

**BİRİKİM MÜHENDİSLİK VE ENDÜSTRİYEL YÜKLENİM LTD ŞTİ
(BİRİKİM ENGINEERING AND INDUSTRIAL CONTRACTING CO. LTD.)**

PERSONAL DATA PROTECTION AND PROCESSING POLICY

Protection of personal data is one of the most important priorities of our company, BİRİKİM MÜHENDİSLİK VE ENDÜSTRİYEL YÜKLENİM LTD ŞTİ (BİRİKİM ENGINEERING AND INDUSTRIAL CONTRACTING CO. LTD.) The key part of this issue is the protection and processing of the personal data of our candidate employees, company shareholders, company officials, visitors, employees, shareholders and officials of the institutions which we cooperate with, and the third parties managed by this Policy.

According to the Constitution of the Republic of Turkey, everyone has the right to demand protection of his/her personal data. Regarding the protection of personal data, which is a right guaranteed by the Constitution, the company pays due attention to protecting the personal data of the candidate employees, company shareholders, company officials, visitors, employees, shareholders and officials of the institutions it cooperates with, and the third parties that are managed by this Policy; and makes it a Company policy.

In this context, the necessary administrative and technical measures are taken by the company to protect the personal data processed within the framework of legal legislation.

The basic principles adopted by the company in the processing of personal data in this Policy are as follows;

- Processing personal data in accordance with law and good faith,
- Keeping personal data accurate and up-to-date when necessary,
- Processing personal data for specific, clear and legitimate purposes,
- Limited and restrained processing of personal data Connected, connected with the purpose for which they are processed.
- Keeping personal data for the period prescribed in the relevant legislation or for the purpose for which they are processed
- Informing and clarifying subjects of the personal data,
- Establishing the necessary system for personal data subjects to exercise their rights,
- Taking necessary measures to keep personal data,
- To act in accordance with the relevant legislation and regulations of Personal Data Protection Board in transferring personal data to third parties in accordance with the requirements of the purpose of processing personal data,
- To show the necessary sensitivity to the processing and protection of sensitive personal data.

ARTICLE 1: PURPOSE OF THE POLICY

The main purpose of the policy is the personal data processing activity carried out by the company in accordance with the law and to ensure transparency and trust by informing the people whose data are processed by our company within this scope; particularly our customers, employees, candidate employees, company shareholders, company officials, visitors, employees, shareholders and officials of the companies which we cooperate with and third persons.

ARTICLE 2: CONTENT AND DEFINITIONS

This Policy; relates to all personal data of our employees, candidate employees, company shareholders, company officials, visitors, employees, shareholders and officials of the institutions that we cooperate with and the third parties which are processed by non-automated means provided that they are part of any data recording system.

The scope of the application of this Policy regarding the groups of personal data subjects in the categories mentioned above may constitute the entire Policy; or only a part of it.

The definitions of the concepts included in this policy text are as follows:

| | |
|--|--|
| Recipient group: | The category of natural or legal persons to whom personal data is transferred by the data controller. |
| Explicit consent: | Consent on a specified issue, based on information and declared by free will. |
| Anonymization: | Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data. |
| Employee: | Company staff |
| Electronic environment: | Environments where personal data can be created, read, changed and written via electronic devices |
| Non-electronic environment: | All written, printed, visual, etc. environments other than electronic environments |
| Service provider: | Natural or legal person providing services within the framework of a specific contract with the institution |
| Related person: | Natural person whose personal data is processed |
| Related user: | Persons who process personal data in accordance with the authority and instruction received from the data controller or within the organization of the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data. |
| Destruction: | Erasure, destruction or anonymization of personal data |
| Law: | Law No. 6698 on Protection of Personal Data |
| Registry medium: | Any medium that is fully or partially automated or containing personal data processed by non-automated means provided that it is a part of any data recording system. |
| Personal data: | Any kind of information about an identified or identifiable natural person |
| Personal data processing inventory: | The inventory detailed by describing the personal data processing activities performed by the data controllers depending on their business processes; the purposes and legal reason for processing personal data, data category, the maximum retention period required for the purpose of processing personal data and formed by associating with the data recipient group and data subject person group to which the data is transferred, the personal data prescribed to be transferred abroad and the measures taken regarding security |
| Processing of personal data: | All kinds of operations carried out on the personal data such as the collection, recording, storage, retention, alteration, re-organization, disclosure, transfer, takeover, making retrievable, classification or preventing the use thereof personal data, fully or partially through automatic means or through non-automatic means only for the process which is a part of any data registry system |
| Board: | Personal Data Protection Board |
| Sensitive personal data: | Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be sensitive data. |

| | |
|--|--|
| Periodical destruction: | Erasure, destruction or anonymization process that will be carried out ex officio at regular intervals and specified in the policy of retention and destruction of personal data in the event that all the processing conditions of the personal data included in the law disappear. |
| Policy: | Personal Data Retention and Destruction Policy |
| Company: | BİRİKİM MÜHENDİSLİK VE ENDÜSTRİYEL YÜKLENİM LTD ŞTİ |
| Data processor: | Natural or legal person who processes personal data on behalf of the data controller based on the authority given by the data controller. |
| Data registry system: | The recording system in which personal data is configured and processed according to certain criteria. |
| Data controller: | Natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data registry system. |
| Data controllers registry information system: | The information system that can be accessed over the internet, created and managed by the Presidency and used by the data controllers in making application to the Registry and other transactions related with the Registry. |
| VERBİS: | Data Controllers Registry Information System |
| Regulation: | Regulation on the Erasure, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28 October 2017 |

ARTICLE 3: APPLICATION OF POLICY AND RELATED LEGISLATION

The relevant legal regulations in force regarding the processing and protection of personal data will primarily find a field of application. If there is a discrepancy between the current legislation and the Policy, our Company accepts that the current legislation will find a field of application.

The policy was created by concretizing the rules laid down by the relevant legislation within the scope of the practices of the Company.

ARTICLE 4: EFFECTIVENESS OF POLICY

This Policy issued by our company comes into effect on the day it is published on our website. If there is any amendment or change in the policy, the effective date will be updated.

The policy is published on our Company's website and made available to the related persons upon the request of personal data subjects.

ARTICLE: 5 ISSUES ON PERSONAL DATA PROTECTION

In accordance with Article 12 of the Law on the Protection of Personal Data, our company takes all necessary administrative, technical and legal measures to prevent the illegal processing of the personal data that it processes, to prevent illegal access to the data and to ensure the protection of the data and it carries out all necessary audits in this context.

ARTICLE 6: PROVIDING THE SECURITY OF PERSONAL DATA

6.1 Technical and Administrative Measures Taken to Ensure the Legal Processing of Personal Data

Our company takes technical and administrative measures according to the technological facilities and implementation cost to ensure that the legal processing of personal data.

6.1.1 Technical Measures Taken to Ensure the Legal Processing of Personal Data

The main technical measures taken by our company to ensure the legal processing of personal data are listed below:

- a. Personal data processing activities carried out within our company are controlled by the established technical systems.
- b. The technical measures taken are periodically reported to the related person, as required by the internal audit mechanism.
- c. Personnel with technical knowledge are employed.

6.1.2 Administrative Measures Taken to Ensure the Legal Processing of Personal Data

The main administrative measures taken by our company to ensure the legal processing of personal data are listed below:

- a. Employees are informed and trained on the protection of personal data law and the legal processing of personal data.
- b. All the activities carried out by our company are analyzed in detail specific to all business units, and as a result of this analysis, personal data processing activities are set out in terms of commercial activities carried out by the relevant business units.
- c. Personal data processing activities carried out by the business units of our company; the requirements to be fulfilled to ensure that these activities comply with the personal data processing requirements as per Law No. 6698 are determined according to each business unit and the specific activity it carries out.
- d. The contracts and documents governing the legal relationship between our company and the employees, except for the instructions of the Company and exceptions brought by law, are provided with the records that bring the obligation not to process, disclose or use personal data and in this regard, the awareness of the employees are raised and inspections are carried out.

6.2 Technical and Administrative Measures Taken to Prevent Illegal Access to Personal Data

Our company takes technical and administrative measures according to the nature of the data to be protected, technological facilities and application cost in order to prevent imprudent or unauthorized disclosure, access, transfer or any other form of illegal access of personal data.

6.2.1 Technical Measures Taken to Prevent Illegal Access to Personal Data

The main technical measures taken by our company to prevent illegal access to personal data are listed below:

- a- It carries out the necessary internal audits within the scope of the installed systems
- b- It carries out the information technology risk assessment and business impact analysis processes within the scope of installed systems.
- c- It ensures the provision of technical infrastructure and the creation of relevant matrices to prevent or prevent data leakage outside the company.
- d- It provides the control of system weaknesses by taking penetration test services regularly and when necessary.
- e- It ensures that the access of employees working in information technology units to personal data is kept under control
- f- The destruction of personal data is provided irrevocably and without leaving an audit trail.
- g- In accordance with Article 12 of the Law, all kinds of digital media where personal data are stored, are protected by encrypted or cryptographic methods in order to meet information security requirements.
- h- Training and awareness studies on data security are conducted for employees at certain intervals.
- i- The employees who changed position or resigned are deauthorized in this regard.
- j- Firewalls are used.

6.2.2 Administrative Measures Taken to Prevent Illegal Access to Personal Data

The main administrative measures taken by our company to prevent illegal access to personal data are listed below:

- a- The access to the stored personal data within the company is limited to the personnel who are required to access by job description. In limiting the access, whether the data is sensitive or not and the importance of data are also considered.
- b- In case the personal data processed are illegally obtained by others, it reports this situation to the concerned and the Board as soon as possible
- c- Regarding the sharing of personal data, it concludes a framework contract on the protection of personal data and data security with the persons whom the personal data is shared with, or it provides data security by the provisions included in the existing contract. (?)
- d- It employs well informed and experienced staff on the processing of personal data and provides necessary training to its personnel within the scope of personal data protection legislation and data security.
- e- It performs the necessary audits and gets them performed with the purpose ensuring the implementation of the provisions of the Law before its legal personality. It eliminates the confidentiality and security weaknesses that arise as a result of inspections.
- f- Personal data security problems are reported quickly.
- g- Physical environments containing personal data are protected against external risks (fire, flood etc.).
- h- Extra security measures are taken for personal data transmitted via paper and related documents are sent in the form of confidential documents.
- i- Personal data are backed up and the security of the backed-up personal data is ensured, as well.
- j- Internal periodical and / or random audits are performed and conducted.
- k- Protocols and procedures for sensitive personal data security are determined and implemented.
- l- If sensitive personal data will be sent by e-mail, it must be sent in encrypted form and using KEP or corporate mail account.
- m- Secure encryption / cryptographic keys are used for sensitive personal data and managed by different units.
- n- Penetration test is applied.
- o- Sensitive personal data which are transferred on the portable memory, CD and DVD media are transferred by encrypting.
- p- Data processing service providers are periodically audited on data security.
Awareness of data processing service providers on data security is provided.

6.3 Storing Personal Data in Secure Environments

Our company takes the necessary technical and administrative measures according to technological facilities and application cost, in order to ensure that personal data are stored in secure environments and prevent them to be destroyed, lost or altered for illegal purposes.

6.3.1 Technical Measures Taken to Store Personal Data in Secure Environments

The main technical measures taken by our company to store personal data in secure environments are listed below:

- a. Systems suitable for technological developments are used to store personal data in secure environments.
- b. Technical expert personnel are employed.
- c. Technical security systems are established for storage areas, the technical measures taken are periodically reported to the related person in accordance with the internal audit mechanism, and the necessary technological solutions are produced by reassessing the risky issues.
- d. Back-up programs are legally used to ensure that personal data are stored securely.

6.3.2 Administrative Measures Taken to Store Personal Data in Secure Environments

The main administrative measures taken by our company to store personal data in secure environments are listed below:

- a. Employees are trained to ensure that personal data are stored securely.
- b. In the event that an external service is received by our company due to technical requirements for the storage of personal data, the provisions regarding that the people whose personal data is transferred will take the necessary security measures for the protection of personal data and ensure that these measures will be followed in their organizations, are included in the contracts concluded with the relevant companies in which personal data are transferred in accordance with the law;

6.4 Auditing the Measures Taken for the Protection of Personal Data

Our company performs or has the necessary audits performed within its own organization in accordance with Article 12 of the Law on the Protection of Personal Data. These audit results are reported to the relevant unit within the scope of the internal operation of the company and necessary activities are carried out to improve the measures taken.

6.5 Measures to be Taken in the Case of Unauthorized Disclosure of Personal Data

In the event that the personal data processed in accordance with Article 12 of the Law on the Protection of Personal Data are illegally obtained by others, our company will ensure that this will be reported to the relevant personal data subject and the Personal Data Protection Board as soon as possible.

If deemed necessary by the Personal Data Protection Board, this may be announced on the website of Personal Data Protection Board or by any other method.

ARTICLE: 7 OBSERVING THE RIGHTS OF THE DATA SUBJECT; CREATING CHANNELS TO TRANSFER THESE RIGHTS TO OUR COMPANY AND EVALUATION OF THE REQUESTS OF DATA SUBJECTS

Our company carries out the necessary channels, internal mechanism, administrative and technical arrangements in accordance with Article 13 of the Law on the Protection of Personal Data in order to evaluate the rights of personal data subjects and to provide necessary information to personal data subjects.

In case the personal data subjects submit their requests regarding their rights listed below to our Company in writing, according to the nature of the request, our Company concludes the request free of charge as soon as possible and within thirty days at the latest. However, in case the transaction requires a separate cost, the fee determined by the Personal Data Protection Board will be charged by our Company. Personal data subjects have the following rights;

- a. To learn whether personal data is processed or not,
- b. If the personal data is processed, to request information about it,
- c. To learn the purpose of processing personal data and whether these are used in accordance with their purpose or not,
- d. To know the third parties to whom personal data is transferred inside the country or abroad,
- e. To request the correction of personal data in case of missing or incorrect processing and to request notification of the transaction performed within this scope to third parties to whom personal data is transferred,
- f. In case the reasons requiring the processing of personal data disappear, despite being processed in accordance with the provisions of the Law on the Protection of Personal Data and other relevant laws, to request the erasure or destruction of personal data and to request notification of the transaction performed within this scope to third parties to whom personal data is transferred,
- g. To object the emergence of a result against the person himself/herself by analyzing the processed data exclusively through automated Systems,
- h. To request the recovery of the loss in case the personal data is damaged due to illegal processing.

More detailed information on the rights of data subjects is included in this Policy.

ARTICLE: 8 PROTECTION OF SENSITIVE PERSONAL DATA

As per the Law on the Protection of Personal Data, special importance is attributed to the personal data due to the risk of causing victimization or discrimination if processed illegally.

These data include; the data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data.

Our company treats with utmost care in the protection of personal data of special quality, which is determined as “sensitive” by the Law on the Protection of Personal Data and processed in accordance with the law. In this context, the technical and administrative measures taken by our Company for the protection of personal data are carefully implemented in terms of sensitive personal data and necessary audits are performed within the company.

Detailed information regarding the processing of sensitive personal data is included in this Policy.

ARTICLE: 9 INCREASING AND CONTROLLING THE AWARENESS OF BUSINESS UNITS ON PERSONAL DATA PROTECTION AND PROCESSING

Our company provides necessary trainings for business units in order to prevent illegal processing of personal data and illegal access to data, and to raise awareness to ensure retention of data.

Necessary systems are established in order to raise awareness of the current employees of the business units of the company and employees who are newly incorporated in the business unit, regarding the protection of their personal data, and if necessary, professional people are employed in this respect.

ARTICLE 10: INCREASING AND CONTROLLING THE AWARENESS OF BUSINESS PARTNERS AND SUPPLIERS ON PERSONAL DATA PROTECTION AND PROCESSING

Our company provides trainings and seminars for business partners in order to prevent illegal processing of personal data, to prevent illegal access to data, and to raise awareness to ensure retention of data.

The trainings carried out for the business partners of the company are periodically repeated, necessary systems are established in order to raise awareness of the current employees of the business units of the business partners and employees who are newly incorporated in the business unit, regarding the protection of their personal data, and if necessary, professional people are employed in this respect.

The training results carried out to raise awareness of the business partners of the company regarding the protection and processing of personal data are reported to the holding. In this regard, our company evaluates the participation in the relevant trainings, seminars and information sessions and performs the necessary audits or have these audits performed. Our company updates and renews its trainings in parallel with the update of the relevant legislation.

ARTICLE 11: ISSUES ON PERSONAL DATA PROCESSING

In accordance with article 20 of the Constitution and article 4 of the Law on the Protection of Personal Data, regarding the processing of personal data, our company carries out purpose-bound, limited and restrained personal data processing activities; by pursuing specific, clear and legitimate purposes; correct and up to date when necessary; in accordance with law and good faith. Our company maintains personal data as long as required by law or as required by the purpose of processing personal data.

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

Our company clarifies the personal data subjects in accordance with the article 20 of the Constitution and the article 10 of the Law on the Protection of Personal Data and provides the necessary information in case the personal data subjects request information.

Our company acts in accordance with the regulations stipulated for the processing of the sensitive personal data in accordance with Article 6 of the Law on the Protection of Personal Data.

Our company acts in accordance with the regulations stipulated in the law and laid down by the Personal Data Protection Board regarding the transfer of personal data, in accordance with Articles 8 and 9 of the Law on the Protection of Personal Data.

ARTICLE 12: PROCESSING OF PERSONAL DATA ACCORDING TO THE PRINCIPLES PROVIDED IN THE LEGISLATION

12.1 Processing Legally and in Good Faith

Our company; acts in accordance with the general rule of trust and good faith and as per the principles brought by legal regulations regarding the processing of personal data. In this context, our Company takes into consideration the proportionality requirements in the processing of personal data and does not use personal data beyond the purpose.

12.2 Keeping Personal Data Accurate and Up-to-date When Required

Our company; ensures that the personal data it processes are accurate and up-to-date, taking into account the fundamental rights of the personal data subjects and their legitimate interests. In this direction, it takes the necessary measures.

12.3 Processing for Specific, Explicit and Legitimate Purposes

Our company clearly and accurately determines the legitimate and lawful purpose of processing personal data. Our company processes the personal data in association with the service that it provides and as much as it is necessary for them.

12.4 Being Connected, Limited, and Restrained for the Purpose They Are Processed

Our company processes the personal data in a way that enables the determined objectives to be achieved and avoids the processing of personal data that are not related with the realization of the purpose or that are not needed. For example, no personal data processing activity is carried out to meet the needs that may arise later.

12.5 Data Retention Period Stipulated in the Relevant Legislation or Required for the Purpose of Processing

Our company keeps personal data only for the time specified by the relevant legislation or required for the purpose of processing. In this context, our Company firstly determines whether a period is stipulated for the storage of personal data in the relevant legislation, if a period of time has been determined, it acts in accordance with this period, and if it has not been determined, it stores the personal data for the period required for the purpose of processing. In the event that this period ends or the reasons that require the processing of the period disappear, the personal data are erased, destroyed or anonymized by our Company. Personal data are not stored by our Company with the possibility of future use. Detailed information on this subject is included in this Policy.

ARTICLE 13: PROCESSING THE PERSONAL DATA BASED ON AND LIMITED TO ONE OR FEW CONDITIONS OF PERSONAL DATA PROCESSING SPECIFIED IN ARTICLE 5 OF THE LAW ON THE PROTECTION OF PERSONAL DATA.

Protection of personal data is a constitutional right. Fundamental rights and freedoms can only be restricted by law, regardless of their essence, only for the reasons stated in the relevant articles of the Constitution. Pursuant to the third paragraph of Article 20 of the Constitution, personal data can only be processed in cases stipulated by law or with the explicit consent of the person. In this direction and in accordance with the Constitution; our company processes personal data only in cases

stipulated by law or with the explicit consent of the person. Detailed information on this subject is included in this Policy.

ARTICLE 14: CLARIFYING AND INFORMING THE PERSONAL DATA SUBJECT

Our company clarifies personal data subjects during the acquisition of personal data in accordance with Article 10 of the Law on the Protection of Personal Data. In this context, it clarifies the identity of the Holding and its representative, if any, the purpose of processing personal data, 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 personal data subject. Detailed information on this subject is included in this Policy.

It is laid down in the Article 20 of the Constitution that everyone has the right to be informed about his/her personal data. Accordingly, in the article 11 of the Law on the Protection of Personal Data, "requesting information" is also considered among the rights of the personal data subject. In this context, our company provides the necessary information in case the personal data subject requests information in accordance with the article 20 of the Constitution and the article 11 of the Law on the Protection of Personal Data. Detailed information on this subject is included in this Policy.

ARTICLE 15: PROCESSING SENSITIVE PERSONAL DATA

In the processing of personal data determined by our company as "sensitive" with the Law on the Protection of Personal Data, the regulations stipulated in the Law on the Protection of Personal Data are strictly followed.

In the article 6 of the Law on the Protection of Personal Data, certain personal data that are at risk of causing victimization or discrimination when processed illegally are defined as "sensitive". These data include; the data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data.

In accordance with the Law on the Protection of Personal Data; sensitive personal data are processed by our Company in the following cases, provided that adequate measures determined by the Personal Data Protection Board are taken:

- a. If the personal data subject has explicit consent or
 - b. If the personal data subject does not have explicit consent;
- 1) Sensitive personal data, other than the health and sexual life of the personal data subject, when required by law,
 - 2) Personal data related to the health and sexual life of the sensitive personal data subject, are processed by the individuals or authorized institutions and organizations that have confidentiality obligation with the purpose of the protecting public health, carrying out preventive medicine, medical diagnosis, treatment and care services and planning and managing health care services and financing.

ARTICLE 16: TRANSFER OF PERSONAL DATA

Our company can transfer the personal data of the personal data of the personal data subject and the sensitive personal data to third parties (third party companies, business partners, third party natural persons) by taking the necessary security measures for the purposes of personal data processing in accordance with the law. In this direction, our company acts in accordance with the regulations stipulated in article 8 of the Law on the Protection of Personal Data. Detailed information on this subject is included in this Policy.

16.1 Transfer of Personal Data

Our company may transfer personal data to third parties based on or limited to one or few conditions of personal data processing specified in article 5 of the Law, for the purposes of legitimate and legal personal data processing:

- a. If the personal data subject has explicit consent;

- b. If there is a clear regulation in the laws regarding the transfer of personal data,
- c. If it is an obligatory for the protection of the life or body integrity of the personal data subject or someone else, and the personal data subject is unable to explain his/her consent due to the actual impossibility or his/her consent is not legally valid;
- d. If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or execution of a contract,
- e. If personal data transfer is mandatory for our company to fulfill its legal obligation,
- f. If the personal data are publicized by the personal data subject,
- g. If personal data transfer is mandatory for the establishment, use or protection of a right,
- h. If personal data transfer is mandatory for the legitimate interests of our Company, provided that it does not damage the fundamental rights and freedoms of the personal data subject.

16.2 Transfer of Sensitive Personal Data

Our company may transfer the sensitive personal data of the data subject to third parties, for the purposes of legitimate and legal personal data processing, by exercising due care, taking the necessary security measures and taking the necessary precautions stipulated by the Personal Data Protection Board, in the following cases.

- a. If the personal data subject has explicit consent or
 - b. If the personal data subject does not have explicit consent;
- 1) Sensitive personal data other than the health and sex life of the personal data subject (race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data), when required by law,
 - 2) Personal data related to the health and sexual life of the sensitive personal data subject, are processed by the individuals or authorized institutions and organizations that have confidentiality obligation with the purpose of the protecting public health, carrying out preventive medicine, medical diagnosis, treatment and care services and planning and managing health care services and financing.

ARTICLE 17: INTERNATIONAL TRANSFER OF PERSONAL DATA

Our company can transfer the personal data of the personal data of the personal data subject and the sensitive personal data to third parties by taking the necessary security measures for the purposes of personal data processing in accordance with the law. Personal data is transferred by our company to foreign countries ("Foreign Countries with Adequate Protection") declared by the Personal Data Protection Board as having adequate protection or in the absence of adequate protection, to foreign countries ("Foreign Country with the Data Controller Committing Adequate Protection") where data controllers in the relevant foreign country commit adequate protection in written and the permission is given by the Personal Data Protection Board. In this direction, our company acts in accordance with the regulations stipulated in article 9 of the Law on the Protection of Personal Data. Detailed information on this subject is included in this Policy.

17.1 International Transfer of Personal Data

If the personal data subject has explicit consent or if the personal data subject does not have explicit consent, our company can transfer personal data to Foreign Countries with Adequate Protection or Foreign Country with the Data Controller Committing Adequate Protection, for the purposes of legitimate and legal personal data processing, in the presence of one of the following cases:

If there is a clear regulation in the laws regarding the transfer of personal data,

- a. If it is an obligatory for the protection of the life or body integrity of the personal data subject or someone else, and the personal data subject is unable to explain his/her consent due to the actual impossibility or his/her consent is not legally valid;

- b. If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or execution of a contract,
- c. If personal data transfer is mandatory for our company to fulfill its legal obligation,
- d. If the personal data are publicized by the personal data subject,
- e. If personal data transfer is mandatory for the establishment, use or protection of a right,
- f. If personal data transfer is mandatory for the legitimate interests of our Company, provided that it does not damage the fundamental rights and freedoms of the personal data subject.

17.2 International Transfer of Sensitive Personal Data

Our company may transfer the sensitive personal data of the data subject to Foreign Countries with Adequate Protection or with the Data Controller Committing Adequate Protection, for the purposes of legitimate and legal personal data processing, by exercising due care, taking the necessary security measures and taking the necessary precautions stipulated by the Personal Data Protection Board, in the following cases.

- a. If the personal data subject has explicit consent or
 - b. If the personal data subject does not have explicit consent;
- 1) Sensitive personal data other than the health and sex life of the personal data subject (race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data), when required by law,
 - 2) Within the scope of personal data related to the health and sexual life of the sensitive personal data subject, processed by the individuals or authorized institutions and organizations that have confidentiality obligation with the purpose of the protecting public health, carrying out preventive medicine, medical diagnosis, treatment and care services and planning and managing health care services and financing.

ARTICLE 18: CATEGORIZATION, PROCESSING PURPOSES AND STORAGE PERIODS OF PERSONAL DATA PROCESSED BY OUR COMPANY

In accordance with Article 10 of the Law on the Protection of Personal Data, our company reports to the personal data subject; the personal data subject groups whose personal data are processed, the purposes of processing the personal data of the personal data subject and the retention periods of the personal data.

ARTICLE 19: CATEGORIZATION OF PERSONAL DATA

In accordance with Article 10 of the Law on the Protection of Personal Data, the relevant people are informed before our Company, for the purposes of legitimate and legal personal data processing, based on and limited to one or few conditions of the personal data processing specified in the article 5 of the Law on the Protection of Personal Data, the personal data in the categories listed below are processed, limited to periods covered by this Policy, complying with the general principles set out in the Law on the Protection of Personal Data and all obligations set out in the Law on the Protection of Personal Data, especially the principles set out in Article 4 regarding the processing of personal data. It is also specified in this Policy that the personal data processed in these categories are related to which data subjects regulated under this Policy.

IDENTITY INFORMATION; All kinds of information contained in documents such as Driver's License, Identity Card, Place of Residence, Passport, Attorney Identity, Marriage Certificate which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

CONTACT INFORMATION; information such as phone number, address and e-mail, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

CUSTOMER INFORMATION; information obtained and produced about the related person as a result of our commercial activities and the operations carried out by our business units in this context, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

PHYSICAL SPACE SAFETY INFORMATION; personal data relating to the records and documents received during the stay in the physical space upon entry to the physical space, which clearly belongs to an identifiable and a natural person and is a part of the data registry system;

PROCESS SAFETY INFORMATION; your personal data processed to ensure our technical, administrative, legal and commercial security while conducting our commercial activities, which clearly belongs to an identifiable and a natural person and is a part of the data registry system;

RISK MANAGEMENT INFORMATION; the data that can be used and processed in accordance with the generally accepted legal, commercial practice and good faith in commercial, technical and administrative areas so that we can manage in this respect, which clearly belong to an identifiable and a natural person and are included in the data risks recording system;

FINANCIAL INFORMATION: Personal data processed with respect to the information, documents and records stating all kinds of financial results created according to the type of legal relationship established by our company with the personal data subject, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

PERSONAL INFORMATION; All kinds of personal data processed to obtain information that will constitute the basis for the personal rights of our employees or natural persons who have a business relationship with our Company, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

CANDIDATE EMPLOYEE INFORMATION; personal data processed with respect to the individuals who applied to be an employee of our company or evaluated as an candidate employee in line with human resources needs of our company as per common rules and good faith or to the individuals who have a business relationship with our Company, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

EMPLOYEE OPERATION INFORMATION; personal data processed with respect to all kinds of work operation performed by our employees or natural persons who are in a business relationship with our company, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

WORKING PERFORMANCE AND CAREER DEVELOPMENT INFORMATION; data processed to measure the performance of our employees or natural persons who have a business relationship with our Company and to plan and execute career developments within the scope human resources policy of our company, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

FRINGE BENEFITS AND INTERESTS INFORMATION; your personal data processed for the planning of the fringe benefits and interests that we offer and will offer to employees or other natural persons who are in a business relationship with our Company, and to determine the objective criteria related to entitlement to these benefits and interests and to follow up the entitlement, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

LEGAL TRANSACTION AND COMPLIANCE INFORMATION; your personal data processed within the scope of determination and follow-up of legal receivables and rights, and execution of our debts and compliance with our legal obligations and our company's policies, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

AUDIT AND INSPECTION INFORMATION; your personal data processed within the scope of legal obligations of our company and compliance with the company policies, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

SENSITIVE PERSONAL DATA; the data specified in Article 6 of Law No. 6698 which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

REQUEST / COMPLAINT MANAGEMENT INFORMATION; personal data regarding the receipt and evaluation of any requests or complaints addressed to our company, which clearly belongs to an identifiable and a natural person, is processed automatically, partially or entirely, or nonautomatically as a part of the data registry system;

ARTICLE 20: PURPOSE OF PROCESSING PERSONAL DATA

According to the categorization prepared by our company, the top objectives regarding the personal data processing are shared below:

- a. Performance of necessary work by our relevant business units and execution of related business processes in order to perform the commercial activities carried out by our company,
- b. Planning and execution of commercial and/or business strategies of our company,
- c. Performance of necessary work by our relevant business units to have relevant persons to benefit from products and services offered by our company and execution of related business processes,
- d. Planning and execution of the human resources policies and processes of our company,
- e. Ensuring the legal, technical and commercial occupational safety of our Company and the related persons who have a business relationship with our Company.

The data processing objectives within the scope of the top objectives listed above are as follows:

1. The Company may process the personal data of the related persons or third parties specified by the related person for a variety of purposes, including but not limited to:
 2. To conduct human resources processes
 3. To provide corporate communication
 4. To ensure company security
 5. To be able to perform statistical studies
 6. To be able to perform business and transactions as a result of signed contracts and protocols
 7. To ensure that legal obligations are fulfilled as required or obligated by legal regulations.
 8. To make contact with real / legal persons who have business relations with the company
 9. To prepare legal reports
 10. To manage call center processes
 11. To fulfill the burden of proof as evidence in the legal disputes that may arise in the future
 12. To perform / follow up legal affairs of the company
 13. To Manage Emergency Management Processes
 14. To Manage Information Security Processes
 15. To Manage Candidate Employee / Trainee / Student Selection And Placement Processes
 16. To Manage The Application Process Of Candidate Employees
 17. To Manage The Employee Satisfaction And Loyalty Processes
 18. To Fulfill The Liabilities Arising From Employment Contract And Legislation For Employees
 19. To Manage The Fringe Benefits And Interest Processes For Employees
 20. To Carry Out Auditing / Ethics Activities
 21. To Carry Out Training Activities
 22. To Exercise Access Rights
 23. To Perform Activities In Compliance With Legislation
 24. To Carry Out Financial And Accounting Affairs
 25. To Carry Out Loyalty Processes For Firms / Products / Services

26. To Ensure Physical Space Security
27. To Conduct Assignment Processes
28. To Carry Out Internal Audit / Investigation / Intelligence Activities
29. To Carry Out Communication Activities
30. To Execute / Control Business Activities
31. To Carry Out Occupational Health / Safety Activities
32. To Receive and Evaluate the Offers for Improving Business Processes
33. To Carry Out Activities for Ensuring Business Continuity
34. To Carry Out Logistics Activities
35. To Conduct Goods / Services Purchasing Processes
36. To Carry Out Goods / Services After Sales Support Services
37. To Conduct Goods / Services Sales Processes
38. To Conduct Goods / Services Production and Operation Processes
39. Organization And Event Management
40. To Carry Out Marketing Analysis Studies
41. To Conduct Performance Assessment Processes
42. To Conduct Advertising / Campaign / Promotion Processes
43. To Carry Out Risk Management Processes
44. To Carry Out Retention and Archive Activities
45. To Carry Out Social Responsibility and Civil Society Activities
46. To Conduct Contract Processes
47. To Carry Out Sponsorship Activities
48. To Carry Out Strategic Planning Activities
49. Requests / Complaints Tracking
50. To Ensure the Security of Movable Goods and Resources
51. To Carry Out Supply Chain Management Processes
52. To Carry Out Wage Policy
53. To Conduct Marketing Processes of Products / Services
54. To Ensure Security of Data Controller Operations
55. Foreign Personnel Work and Residence Permit Procedures
56. To Conduct Investment Processes
57. To Carry Out Talent / Career Development Activities
58. To Give Information to Authorized Persons, Institutions and Organizations
59. To Carry Out Management Activities
60. To Create and Track of Visitor Records

ARTICLE 21: RETENTION PERIOD OF PERSONAL DATA

If required by relevant laws and regulations, our company retains personal data for the period specified in these regulations.

Unless there is a period specified in the legislation regarding how long the personal data should be stored, the personal data is processed, for the processing period required by the practices of our Company and of practices of commercial life, depending on the services it offers and then erased, destroyed or anonymized. Detailed information on this subject is included in this policy.

If the purpose of processing personal data has expired; and the retention periods determined by the company and the relevant legislation have come to an end; the personal data can only be stored for the purpose of constituting evidence in possible legal disputes, or for the purpose of claiming the relevant right based on personal data or establishing a defense. Retention periods are determined based on the time-out periods for claiming the above mentioned right in the establishment of the periods herein and the examples in the requests submitted to our Company on the same subjects, despite the time-out periods have elapsed. In this case, the stored personal data cannot be accessed for any other purpose, and access is provided only when it is required to be used in the relevant legal dispute. Personal data is erased, destroyed or anonymized after the mentioned period is over.

ARTICLE 22: CATEGORIZATION ON THE SUBJECTS OF PERSONAL DATA PROCESSED BY OUR COMPANY

Although the personal data of the personal data subject categories listed below are processed by our company, the scope of the application of this Policy is limited to our customers, potential customers, candidate employees, company shareholders, company officials, visitors, employees, shareholders and officials and of the institutions we cooperate with and the third parties.

The personal data protection and processing activities of our employees will be considered under the Personal Data Protection and Processing Policy of Holding Employees.

Although the categories of the persons whose personal data are processed by our company are within the scope mentioned above, those who are outside of these categories will also be able to direct their requests to our Company under the Law on the Protection of Personal Data; and the requests of these persons will also be evaluated within the scope of this Policy.

The concepts of the customer, potential customer, visitor, candidate employee, shareholder and board member, natural persons in the institutions we cooperate with, and third parties associated with them are clarified below.

ARTICLE 23: CATEGORIES AND DESCRIPTIONS

Visitor; Natural persons who have enter the physical settlements of our company for various purposes or visit our websites.

Third Parties; Third-party natural persons associated with abovementioned persons in order to ensure the security of business transactions between the parties of our company or to provide benefits of these people or the natural persons who are not covered by this policy or the policy on protection and processing of personal data of company employees.

Candidate Employee; Natural persons who applied for a job to our company in any way or disclosed their curriculum vitae information to our company.

Company Shareholder; Natural persons who are the shareholders of our company.

Company Official; The board members of the company and other authorized natural persons.

The employees, shareholders and officials of the institutions we cooperate with; Natural persons (including shareholders and officials of these institutions, such as but not limited to business partners, offices, suppliers, etc.) in the institutions that our company has any kind of business relationships with.

ARTICLE 24: THIRD PARTIES TO WHOM PERSONAL DATA ARE TRANSFERRED BY OUR COMPANY AND PURPOSE OF TRANSFER

Our company reports to the personal data subject the groups of people to whom personal data are transferred in accordance with Article 10 of the Law on the Protection of Personal Data.

In accordance with the articles 8 and 9 of the Law on the Protection of Personal Data, personal data of our company can be transferred to the categories of people listed below:

- a. To business partners of the Company,
- b. To suppliers of the Company,
- c. To affiliates of the Company,
- d. To shareholders of the Company,
- e. To legally authorized public institutions and organizations,
- f. To legally authorized private law persons.

The scope of the above mentioned persons to whom data are transferred and purpose of data transfer are as follows;

1. Limited to ensure that the objectives of the business partnership are fulfilled,

2. Limited to ensure that the services outsourced from the supplier by our company and required to carry out the commercial activities of our company are provided to our company,
3. Limited to ensure that the commercial activities that also require the participation of the affiliates of our company are carried out,
4. Limited to the purpose of auditing and designing the commercial activities and audit activities of our company in accordance with the legal regulations,
5. Limited to the purpose requested within our legal powers, in the event that legally authorized public institutions and organizations request information and documents from our company within the framework of legal regulation,
6. Limited to the purpose requested within our legal powers, in the event that legally authorized private law persons request information and documents from our company within the framework of legal regulation.

Our company act in accordance with the issues regulated in the policy in the transfers performed.

Our company clarifies the personal data subject about the personal data it processes in accordance with Article 10 of the Law on the Protection of Personal Data.

Although the legal basis for the processing the personal data by our company differs, the general principles set out in Article 4 of the Law No. 6698 are followed in all kinds of personal data processing activities.

Explicit consents are obtained from visitors and third parties for the processing of personal data based on the explicit consent of the personal data subject.

If clearly prescribed by law, the personal data of the data subject can be legally processed.

Personal data of the data subject can be processed if it is necessary to process the personal data in order to protect the life or body integrity of the person who is unable to explain his/her consent due to actual impossibility or whose consent cannot be validated or of another person.

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

If processing is mandatory to fulfill its legal obligations as the data controller of our company, the personal data of the data subject can be processed.

If the data subject has publicized his/her personal data, the relevant personal data can be processed.

If data processing is mandatory for the establishment, use or protection of a right, the personal data of the data subject can be processed (invoice etc.).

If the data processing is mandatory for our Company's legitimate interests, the personal data of the data subject can be processed, provided that it does not harm the fundamental rights and freedoms of the personal data subject. (for the purpose of making internal calculations, etc.)

Personal data processing activities carried out by our company at the facility entrances and within the facility are performed in accordance with the Constitution, the Law on the Protection of Personal Data and other relevant legislation.

In order to ensure the security by our Company, personal data processing activities are carried out in the buildings and facilities of our Company for surveillance with security cameras and following the entries and exits of guests.

Personal data processing activities are carried out by our Company through the use of security cameras and recording the entries and exits of guests.

In this context, our Company acts in accordance with the Constitution, the Law on the Protection of Personal Data and other relevant legislation. Our company has aims such as improving the quality of the service provided, ensuring its reliability, ensuring the safety of the company, its employees and others, and protecting the interests of third parties regarding the provided service, within the scope of monitoring activity with security camera. The camera monitoring activity performed by our company is carried out in accordance with the Law on Private Security Services and related

legislation. In the execution of the camera surveillance activities for security purposes, our company follows the regulations specified in the Law on the Protection of Personal Data.

In order to ensure security in its buildings and facilities, our company conducts security camera surveillance activities for the purposes stipulated in the laws and in accordance with the personal data processing conditions specified in the Law on the Protection of Personal Data.

The announcement of the surveillance activities by our company is made in accordance with the article 10 of the Law on the Protection of Personal Data.

In addition to the clarification it makes regarding general issues, our company notifies with more than one method regarding camera surveillance activity in accordance with the current regulations in the EU. In this way, it is aimed to prevent any damage to the fundamental rights and freedoms of the personal data subject, to ensure transparency and clarification of the personal data subject.

In accordance with Article 4 of the Law on the Protection of Personal Data, our company processes personal data in a limited and restrained manner related with the purpose for which they are processed.

The purpose of continuing the video camera surveillance activity by our company is limited to the objectives listed in this Policy. Accordingly, the surveillance areas of the security cameras, their number and when to be monitored, are implemented to be adequate and limited to this purpose. The areas, where exceeding the security objectives may cause breaching the privacy of the person, are not subject to surveillance (such as toilets).

In accordance with article 12 of the Law on the Protection of Personal Data, necessary technical and administrative measures are taken by our company to ensure the security of personal data obtained as a result of camera surveillance activity.

Only a limited number of company employees have access to the records that are registered and stored in digital form. Live camera images can be watched by outsourced security services. A limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with the commitment of confidentiality.

Personal data processing activities are carried out by our company; in order to ensure security and to follow the entries and exits of guests in the company buildings and facilities for the purposes specified in this Policy.

The names and surnames of the persons who visited the company buildings as guests are acquired or the relevant personal data subjects are illuminated in this context by means of the texts that are hanged in the Company or made available to the guests in other ways. The data obtained for the purpose of monitoring entries and exits of guests is processed only for this purpose, and the relevant personal data are recorded in the data registry system in the physical environment.

Regarding the camera surveillance activity by our company; this Policy is published on the website of our company (*online policy regulation*) and a notification letter is hanged on the entrance of the areas where the surveillance is made (*in-situ clarification*).

On the websites of our company; the internet activities on the site are recorded by technical means in order to ensure that visitors of these sites conduct their visits on the sites in a manner appropriate for the purposes of their visit and show them a customized content.

Detailed explanations regarding the protection and processing of personal data with respect to these activities of our company are included in the “.....” texts of the related websites.

Although our company has been processed in accordance with the provisions of the relevant law, as stipulated in the article 138 of the Turkish Penal Code and the article 7 of the Law on the Protection of Personal Data, in case the reasons requiring processing disappear, then the personal data is erased, destroyed or anonymized based on the decision of our Company or upon the request of the personal data subject. Our company fulfills this relevant legal obligation by legal methods.

ARTICLE 25: ERASING, DESTROYING PERSONAL DATA

25.1 Techniques of Erasing and Destroying Personal Data

Although they have been processed in accordance with the provisions of the relevant law, if the reasons requiring the processing disappear, our company may erase or destroy the personal data based on its decision or upon the request of the personal data subject. The most commonly used erasing or destroying techniques by our company are listed below:

25.1.1 Physical Destruction

Personal data can also be processed in non-automatic ways, provided that they are a part of any data recording system. While erasing / destroying such data, the physical personal data destruction system is implemented, in a way that they cannot be used again.

25.1.2 Safely Erasure from the Software

While erasing / destroying the data processed fully or partially automatically and stored in digital media; the methods for erasing the data from the related software are used, in a way that they cannot be recovered again.

25.1.3 Safely Erasure by the Expert

In some cases, the company may employ a specialist to erase the personal data on his behalf. In this case, the personal data are safely erased / destructed by the person specialized in this respect, in a way that they cannot be recovered again.

25.1.4 Other Methods

Servers: For the personal data whose retention period on the servers has expired, the system administrator applies the erasing procedure by removing the access authorization of the related users.

Electronic environment: The personal data whose retention period in the electronic environment has expired, are made inaccessible and unusable for other employees (related users) except for the database manager.

Physical environment: The personal data whose retention period in the physical environment has expired, are made inaccessible and unusable for other employees except for the unit manager responsible for the document archive. In addition, blackening is applied by drawing / painting / erasing in an unreadable manner.

Portable media: The personal data whose retention period in the flash-based storage media have expired, are encrypted by the system administrator and stored in secure environments with encryption keys by granting access authorization to the system administrator only.

ARTICLE 26: RIGHTS OF THE DATA SUBJECT AND EXERCISING THESE RIGHTS

26.1 Rights of the Personal Data Subject

Personal data subjects have the rights specified below:

- a. To learn whether personal data is processed or not,
- b. If the personal data is processed, to request information about it,
- c. To learn the purpose of processing personal data and whether these are used in accordance with their purpose or not,
- d. To know the third parties to whom personal data is transferred inside the country or abroad,
- e. To request the correction of personal data in case of missing or incorrect processing and to request notification of the transaction performed within this scope to third parties to whom personal data is transferred,
- f. In case the reasons requiring the processing of personal data disappear, despite being processed in accordance with the provisions of the Law on the Protection of Personal Data

and other relevant laws, to request the erasure or destruction of personal data and to request notification of the transaction performed within this scope to third parties to whom personal data is transferred,

- g. To object the emergence of a result against the person himself/herself by analyzing the processed data exclusively through automated Systems,
- h. To request the recovery of the loss in case the personal data is damaged due to illegal processing.

26.2 The Cases that the Personal Data Subject Cannot Claim Rights

As the following conditions are excluded from the scope of the Law on the Protection of Personal Data, pursuant to Article 28 of the Law on the Protection of Personal Data, the personal data subjects cannot claim the rights of personal data subjects listed below in these matters:

- a. Processing personal data for research, planning, statistics etc. purposes by anonymizing with official statistics.
- b. Processing of personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, provided that they do not violate national defense, national security, public security, public order, economic security, privacy or personal rights, or constitute a crime.
- c. Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
- d. Processing of personal data by judicial authorities or enforcement authorities regarding investigations, prosecutions, trials or enforcement proceedings

As per article 28/2 of the Law on the Protection of Personal Data; personal data subjects cannot claim their other rights listed below, except for the right to request the recovery of losses, in the cases listed below:

1. The fact that personal data processing is required for the prevention of crime or for criminal investigation.
2. Processing the personal data publicized by the personal data subject.
3. The fact that personal data processing is required for the disciplinary investigation or prosecution by the assigned and authorized public institutions and organizations and the public professional organizations based on the authority given by the law.
4. Processing of personal data by judicial authorities or enforcement authorities regarding investigations, prosecutions, trials or enforcement proceedings.

26.3 Exercise of Rights by Personal Data Subject

Personal data subjects will be able to submit their requests regarding the rights listed above to our Company free of charge by the following method:

- a. By applying to address in person after filling out the form at the addresscom and signing it with wet signature
- b. By applying to address by cargo or mail after filling out the form at the addresscom and signing it with wet signature
- c. By sending the secure electronically signed form via e-mail to@.....com address filling out the form at the addresscom and signing it with your “secure electronic signature” within the scope of Electronic Signature Law No. 5070,

It is not possible the third parties to make request on behalf of personal data subjects.

In order for a person other than the personal data subject to make a request, there must be a special power of attorney issued on behalf of the person to apply by the personal data subject.

Personal data subjects, in their application to exercise their rights, will fill out the "Application Form Regarding the Applications to be Made to the Data Controller by the Related Person (Personal Data Subject) in accordance with the Personal Data Protection Law No. 6698" linked above. The method of application to be made is also explained in detail in this form.

26.4 Right of Personal Data Subject to Complain to Personal Data Protection Board

In case the application is rejected in accordance with Article 14 of the Law on the Protection of Personal Data, the given response is considered insufficient, or the application is not responded in due time; the data subject can make a complaint to the Personal Data Protection Board within thirty days as from learning the response of the company, and in any case, sixty days as from the date of application.

ARTICLE 27: RESPONSE OF THE COMPANY TO THE APPLICATIONS

27.1 Method and Duration of Response Of Our Company to Applications

In case the personal data subject submits his/her request to our Company in accordance with the procedure specified in the section above, our Company will conclude the request free of charge as soon as possible and within thirty days at the latest.

However, if the transaction requires a separate cost, the fee determined by the Personal Data Protection Board will be charged from the applicant.

27.2 Information that Our Company May Request from the Applicant Personal Data subject

Our company may request information from the related person to determine whether the applicant has personal data.

Our company may ask questions to the personal data subject regarding the application in order to clarify the issues in the application of the personal data subject.

27.3 Our Company's Right to Refuse the Application of the Personal Data Subject

Our company may reject the application of the applicant in the following situations by explaining the reason for it:

- a- Processing personal data for research, planning, statistics etc. purposes by anonymizing with official statistics.
- b- Processing of personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, provided that they do not violate national defense, national security, public security, public order, economic security, privacy or personal rights, or constitute a crime.
- c- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
- d- Processing of personal data by judicial authorities or enforcement authorities regarding investigations, prosecutions, trials or enforcement proceedings
- e- The fact that personal data processing is required for the prevention of crime or for criminal investigation.
- f- Processing the personal data publicized by the personal data subject.
- g- The fact that personal data processing is required for the disciplinary investigation or prosecution by the assigned and authorized public institutions and organizations and the public professional organizations based on the authority given by the law.
- h- The need for personal data processing to protect the economic and financial interests of the State in relation to budget, tax and financial issues.
- i- The possibility of the request of the personal data subject to hinder rights and freedoms of other peoples.
- j- Making requests requiring disproportionate effort.
- k- The fact that requested information is a public information.

ARTICLE 28: THE RELATIONSHIP BETWEEN THE PERSONAL DATA PROTECTION AND PROCESSING POLICY OF THE COMPANY AND OTHER POLICIES

The fundamental policies that are written about the protection and processing of personal data related with the principles set forth by the company in this Policy, are specified. Associating these policies with the fundamental policies carried out by the Company in other areas, the harmonization

is provided between these policies and the processes operated by the Company with different policy principles for similar purposes.

In accordance with the decision of the senior management of the Company, the "Personal Data Protection Board" has been established in order to manage this policy and other connected and related policies. The duties of this board are specified below.

- a. To prepare the fundamental policies regarding the Protection and Processing of Personal Data and submit it to the approval of the senior management in order to put it into effect.
- b. To decide on the implementation and control of the policies regarding the Protection and Processing of Personal Data and to present to the approval of the senior management to make assignments in the company within this framework and to ensure coordination.
- c. To determine the issues to be done in order to ensure compliance with the Personal Data Protection Law and related legislation and to present the things to be done to the approval of the senior management; to observe its implementation and to ensure its coordination.
- d. To raise awareness regarding the Protection and Processing of Personal Data within the Company and by the institutions that the Company cooperates with.
- e. To determine the risks that may occur in the personal data processing activities of the company and to ensure that necessary measures are taken; to present suggestions for improvement to the approval of senior management.
- f. To design and implement trainings on personal data protection and policy implementation.
- g. To conclude the applications of personal data subjects at the highest level.
- h. To coordinate the execution of information and training activities in order to ensure that personal data subjects are informed about personal data processing activities and their legal rights.
- i. To prepare the changes to the fundamental policies regarding the Protection and Processing of Personal Data and present it to the approval of the senior management in order to put it into effect.
- j. To follow the developments and regulations on the Protection of Personal Data; to advise senior management on things to be done within the Company in accordance with these developments and regulations.
- k. To coordinate the relations with the Personal Data Protection Board and Institution.
- l. To perform other duties to be given by the senior management of the company regarding the protection of personal data.

Some of the specified policies are for internal use. The principles of the internal policies of the company are reflected in publicly available policies to the extent that they are relevant, and it is aimed to inform those concerned within this framework and ensure transparency and accountability about the personal data processing activities carried out by the Company.