AKFEN TURİZM YATIRIMLARI VE İŞLETMECİLİK A.Ş.

PERSONAL DATA PROCESSING INVENTORY AND PERSONAL DATA PROTECTION POLICY

INTRODUCTION

The principal office of AKFEN TURİZM YATIRIMLARI VE İŞLETMECİLİK ANONİM ŞİRKETİ (hereinafter shall be referred to as the "**Company**") is located at Kazım Özalp Mahallesi Koza Caddesi No: 22 Çankaya Ankara.

The company is the data controller legal entity pursuant to the Law No.6698 on Protection of Personal Data (hereinafter shall be referred to as the "**KVK Law**" or the "**Law**").

Personal data subjects are natural persons whose personal data are collected, processed and transferred in accordance with the provisions of KVK Law No.6698 and other legislations that the Company is subject to. The company shows utmost sensitivity to the security of personal data. Aware of this fact, the personal data of personal data subjects are processed and stored in accordance with the Law and other legislation that constitute secondary regulations of the Law.

A. PURPOSE AND SCOPE OF THE POLICY

With this Policy, it is aimed to effectively implement the regulations to be introduced by the Company in accordance with the basic principles to be disclosed hereunder in order to ensure compliance with the KVK Law by the shareholders, officials, employees, subsidiaries, affiliates and the business partners.

In line with the basic regulations stipulated by this Policy, it is aimed to take all kinds of administrative and technical measures with respect to processing and protection of the personal data, to establish the necessary internal procedures and regulations, to provide all necessary trainings to raise awareness, and to establish appropriate and effective control mechanisms for compliance with the processes within the functioning of the Company.

This Policy regulates the basic principles to be observed throughout all such processes, the liabilities of the Company to direct the internal operation in accordance with the regulations introduced by the KVK Law, the internal procedures/regulations and the compliance activities that the Company shall carry out regarding protection of the personal data.

All employees of the Company are obliged to act in accordance with the regulations introduced by this Policy and the provisions of the KVK Law and all other applicable legislation while performing duties thereof.

In case of failure to comply with this Policy and the provisions of the applicable legislation, in addition to the penal and legal liability as stipulated by the provisions of the legislation, further sanctions which may even lead to termination of the employment contract for just cause pursuant to the legislation

that regulates the business life shall be implemented at the Company depending on the nature of the incident.

B. DEFINITIONS AND ABBREVIATIONS

EXPLICIT CONSENT	Consent on any specific subject, based on information and expressed with free will
RELATED USER	The persons processing the personal data within the data controller organization or in accordance with the authority and instruction received from the data controller, except for the person or the unit responsible for the technical aspect of storage, protection and backup of the data
DESTRUCTION	Deletion, destruction or anonymization of the personal data
LAW / KVKK	Law No. 6698 on Protection of the Personal Data
RECORD MEDIA	Any media containing personal data that is either fully or partially automated or processed via non-automatic means provided that such means represent an integral part of any data recording system
PERSONAL DATA	All kinds of information regarding any identified or identifiable natural person
PROCESSING OF THE PERSONAL DATA	All kinds of transactions performed on the data such as obtaining, recording, storing, preserving, modifying, reediting, disclosing, transferring, taking over, making available, classifying or preventing usage of the personal data through either fully or partially automatic means or via non-automatic means provided that such means represent an integral part of any data recording system
ANONYMIZING THE PERSONAL DATA	Rendering personal data non-associable to any identified or identifiable natural person under any circumstances, even by matching with other data
DELETION OF THE PERSONAL DATA	The process of rendering the Personal Data inaccessible and non-reusable by the Related Users by any means
DESTRUCTION OF THE PERSONAL DATA	The process of rendering the Personal Data inaccessible, unrecoverable and non-reusable by everyone by any means
BOARD	Personal Data Protection Board
SENSITIVE PERSONAL DATA	The data on the race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, memberships to the associations, foundations or unions, medical condition, sexual life, criminal conviction and security measures of the individuals as well as and biometric and genetic data
PERIODIC DISPOSAL	Deletion, destruction or anonymization process as specified in the personal data storage and disposal policy and shall be carried out ex officio at recurrent intervals in the event that all conditions for processing of personal data as provided in the Law are eliminated
DATA SUBJECT/ RELATED PERSON	The natural person whose personal data is processed

DATA CONTROLLER	The natural person or legal entity that sets the objectives and means of processing the personal data and is responsible for establishment and management of the data recording system
REGULATION	Regulation on Data Controllers Registry

Within the scope of the KVK Law, the Company bears the capacity of Data Controller and shall be registered with the VERBİS system. Paragraph 1 of the article 11 of the Regulation regulates that "The data controller obligations of the legal entities domiciled in Turkey under the Law are fulfilled by the competent body authorized to represent and bind the legal entity according to the provisions of the applicable legislation or by the person or persons as specified in the applicable legislation. The body authorized to represent the legal entity may assign one or more persons in relation to the obligations to be fulfilled in terms of implementation of the Law".

The persons who are entrusted with management and representation of the company by the Board of Directors in accordance with the relevant articles of the Turkish Commercial Code ("TCC") are responsible for the transactions and actions that take place within their jurisdiction within the scope of TCC, Turkish Code of Obligations and Turkish Penal Code. In addition, the top tier employee in each department shall be obliged to supervise whether the Related Users in the department act in accordance with this Policy issued pursuant to the Law and Regulation, and to report to the Board of Directors.

C. GENERAL PRINCIPLES APPLICABLE IN PROCESSING OF THE PERSONAL DATA

The Company hereby acknowledges that the company shall process the personal data covered by this Policy in accordance with Article 4 of the KVK Law in line with the principles set forth hereunder:

- Compliance with the law and good faith

The Company, with his capacity as the Data Controller and as a prudent merchant, hereby acknowledges that the company shall carry out personal data processing activities in accordance with the provisions of all applicable legislations are and will come into force, especially the Constitution and KVK Law, and in line with the rule of good faith as stipulated by Article 2 of the Turkish Civil Code.

- Accuracy and currency

The Company takes all measures as required for ensuring accuracy and currency of the personal data, to the extent as permitted by the art, in processing of the personal data.

The administrative and technical mechanisms established by the Company shall be operated in order to remedy and supervise accuracy of the inaccurate or obsolete personal data in line with the requests to be notified by the Related Person to the Company in the capacity of Data Controller and with the situations that the Company deems necessary.

- Processing for specific, explicit and legitimate purposes

The personal data is processed by the Company in accordance with the law as being limited to the services provided or to be provided in line with the requirements of the provisions set forth in the applicable legislation, and the intended purpose of processing the personal data is determined explicitly and precisely prior to processing of the data.

- Restricted and measured processing the data in connection with the intended purpose of processing

The personal data are processed by the Company in connection with and as limited to the intended purpose of the processing and to the extent as necessary for achievement of such purpose. In this context, it is essential to avoid processing of the personal data not related to the intended purpose of processing of the data and the personal data not needed in this respect.

- Processing the data as restricted to the period as stipulated by the provisions of the legislation or as required by the intended purpose of processing

The personal data are stored for the periods as stipulated by the provisions of the applicable legislation, or for the period as required for the intended purpose of data processing. The personal data are deleted, destroyed or anonymized by the Company upon expiry of the period as stipulated by the provisions of the applicable legislation or upon expiry of the period as required by the intended purpose of data processing. Necessary administrative and technical measures shall be adopted to prevent the data from being stored at the end of the mandatory period.

D. CONDITIONS FOR PROCESSING THE PERSONAL DATA

The conditions for processing of the personal data are regulated by the KVK Law, and the Company processes the personal data in accordance with such conditions as set forth hereunder.

- Conditions for Processing of the Personal Data

Except for the exceptions as listed in the KVK Law, the Company processes the personal data only by obtaining the explicit consent of the data subjects.

In case of existence of the following situations as listed in the Law, the personal data can be processed even without the explicit consent of the data subject:

- If stipulated explicitly in the laws,
- If mandatory for protection of the life or physical integrity of the person or someone else who is unable to disclose his/her consent due to the actual impossibility or whose consent is not legally valid,
- If it is necessary to process the personal data belonging to the parties of the contract, provided that such data is directly related to establishment or performance of any contract,
- If it is mandatory for the data controller to fulfill his legal obligation,

- If made public by the data subject in person,
- If processing of the data is mandatory for establishment, exercise or protection of any right, and
- If processing of the data is mandatory for the legitimate interests of the data controller, on the condition not to harm the fundamental rights and freedoms of the data subject.

➢ Conditions for Processing of the Sensitive Personal Data

The Company demonstrates special sensitivity towards processing of the sensitive personal data considered to have vital importance for the data subjects in various respects. In this context, such data cannot be processed without explicit consent of the data subjects, provided that adequate measures as identified by the Board are duly adopted. However, the sensitive personal data other than the data related to health and sexual life, can also be processed without the explicit consent of the data subject in cases as stipulated by the law.

However, the data on health and sexual life can be processed without explicit consent, provided that adequate measures are adopted and that the justifications set forth hereunder are present:

- Protection of the public health,
- Preventive medicine,
- Medical diagnosis,
- Delivery of treatment and care services, and
- Planning and management of health services and financing.

E. METHODS FOR ACQUISITION AND PROCESSING OF THE PERSONAL DATA

The company processes the personal data of natural persons on the basis of the Personal Data Processing Inventory, which must be regulated in accordance with the KVK Law and within the scope of articles 5, 7, 9 and 10 of the Regulation, and which must include the information set forth hereunder.

Although this Policy does not include an independent chapter entitled the Personal Data Processing inventory, the relevant articles shall be deemed to have the force of the "Personal Data Processing Inventory" if the information listed hereunder is included under this title and the subsequent titles.

1. The purposes of processing the personal data,
2. Data category,
3. The group or groups of recipient(s) to which the data is transferred,
4. Data subject person groups,
5. Associating the data category with the data subject person groups,
6. The personal data envisaged to be transferred to foreign countries,
7. Measures taken regarding data security, and
8. The maximum period required for the purposes for which personal data are processed

Personal Data Subject Person Groups

PERSONAL DATA SUBJECT PERSON GROUPS	DESCRIPTION
EMPLOYEE CANDIDATE / INTERNSHIP CANDIDATE	Natural persons applying for employment /internship within the company
EMPLOYEE / INTERN	Natural persons employed or doing internship within the company
REFERENCES OF THE EMPLOYEE CANDIDATE	Natural persons given as reference by natural persons applying for employment within the company
GROUP EMPLOYEES	Natural persons working in companies that are under the same control structure as the company
EMPLOYEE'S RELATIVE	Employees' relatives specified by employees within the company
EMPLOYEE'S RELATIVE TO BE REFERRED TO IN CASE OF EMERGENCIES	Employees' relatives that the employees within the company ask to be informed in case of any emergency
SUPPLIER'S/ CONSULTANT'S EMPLOYEE	Natural persons employed by the supplier /consultant organization from which the company procures goods and services
SUPPLIER'S/ CONSULTANT'S OFFICIALS	Natural persons authorized at the supplier /consultant organization from which the company procures goods and services
VISITOR	Natural persons visiting the Company premises due to any reason whatsoever
SHAREHOLDER	Natural persons holding shares of the company
COMPANY OFFICIAL / EXECUTIVE	Persons authorized to represent and bind the Company or the Company Executives
GROUP EXECUTIVE	Natural persons with management authority in companies that are under the same control structure as the company
PERSON RECEIVING GOODS OR SERVICES (CUSTOMER)	Persons receiving the company's mail and services

Data Categorization

DATA CATEGORIZATION
IDENTITY
CONTACT INFO
PERSONAL
PROFESSIONAL EXPERIENCE
FINANCE
RISK MANAGEMENT
LEGAL ACTION
INFORMATION SECURITY
CUSTOMER SERVICES
MARKETING
PROCESS SECURITY

VISUAL AND AUDIO RECORDS
CLOTHING
PHYSICAL SPACE SECURITY
UNION MEMBERSHIP
FOUNDATION MEMBERSHIP
MEDICAL DATA
PENAL CONVICTIONS AND SECURITY MEASURES
RACE AND ETHNIC ORIGIN
PHILOSOPHICAL BELIEF, RELIGION, SECT AND OTHER BELIEFS

Acquisition and Processing Purposes of the Personal Data of Personal Data Subjects Included in Personal Data Subject Groups

The company collects the personal data via printed forms, directly from the concerned person, from Contracts, suppliers, electronic mail, Company common areas, Company's concerned departments, notifications from administrative and judicial authorities and other communication channels in the audio, electronic or written format in line with the personal data processing conditions as set out in the KVKK and in accordance with the legal grounds as specified in this Policy.

Associating the Data Subject Groups with the Data Categories of such Persons

PERSONAL DATA CATEGORIZATION	DATA SUBJECT CATEGORY THAT RESPECTIVE PERSONAL DATA RELATES
IDENTITY	Employee, Executive, Supplier's Employee, Supplier's Official, Employee Candidate, Intern, Person Given as Reference by the Employee Candidate, Employee, Employee's Relative, Visitor, Group employee, Person Receiving Goods or Service (customer), Group employee, Executive, Prospective buyer of good or service, Shareholder, all natural persons
CONTACT INFO	Employee, Executive, Supplier's Employee, Supplier's Official, Employee Candidate, Intern, Person Given as Reference by the Employee Candidate, Employee's Relative, Visitor, Group employee, Person Receiving Goods or Service, Prospective buyer of good or service, Shareholder, all natural persons
PERSONAL	Employee Candidate, Intern, Employee, Supplier's Employee, Executives, Group employee, Prospective buyer of good or service, Supplier's Official, Shareholder, Supplier's Official, Supplier's Employee, Person Receiving Goods or Service
LEGAL ACTION	Employee, Supplier's Employee, Executives, Group employee, Person Receiving Goods or Service, Group employee, Shareholder, Supplier's Official
PHYSICAL SPACE SECURITY	Supplier's Official, Supplier's Employee,

	Employee, Visitor, Prospective buyer of good or service, Person Receiving Goods or Service, Group employee, Executives
PROCESS SECURITY	Employee, Supplier's Employee, Supplier's Official, Visitor, Person Receiving Goods or Service, Executives, Group employee
RISK MANAGEMENT	Employee, Executive, Supplier's Employee, Supplier's Official, Group employee, visitor, Shareholder
FINANCE	Employee, Person Receiving Goods or Service, Prospective buyer of good or service, Supplier's Official, Group employee, Executive, Shareholder, Supplier's Employee, Employee, Person Receiving Goods or Service, Executives
MARKETING	Person Receiving Goods or Service, Prospective buyer of good or service
CUSTOMER SERVICES	Person Receiving Goods or Service
CLOTHING	Supplier's Employee, Employee, Visitor, Supplier's Official
PROFESSIONAL EXPERIENCE	Employee Candidate, Intern, Employee, Prospective buyer of good or service, Supplier's Official Supplier's Employee, Executives, Shareholder
VISUAL AND AUDIO RECORDS	Employee Candidate, Intern, Employee, Group employee, executive, Supplier's Employee, Person Receiving Goods or Service, Supplier's Official, Visitor, Shareholder
UNION MEMBERSHIP	Employee Candidate, Intern, Employee
FOUNDATION MEMBERSHIP	Employee Candidate, Intern, Employee
MEDICAL DATA	Employee Candidate, Employee, Supplier's Employee, Supplier's Official, Visitor, Person Receiving Goods or Service
PENAL CONVICTIONS AND SECURITY MEASURES	Employee, Executives, Supplier's Official, Supplier's Employee, Executives, Shareholder
RACE AND ETHNIC ORIGIN	Employee Candidate, Supplier's Employee, Employee, Person Receiving Goods or Service, Supplier's Official, Person Receiving Goods or Service, Group employee, Executive
PHILOSOPHICAL BELIEF, RELIGION, SECT AND OTHER BELIEFS	Employee Candidate, Employee, Supplier's Employee, Executives, Supplier's Official, Supplier's Employee

F. PRINCIPLES FOR TRANSFER OF THE PERSONAL DATA

The Company can transfer the personal data of the data subjects to the third parties and institutions pursuant to the personal data processing conditions as specified in Articles 5 and 6 of the KVK Law No.6698 and in accordance with articles 8 and 9 of the KVK Law and as limited with the purposes set out in this Policy.

The scope of the above-mentioned parties to which the data is transferred and the purposes for such data transfer are as set forth hereunder.

RECIPIENT GROUPS ELIGIBLE FOR DATA TRANSFER	DEFINITION OF RECIPIENT GROUPS	PURPOSE OF TRANSFER
COMPETENT PUBLIC INSTITUTIONS AND ORGANIZATIONS	Public legal institutions and organizations authorized to collect information and documents from the Company in accordance with the provisions of the applicable legislation	Limited to the purposes requested by the relevant public institutions and organizations pursuant to legal authority
NATURAL PERSONS OR PRIVATE LAW LEGAL ENTITIES	Private law entities authorized to collect information and documents from the Company in accordance with the provisions of the applicable legislation	Limited to the purposes requested by the relevant Private law entities pursuant to legal authority
PUBLIC	Printed or visual press/media, all natural persons transmitted via social media	Limited to the purposes such as fulfilling the legal obligations of the company (such as disclosure of financials), conducting social responsibility projects, promoting the company, etc.
SHAREHOLDERS	Natural persons and legal entities who are shareholders of the company	Limited to designing strategies regarding the business activities of the Company, ensuring the highest level of management and auditing purposes in accordance with the provisions of the applicable legislation
BUSINESS PARTNERS	The institutions and organizations where projects are carried out, services are procured and partnerships are established while the company is carrying out its activities	In relation and limited to the business objectives of the business partnership
SUBSIDIARIES AND AFFILIATES	The companies that are affiliates and subsidiaries of the company	In relation and limited to the business objectives
GROUP COMPANIES	The companies that are under the same control	In relation and limited to the business objectives

	structure as the company	
SUPPLIERS	The suppliers who provide services to the Company individually on contractual basis or without any contract in accordance with the Company's orders and instructions as the Company carries out the business activities thereof; the parties, tenants, third persons, companies or organizations from whom the Company receives service in any way while performing its activities, suppliers, consultants, lawyers, etc.	In relation and limited to the performance of the rendered services

G. TRANSFER OF PERSONAL DATA TO FOREIGN COUNTRIES

The company can transfer personal data to the foreign countries ("Foreign Country with Sufficient Protection") declared to have adequate protection by the KVK Board or, in absence of adequate protection, to the foreign countries ("Foreign Country where Data Controller Committing Adequate Protection Resides") where the data controllers in Turkey and the relevant foreign country undertake adequate protection in writing and permitted by the KVK Board.

In this respect, the company acts in accordance with the regulations as stipulated in Article 9 of the KVK Law.

Transfer of Personal Data Abroad

The company can transfer the personal data to Foreign Countries with Adequate Protection or to Foreign Country where Data Controller Committing Adequate Protection Resides if the personal data subject has explicit consent in line with legitimate and lawful personal data processing purposes, or upon existence of any of the cases listed hereunder if the personal data subject does not have explicit consent:

- If the laws contain any explicit regulation regarding transfer of the personal data,
- If mandatory for protection of the life or physical integrity of the person or someone else who is unable to disclose his/her consent due to the actual impossibility or whose consent is not legally valid,
- If it is necessary to transfer the personal data belonging to the parties of the contract, provided that such data is directly related to establishment or performance of any contract,
- If the personal data transfer is mandatory for the company to fulfill his legal obligation,
- If the personal data is made public by the data subject in person,

- If transfer of personal data is mandatory for establishment, exercise or protection of any right, and
- If transfer of personal data is mandatory for the legitimate interests of the Company, on the condition not to harm the fundamental rights and freedoms of the data subject.

Transfer of Sensitive Personal Data Abroad

The company can transfer the sensitive personal data of the personal data subject to the Foreign Countries with Adequate Protection or to the Foreign Country where Data Controller Committing Adequate Protection Resides in line with legitimate and lawful personal data processing purposes with due diligence and by adopting all safety measures as required and by adopting adequate measures as stipulated by the KVK Board;
- if the personal data subject has explicit consent or
- if the personal data subject does not have explicit consent;
  - → in cases as stipulated by law if the sensitive personal data other than the health and sexual life of the personal data subject (race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, clothing, association, foundation or union membership, criminal conviction and security measures and biometric and genetic data),
  - → only for protection of public health, execution of preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing, persons if the sensitive personal data regarding the health and sexual life of the personal data subject under the scope of processing by entities under confidentiality obligation or by authorized institutions and organizations.

As a rule, the personal data acquired by the company are not shared abroad.

H. STORAGE OF THE PERSONAL DATA

The personal data so acquired are stored securely in physical or electronic media for a suitable period of time in order for the Company to carry out its commercial activities.

Within the scope of such activities, the Company acts in accordance with the obligations as stipulated in all applicable legislation, in particular the KVK Law, regarding protection of the personal data.

In accordance with the applicable legislation, with the exception of cases wherein storage of the personal data for prolonged period is either permitted or mandatory, in the event where the intended purpose of processing the personal data is no longer available, then the personal data shall be deleted, destroyed or anonymized by the Company either as ex officio or at the request of the concerned parties.

If the personal data is deleted via these methods, such data shall be destroyed in such a way that they cannot be reused and recovered in any way.

However, in cases where the data controller has any legitimate interest, the personal data may be stored until expiry of the statute of limitations as specified

in the Code of Obligations or any other legislation concerning the Company, provided not to harm the fundamental rights and freedoms of the data subjects despite the fact that the intended purpose of processing is no longer available and that the periods as specified in the applicable laws expire. The personal data shall be deleted, destroyed or anonymized after expiry of the aforementioned statute of limitations.

İ. MEASURES ON PROTECTION OF THE PERSONAL DATA

The Company adopts necessary technical and administrative measures to prevent unlawful processing of the personal data processed by the company, to prevent unlawful access to the data and to ensure protection of the data in accordance with the conditions as specified in the KVK Law, and to perform or procure performance of necessary audits in this context.

In the event where the personal data so processed is illegally seized by the third parties despite all technical and administrative measures adopted in this respect, the Company informs relevant units as soon as possible.

Administrative and Technical Measures Adopted

- Network security and application security is ensured.
- Closed system network is used for personal data transfers via network.
- Security measures are adopted within the scope of procurement, development and maintenance of information technology systems.
- The security of the personal data stored in the cloud is ensured.
- Disciplinary regulations including data security provisions are in place for employees.
- Training and awareness rising events on data security are carried out periodically for employees.
- Access logs are regularly maintained.
- Corporate policies on access, information security, usage, storage and disposal issues have been compiled and implemented.
- Confidentiality commitments are executed.
- The authorizations granted to the employees, who are reassigned or leave employment, in this respect are removed.
- Up-to-date anti-virus systems are installed and used.
- Firewalls are installed and used.
- The contracts executed contain data security provisions.
- Data processing service providers are audited regularly regarding data security.
- The awareness of the service providers that process personal data concerning data security is ensured.
- Personal data security is closely monitored.
- Necessary security measures are being adopted as required at points of access to the physical spaces that contain personal data.
- Security of the physical spaces that contain personal data against external risks (fire, flooding etc.) is ensured.
- Security of the media that contain personal data is ensured.
- The quantity of the personal data is minimized to the most possible extent.
- The personal data is backed up and the security of the backed-up personal data is also ensured.
- The user account management and authorization control system is implemented and closely monitored.

- In-house periodical and/or randomized audits are carried out and procured for.
- The logs are kept so as to prevent any user intervention.
- Apparent risks and threats are identified.
- Attack detection and prevention systems are in place.
- Penetration test is implemented.
- Cyber security measures are adopted, and implementation of such measures is constantly monitored.
- Measures are adopted with fire extinguishing system, air conditioning system and software firewalls, attack prevention systems, network access control, anti-malware systems and access to the personal data stored in electronic or non-electronic media is classified according to access principles.
- An access control system that allows only authorized personnel to enter the hardware (system) room and 24/7 employee monitoring system is available in order to ensure security of the information systems against peripheral threats, and the physical security of edge switches that form up the local area network is ensured.
- Regular trainings are delivered to the employees involved in the processing of sensitive personal data, and the security of the media where such data is processed and stored is ensured.
- The obligation to inform the relevant persons is fulfilled.
- Provisions regarding confidentiality and protection of personal data are included in employment contracts, supply contracts and other contracts.

Supervision of the Measures Adopted for Protection of the Personal Data

Within the scope of the KVK Law, the Company bears the capacity of Data Controller and shall be registered with the VERBIS system. Paragraph 1 of the article 11 of the Regulation regulates that "The data controller obligations of the legal entities domiciled in Turkey under the Law are fulfilled by the competent body authorized to represent and bind the legal entity according to the provisions of the applicable legislation or by the person or persons as specified in the applicable legislation. The body authorized to represent the legal entity may assign one or more persons in relation to the obligations to be fulfilled in terms of implementation of the Law".

The top executives of each department shall be obliged to audit whether the Related Users in the departments comply with this Policy issued pursuant to the Law and Regulation, and report the findings to the Board of Directors. In cases that require taking any decision, the decision so taken shall be implemented after the Board of Directors takes the decision in consultation with the Legal Consultant.

J. DISCLOSURE REQUIREMENT OF THE DATA CONTROLLER

In line with Article 10 of the KVK Law, the company discloses the rights of the personal data subject and guides the personal data subject on how to exercise such rights.

The company executes necessary channels, internal functioning, administrative and technical regulations in accordance with Article 13 of the KVK Law in order to allow the personal data subjects to exercise their rights and to disclose necessary information to personal data subjects.

Within the scope of Article 10 of the KVK Law, the data subjects must be informed before or, at latest, during acquisition of the personal data. The information to be conveyed to data subjects pursuant to aforementioned disclosure obligation is as follows:

1. The identity of the data controller and representative thereof, if any,
2. The intended purpose of processing the personal data,
3. To whom and for what purpose the processed personal data can be transferred,
4. The method and legal grounds for collecting personal data, and
5. Other rights as listed in Article 11 of the KVK Law.

In order to fulfill its disclosure obligation, the company has compiled disclosure statements on the basis of the process and the persons whose data are processed, to be submitted to the data subjects pursuant to the KVK Law mentioned above.

After presenting the disclosure statements to the data subjects, explicit consent statements have also been prepared for data processing operations and data categories that require data subject's explicit consent to perform the activities of the Company.

On the other hand, the Company does not have any disclosure obligation in cases listed within the framework of Article 28 (1) of the KVK Law.

K. COMPANY'S RESPONSE TO THE APPLICATIONS

The Procedure and Duration of the Company to Respond to Applications

If the personal data subject submits his/her request to the Company, the Company shall conclude the request free of charge within thirty days at latest, depending on the nature of the request.

However, in case any fee is stipulated by the KVK Board, the fee specified in the tariff set by the KVK Board shall be collected from the applicant by the Company.

The Information that the Company may request from the Applicant Personal Data Subject

The company may request information from the person concerned in order to determine whether the applicant is actually the personal data subject. In order to clarify the matters included in the application of the personal data subject, the company may ask question to the personal data subject regarding his/her application.

The Company's Right to Reject the Application of the Personal Data Subject

The company may reject the application of the applicant in the following cases by providing justification:

1. Processing of the personal data for purposes such as research, planning and statistics by anonymizing such data with official statistics.
2. Processing of the personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, on the condition not to violate the national defense, national security, public security, public order, economic security, privacy of private life or personal rights, or not to constitute any criminal act.
3. Processing of the personal data within the scope of preventive, protective and intelligence operations carried out by public institutions and organizations authorized by the law to ensure national defense, national security, public security, public order or economic security.
4. Processing of the personal data by judicial authorities or execution authorities in relation to any investigation, prosecution, trial or execution proceedings.
5. If processing of the personal data is necessary for prevention of any criminal activity or for any criminal investigation.
6. Processing of the personal data made public by the personal data subject in person.
7. If processing of the personal data is necessary for execution of supervisory or regulatory duties and for disciplinary investigation or prosecution by the authorized and competent public institutions and organizations and public professional organizations on the basis of the authority vested by the law.
8. If processing of the personal data is necessary for protection of the economic and financial interests of the State regarding budget, tax and financial issues.
9. If the personal data subject's request might hinder the rights and freedoms of other persons.
10. If the requests made require exertion of disproportionate effort.
11. If the information so requested is already in public domain.

L. REVISION AND ABOLITION

IF this Policy is revised or abolished, then the revised version of the Policy or the new policy sample shall be announced at respective sites.

M. VALIDITY

This policy enters into force on 28.01.2018.

N. EXECUTION

The data controller and the board of directors liable from fulfilment of the obligations of the data controller as well as the executives of all departments (the top executive in the department) are responsible for execution of this Policy.