (photograph, camera records). |
| **Location Data** | Any personal data which it is clear that it belongs to an identified or identifiable real person and is processed in full or in part automatically or non-automatically provided that it shall be part of a data recording system; any information which identifies the location of the personal data subject during his/her use of use of ARZUM products and services or of the employees of organizations which ARZUM collaborates with while such employees use any means of ARZUM, in scope of the operations carried out by ARZUM’s business units; such as GPS location, travel data etc. |
| **Family Members and Relatives Data** | Any personal data which it is clear that it belongs to an identified or identifiable real person and is processed in full or in part automatically or non-automatically provided that it shall be part of a data recording system and; any information related to ARZUM’s products and services and any family data of the personal data subject (such as contact information of the spouse, mother, father and children) for the purpose of protecting ARZUM’s or the personal data subject’s legal and other rights, in scope of the operations carried out by ARZUM’s business units. |
| **Other Data** | Professional vehicle information, driving license class (in case of vehicle allocation), business telephone tariff usage, information of the department which the employee works at (such as retail, wholesale, chains, e-commerce), targeted sales figure, emergency state information form data, office entries-exits, psycho-technic test data, personality inventory test data, knowledge test data, personal data related to any records shot at the entry to, inside and during the stay in the physical space and respective documents , camera records. |

**8.2.** The following chart shows in details the personal data subject classes and the types of personal data processed of the persons under the respective classes.

|  |  |
| --- | --- |
| **Employees** | **Identity Data:** Name - surname, Turkish Republic identity number, date of birth, social security number;  **Communicative data:** mobile phone number, home address, personal e-mail address, computer number, system user name, IP number, access URL (web);  **Personal Data:** resume, education, salary and bonus, promotion/warning, employment date, job position(s), job assignments, working hours, performance, discharge certificate, annual leaves;  **Finance:** Bank information, employee’s costs, social security data, salary, workplace credit card data (if any);  **Audiovisual Records:** Employee’s photograph;  **Location Data:** GPS location, travel data;  **Family Members and Relatives Data:** contact details of family members and relatives, status of spouse and children;  **Other Data:** Professional vehicle information (in case of a vehicle allocation), business phone tariff usage, office entries-exits, personal data related to any records shot at the entry to, inside and during the stay in the physical space and respective documents , camera records, emergency state information form data. |
| **Sales Team** | **Identity**: Name- surname;  **Personal**: Performance information;  **Location Data:** GPS location, travel data;  **Other Data:** the sales division which the employee is part of (such as retail, wholesale, chains, e-commerce), targeted sales figures and achievement rate, previous years’ performance and comparisons, office entries-exits, personal data related to any records shot at the entry to, inside and during the stay in the physical space and respective documents , camera records, emergency state information form data. |
| **Former Employees** | **Identity:** Name – surname, Turkish Republic identity number, date of birth, social security number;  **Communication:** home address, personal e-mail address;  **Personal:** resume, education, salary and bonus, promotion/warning, employment date, job position(s), job assignments, performance, discharge certificate, annual leaves, resignation certificate;  **Finance:** Bank information, social security data, salary, workplace credit card data (if any);  **Audiovisual Records:** Employee’s photograph. |
| **Family Members of Employees** | **Identity:** name – surname. |
| **Employee Candidates** | **Identity Data:** Name – surname  **Communicative Data:** mobile phone number, e-mail address  **Personal Data:** resume  **Audiovisual Records:** Candidate’s photograph (if available in his/her resume)  **Other Data:** Psycho-technic test data, personality inventory test information, knowledge test data |
| **Real Person Dealer** | **Identity:** Name- surname, Turkish Republic identity number, tax identity number;  **Communication:** Telephone number, workplace address. |
| **Legal Entity Dealer** | **Identity:** Name- surname, Turkish Republic identity number, tax identity number;  **Communication:** Telephone number, address. |
| **Guarantors of the Dealer** | **Identity:** Name- surname, Turkish Republic identity number;  **Contact:** Telephone number, home address;  **Family Members and Relatives Data:** Name and surname of the guarantor’s (guarantors’) spouse (if the spouse’s consent is mandatory for the bailment contract). |
| **Real Person Dealer Candidate** | **Identity:** Name- surname, Turkish Republic identity number, tax identity number;  **Communication:** Telephone number, workplace address. |
| **Legal Entity Dealer Candidate** | **Identity:** Name- surname, Turkish Republic identity number, tax identity number;  **Communication:** Telephone number, address. |
| **Guarantors of the Dealer Candidate** | **Identity:** Name- surname, Turkish Republic identity number;  **Communication:** Telephone number, home address;  **Family Members and Relatives Data:** Name and surname of the guarantor’s (guarantors’) spouse (if the spouse’s consent is mandatory for the bailment contract). |
| **Real Person Authorized Service** | **Identity:** Name- surname, tax identity number;  **Communication:** Telephone number, address;  **Audiovisual Records:** photograph of the authorized service shop. |
| **Legal Entity Authorized Service** | **Identity:** Name- surname, Turkish Republic identity number, tax identity number;  **Communication:** Telephone number, address. |
| **Consumer / Customer** | **Identity:** Name - surname, date of birth, gender;  **Communication:** mobile phone number, home address, e-mail address;  **Finance:** Credit card information. |

**9. DELETING, DESTRUCTING AND ANONYMIZATION PERSONAL DATA**

**9.1.** As stipulated in the KVKK article 7, despite the processing of personal data in compliance with the respective provisions of the law, ARZUM deletes, destroys or anonymizes the personal data upon its own decision when the reasons for processing do not exist anymore or upon the request of the personal data subject. In this respect, ARZUM has developed a policy in accordance with the provisions of the KVKK and the Regulation related to the Deleting, Destroying or Anonymization Personal Data and destroys the personal data depending on the nature of the data in accordance with this policy. In this scope, the periodical destruction dates have been defined by ARZUM and with the beginning of the obligation a schedule has been created for periodical destruction of personal data at certain intervals.

**9.2. Techniques of deleting, destroying and anonymization personal data**

**9.2.1. The deleting or destroying techniques mostly used by ARZUM are as following:**

**9.2.1.1.** **Physical destruction:** Personal data may be processed non-automatically provided that they shall be part of a data recording system. While deleting/destroying such data a system which is based on physical destruction of personal data in such manner so that they shall not be used later on is applied.

**9.2.1.2.** **Safe deleting from the software:** While deleting/destroying data which are processed automatically or partly automatically and are stored in digital environments a method is applied which deletes the data from the respective software in such way which prevents data recovery.

**9.2.1.3.** **Safe deleting by an expert:** In some cases, ARZUM may agree with an expert who shall delete personal data on behalf of ARZUM. In this case, the personal data are safely deleted/destroyed by an expert in this field in such way that they cannot be recovered again.

**9.2.2. The anonymization techniques mostly used by ARZUM are as following:**

**9.2.2.1.** The personal data is rendered anonymous by removing the basic determining information of the personal data from the data set with the masking method.

**9.2.2.2.** Many data are aggregated by the consolidation method and personal data are rendered so that they cannot be associated with any person.

**9.2.2.3.** With the data derivation method, a content is created which is more general than the personal data content and the personal data is rendered so that they cannot be associated with any person.

**9.2.2.4.** With the data mixing method, the values within the personal data set are mixed and the connection between the values and persons is broken.

In accordance with article 8 of the KVKK, anonymized personal data may be processed for purposes such as research, planning and statistics. Such processing are out of scope of the KVKK and the explicit consent of the personal data subject is not required.

**10. TRANSFERRING PERSONAL AND PROCESSING BY THIRD PARTIES**

**10.1**. **Conditions of transferring personal data**

ARZUM may lawfully transfer personal data and sensitive personal of personal data subjects to third parties in line with ARZUM’s personal data processing purposes by constituting the necessary confidentiality terms and taking confidentiality measures. In the course of transferring personal data, ARZUM acts in compliance with the regulations stipulated by law. In this scope, ARZUM may transfer personal data to third parties in line with its lawful and legitimate personal data processing purposes, based on and limited to one or several personal data processing conditions stated in article 5 of the law, described as following:

* + 1. If the explicit consent of the personal data subject is available or;
    2. If a clear arrangement related to the transfer of personal data is available in the laws,
    3. If it is necessary for the protection of the life or bodily integrity of the personal data subject or any other person and if the personal data subject is incapable of giving his/her consent due to actual incapacity or if the consent of the personal data subject is not legally valid,
    4. If the transfer of personal data of contractual parties is necessary provided that it shall be directly associated with the establishment or execution of a contract,
    5. If the personal data transfer is mandatory for the execution of ARZUM’s legal obligations,
    6. If the personal data have been made public by the personal data subject,
    7. If the personal data transfer is mandatory for the establishment, exercise or protection of any rights,
    8. If the personal data transfer is mandatory for ARZUM’s legal interests, such personal data may be transferred without seeking explicit consent provided that the personal data subject’s fundamental rights and freedoms shall not be harmed.

**10.2. Conditions for transferring sensitive personal data**

The company may transfer the personal data subject’s sensitive personal data in line with its lawful and legitimate personal data processing purposes under following conditions by exercising due diligence, taking the required security measures as well as adequate measures stipulated by the KVK Council:

**10.2.1.** If the explicit consent of the personal data subject is available or

**10.2.2.** If following conditions are available, the personal data may be transferred without seeking the personal data subject’s explicit consent;

**10.2.2.1.** Sensitive personal data other than the personal data subject’s health and sexual life (data related to race, ethnic origin, political view, philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations and unions, penal sentences and security measures as well as biometric and genetic data) may be transferred in cases where stipulated by law,

**10.2.2.2.** The personal data subject’s sensitive personal data related to his/her health and sexual life may be transferred only for purposes of the protection of public health, preventive medicine, carrying out medical diagnosis, treatment and nursing and the planning and management of health services and its financing only by persons under confidentiality obligation or authorized institutions and organizations.

**10.3. Conditions for transferring personal data abroad**

ARZUM may transfer personal data and sensitive personal data of personal data subjects to third parties abroad in line with ARZUM’s personal data processing purposes by taking the necessary security measures. For such transferring, firstly the explicit consent of the respective person in scope of the legislation is required. If explicit consent cannot be obtained the personal data may be transferred by ARZUM to foreign countries which have been declared by the KVK Council as having adequate protection; if adequate protection is not available, such personal data may be transferred to other foreign countries for which the data controllers in Turkey and the respective foreign country guarantee in written an adequate protection and where the KVK Council has a permit.

**11. RIGHTS OF THE PERSONAL DATA OWNER AND EXERCISE OF SUCH RIGHTS**

**11.1.** The personal data subject’s rights are stated below

**11.1.1.** Knowing whether the personal data is processed,

**11.1.2.** If the personal data are processed, requesting information in this respect,

**11.1.3.** Knowing the purpose of processing personal data and whether they are used for such intended purpose,

**11.1.4.** Knowing the third parties inland and abroad who the personal data have been transferred to,

**11.1.5.** Requesting the correction of personal data if the personal data have been processed incomplete or incorrect and, in this scope, requesting the notification of such correction process to third parties who the personal data have been transferred to,

**11.1.6.** Requesting the erasure or destruction of personal data if the causes for processing personal data do not exist anymore even if such personal data have been processed in compliance with the KVK Arrangements and, in this scope, requesting the notification of such process to third parties who the personal data have been transferred to,

**11.1.7.** To raise objection if, upon the analysis of the processed data by exclusively automatic systems bring forward a result which is against the respective,

**11.1.8.** To request the remedy of any loss and damage if the respective person is exposed to any loss and damage due to processing the personal data in contradict with the KVK Arrangements.

**11.2.** According to article of the KVKK, ARZUM notifies the personal data subjects’ rights to the personal data subject and also guides the personal data subject on how to exercise such rights which are regulated in article 11 of the KVKK.

**11.3.** For the purpose of evaluating the rights of personal data subjects and to notify personal data subjects, ARZUM carries out the necessary channels, internal operations, administrative and technical regulations according to article 13 of the KVKK.

**11.4. Cases where personal data subjects cannot claim any rights**

As, according to article 28 of the KVKK, following cases are held out of scope of the KVKK, the personal data subject cannot claim any rights specified in article 11.1:

**11.4.1.** Processing of personal data by anonymization in form of official statistics for research, planning and statistics purposes,

**11.4.2.** Processing personal data for artistic, historical, literary or scientific purposes or in scope of freedom of expression provided that such personal data shall not violate national defense, national security, public security, public order, economic security, right to privacy or personal rights or shall not constitute any crime,

**11.4.3.** Processing personal data in scope of preventive, protective and intelligence activities which are carried out by public institutions and organizations which are assigned and authorized by law for ensuring national defense, national security, public security, public order or economic security,

**11.4.4.** Processing of personal data by judicial authorities or enforcement authorities in relation with investigations, proceedings, judgements or execution processes.

According to KVKK article 28/2: excluding the right of claiming remedy of, the personal data subject cannot claim his/her other rights stated in article 11.1 under following conditions:

**11.4.5.** If the processing of personal data is necessary for the prevention of crime or a crime investigation,

**11.4.6.** Processing of personal data which have been made public by the personal data subject himself/herself,

**11.4.7.** If the processing of personal is necessary for carrying out auditing or regulation tasks of assigned and authorized public organizations and institutions and professional institutions of public institution status based on the authority given by law as well as for disciplinary investigations and proceedings,

**11.4.8.** If the processing of personal data is necessary in respect with matters such as budget, taxation and financial matters for the protection of the State’s financial interests.

**11.5. Exercise of the rights by the personal data subject**

**11.5.1.** The personal data subject may submit any requests related to his/her rights specified in this policy to ARZUM free of charge together with any information and documents of identity through the methods stated below or other methods determined by the Council upon filling in and signing the application form. Besides, you are obliged, as the personal data subject, to attach any information and documents related to your request to your application.

As the personal data subject, you can submit your requests related to your rights and to the execution of the Law with the application form created by ARZUM and available in our website or by requesting this form in hand and submitting with your wet-ink signature or via the notary public to our address ‘’Flatofis Binası, Otakçılar Caddesi, Numara 78, Kat 1, B Blok, Numara B1B, Eyüp 34050 İstanbul / Türkiye”, or;

By submitting to the request by e-mail with the “secure electronic signature” of the applicant as defined in the Electronic Signature Law 5070 to the related address defined in [Arzum@hs02.kep.tr](mailto:Arzum@hs02.kep.tr) or to our electronic mail address [kvkk@arzum.com](mailto:kvkk@arzum.com). Upon submitting your requests, your requests will be finalized free of charge latest within 30 days depending on the nature of your request. If your request will be answered in written, no fee will be charged up to the first 10 (ten) pages whereas a handling fee of 1 TL will be charged for each page exceeding 10 (ten) pages according to the Communique related to the Principles and Practices of Applying to the Data Controller. If the answer to your request will be presented in recorded media such as CD, flash memory etc. the cost of the recording media will be charged to you.

For ensuring that your aforementioned application shall be accepted as a valid application, it is mandatory to submit following information of the respective person to the data controller according to the Communique related to the Principles and Procedures for Application;

**11.5.1.1.** Name, surname and signature, if the application is made in written,

**11.5.1.2.** Turkish Republic identity number for citizens of the Republic of Turkey, nationality information, passport number or identity number, if available, for foreign applicants,

**11.5.1.3.** Location or workplace address subject to notifications,

**11.5.1.4.** Electronic mail address, telephone and fax number, if any, which shall be subject to notifications,

**11.5.1.5.** Subject of the request.

Otherwise, the application will not be assessed as a valid application. For applications submitted without an application form, all aspects mentioned herein shall be submitted in full to ARZUM.

For applications to be made by third parties on behalf of the personal data subject, a notarized special power of attorney issued by the personal data subject to the name of the applicant shall be available.

**11.5.2.** When the personal data subject has submitted his/her request to ARZUM; ARZUM will finalize the respective request by latest thirty days depending on the nature of the request. If the transaction requested by the personal data owner requires an additional cost, a fee as determined in the tariff defined by the Council may be charged. If the request is caused by any failure of ARZUM, the charged fee will be returned to the respective person. ARZUM may request information from the respective person in order to identify whether the applicant is the personal data subject. In order to clarify the aspects taking place in the personal data subject’s application, ARZUM may address some questions related to the application to the personal data subject. ARZUM accepts the request or rejects the request by declaring the justification for doing so and sends its reply to the respective person in written or electronically. If the request taking place in the application will be accepted ARZUM will act accordingly.

**11.5.3.** Under the situations stated in article 11.4 and/or following situations, ARZUM may reject the applicant’s application by declaring the respective justification.

**11.5.3.1.** If there is a possibility that the personal data subject’s request may restrain others’ rights and freedoms,

**11.5.3.2.** The request requires non-proportional efforts,

**11.5.3.3.** The requested information is publicly available,

**11.5.3.4.** The said data has to be processed due to the nature of the received service.

**11.5.4.** The personal data subject’s right to file a complaint to the Council

In accordance with the KVKK article 14: if the personal data subject’s application is rejected, the reply to the request is found insufficient or if no reply has been given to the request within the granted time period; the personal data subject may file a complaint to the Council within thirty days after having known ARZUM’s reply and in all cases, within sixty days as of the application date.

**12. PURPOSES OF PROCESSING AND TRANSFERRING PERSONAL DATA AND PERSONS WHOM PERSONAL DATA ARE TRANSFERRED TO**

**12.1. Purposes of processing and transferring personal data**

Personal data are processed lawfully and in compliance with the purpose of such law, being limited to the company’s following purposes and in scope of the personal data processing conditions specified in articles 5 and 6 of the law:

**12.1.1.** -Planning and executing the human resources policies in the best manner,

-Planning, executing and managing business partnerships and strategies in a correct manner,

-Ensuring the legal, commercial and physical security of itself and its business partners,

-Ensuring corporate function, planning and execution of management and communication activities,

-Enabling personal data subjects to benefit from products and services in the best possible way and making suggestions by tailoring such products and services according to their demands, needs and requests,

-Ensuring data security at highest level,

-Creating databases,

-Developing the services presented in the Internet and removal of the failures having occurred in the website,

-Contacting personal data subjects who have relayed their requests and complaints to the company and ensuring management of such requests and complaints,

-Management of relations with business partners and suppliers,

-Execution of personnel recruitment processes,

-Planning and execution of the auditing activities in order to ensure that the company operations shall be carried out in compliance with the respective legislation,

-Supporting the process of planning and execution of the fringe benefits and interests to be provided to the company’s executives,

-Providing support in the realization of company law and corporations law transactions,

-Execution/follow up of financial reporting and risk management transactions,

-Execution/follow up of the company’s legal affairs,

-realization of the works related to the protection of the company’s reputation,

-Giving information based on legislation to authorized organizations,

-Creation and follow up of visitor cards

If the processing activities which are carried out for the said purposes do not meet any of the conditions stipulated by law, your explicit consent will be provided in respect with the related transaction process.

**12.2. Persons who the personal data will be transferred to**

In order to ensure a full and flawless service to you and only to the extent that the personal data is appropriate to the nature of the service: personal data may be shared with our suppliers, business and solution partners, banks and other third parties who fulfill other transactions such as technical or logistics on our behalf. These third parties consist of persons who are obliged to have access to these personal data in order to ensure full and flawless services.

Apart from these, in cases where the transfer of your personal data is imperative for the purpose of the company’s fulfillment of its legal obligations or where it is stipulated by law or where a lawful administrative/legal order exists to do so, your personal data may be transferred – being limited to the respective person or organization only.

**13. ISSUES RELATED TO THE PROTECTION OF PERSONAL DATA**

According to article 12 of the law, the company takes any technical and administrative measures required in order to prevent any unlawful processing of the personal data, prevent any unlawful access to the data, ensure the keeping of the data and to ensure an appropriate security level and also executes or has executed to others the necessary audits in this scope.

**13.1. Ensuring personal data security**

**13.1.1. Technical and administrative measures taken in order to ensure lawful processing of personal data**

For the purpose of ensuring a lawful processing of personal data, the company takes technical and administrative measures depending on technologic capacity and operation costs.

**13.1.1.1. Technical measures taken in order to ensure a lawful processing of personal data**

The main technical measures taken by the company to ensure a lawful processing of personal data are stated below:

-The personal data processing operations carried out within the company are controlled by established technical systems.

-The technical measures are periodically reported to the respective person/body according to the internal audit mechanism.

-Personnel with technical skills are employed.

**13.1.1.2. Administrative measures taken in order to ensure a lawful processing of personal data**

The main administrative measures taken by the company to ensure a lawful processing of personal data are stated below:

-Employees are informed and trained on the Personal Data Protection Law and the lawful processing of personal data.

-All activities carried out by the company are analyzed in details being specific to all business units and upon such analysis the personal data processing operations are set forth being specific to the activities of all related business units.

-The personal data processing activities carried out by the company’s business units and the requirements to be fulfilled in order to ensure such activities’ compliance with personal data processing conditions stipulated by law are defined being specific to all business unit and the detailed activities carried out by each unit.

-In order to ensure legal compliance requirements which are defined per each business unit awareness is established and the execution rules are defined being specific to each related business unit whereas the administrative measures which are required to ensure the control of these issues and to ensure the continuity of the execution are realized by in-house policies and trainings.

-Any contracts and documents which administrate the legal relationship between the company and the employees are vested with annotations to ensure obligations of non-processing, nondisclosure and non-use of personal data, excluding the company’s instructions and any exemptions brought by law whereas awareness in this respect is raised among employees, audits are carried out and any obligations by law are fulfilled.

**13.1.2. Technical and administrative measures taken to prevent any unlawful access to personal data**

In order to prevent the negligent or unauthorized disclosure, access, transfer or otherwise any unlawful access to the personal data, the company takes technical and administrative measures depending on the nature of the data to be protected, technologic capacity and operation costs.

**13.1.2.1. Technical measures taken to prevent any unlawful access to personal data**

The main technical measures taken by the company to prevent any unlawful access to personal data are stated below:

-Technic measures which are appropriate to technological development are taken whereas the taken measures are updated and renewed periodically.

-Technical solutions for access and authorization are applied in accordance with legal compliance requirements which are defined per business unit.

-Access authorities are limited and authorities are reviewed periodically.

-The taken technical measures are periodically reported to the respective person/body according to the internal audit mechanism, any aspects which pose a risk are reevaluated and the necessary technical solution is created.

-Software and hardware including virus protection systems and firewalls are configured.

-Personnel with technical skills are employed.

-In order to identify the security gaps in the applications where the personal data are collected, periodical security scans are executed. The closing of such security gaps is ensured.

**13.1.2.2. Administrative measures taken to prevent any unlawful access to personal data**

The main administrative measures taken by the company to prevent any unlawful access to personal data are stated below:

-Employees are trained on the technical measures to be taken in order to prevent any unlawful access to personal data.

-In accordance with the legal compliance requirements for personal data processing, the personal data access and authorization processes per each business unit are designed and applied in the company.

-Employees are informed on the facts that they cannot unlawfully disclose the personal data which they have learned to others, cannot use them for purposes other than the processing purpose and that this obligation will remain in effect after they have resigned from their jobs and the necessary written covenants in this respect are collected from the employees.

-In contracts concluded between the company and persons who the personal data will be lawfully transferred to; provisions will be included in the contracts which ensure that persons receiving the transferred personal data will take necessary security measures to protect personal data and that such measures will be strictly followed in their own organizations.

**13.1.3. Keeping personal data in safe environments**

The company takes technical and administrative measures depending on technologic capacity and operation costs in order to keep personal data in safe environments and to prevent the unlawful destruction, loss or replacement of such personal data.

**13.1.3.1. Technical measures taken to keep personal data in safe environments**

The main technical measures taken by the company to keep personal data in safe environments are stated below:

-Systems which are appropriate to technological development are used to keep personal data in safe environments.

-Personnel with technical expertise are employed.

-Technical security systems for storage areas are established, security tests and researches are made in order to identify the security gaps in the IT systems and any issues which are an actual risk or pose a potential risk which have been identified upon the aforementioned tests and researches are removed. The technical measures having been taken are periodically reported to the respective person/body according to the internal audit mechanism.

-Back up programs are used in a lawful manner in order to ensure the safe keeping of personal data.

-Access to environments (and thus, data) where the personal data is kept is restricted and only authorized persons with permission limited to the purpose of keeping personal data are allowed to access environments where personal data are kept, access to data storage areas where the personal data are located are logged and inappropriate accesses or access attempts are instantly transmitted to the respective persons/bodies.

**13.1.3.2. Administrative measures taken to keep personal data in safe environments**

The main administrative measures taken by the company to keep personal data in safe environments are stated below:

-Employees are trained on ensuring the safe keeping of personal data.

-Legal and technical consulting services are gained in order to follow up any developments in information security, privacy and personal data protection and in order to take necessary actions.

-In cases where, due to technical requirements, a service is outsourced by the company in respect with the keeping of personal data: In contracts concluded between the company and other companies which the personal data will be lawfully transferred to; provisions will be included in the contracts which ensure that persons receiving the transferred personal data will take necessary security measures to protect personal data and that such measures will be strictly followed in their own organizations.

**13.1.4. Audits of the measures taken for personal data protection**

In accordance with article 12 of the law, the company carries out or makes carried out necessary audits. Such audit results are reported to the respective department in scope of the company’s internal function and the actions needed to improve the taken measures are carried out.

**13.1.5. Measures to be taken in case of unauthorized disclose of the personal data**

The company operates a system which enables the notification to the respective personal data subject and the KVK Council if the personal data which have been processed according to article 12 of the law will be unlawfully acquired by others. If deemed necessary by the KVK Council, this issue will be published in the KVK Council’s website or by other methods.

**13.2. Protection of the legal rights of personal data subjects**

The company protects all legal rights of personal data subjects by the execution of the policy and the law and also takes all measures required to protect such rights. Detailed information on the rights of personal data subjects is taking place in chapter six of this policy.

**13.3. Protection of sensitive personal data**

The law attributes a special importance to certain personal data due to the risk of causing suffering and/or discrimination of persons if such personal data will be unlawfully processed. These are data related to; race, ethnic origin, political view, philosophical belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, penal sentences and security measures as well as biometric and genetic data. The company pays highest sensibility to the protection of sensitive personal data which are defined as “sensitive” by law and processed lawfully. In this scope, the technical and administrative measures taken by the company to protect personal data are applied with highest care also for sensitive personal data and the necessary controls are carried out within the company in this respect.

**Appendix 1 Update Chart**

Any changes in this policy are taking place in the chart below.

|  |  |
| --- | --- |
| **UPDATE DATE** | **SCOPE OF CHANGES** |
|  |  |
|  |  |
|  |  |