PERSONEL DATA PROTECTION POLICY

1. PURPOSE

The Company (Akmerkez GYO A.Ş.) undertakes to comply with the national personal data protection legislations as part of its legal and social responsibility. This Personal Data Protection Policy (the "Policy") is applied in the entire Company in line with the regulations in force based on the nationally accepted fundamental principles regarding protection of personal data.

This Policy sets forth the details as to the types of personal data collected for the performance of corporate activities, utilization and disclosure of the personal data, measures adopted for guaranteeing the security of personal data, rights of data subjects on their respective personal data processed by the Company, methods for exercising the relevant rights and the duration designated for storage of the personal data.

2. DEFINITIONS AND ABBREVIATIONS

Explicit consent: refers to the consent provided with free will on a given subject based on the supply of information.

Anonymization: refers to the alteration of personal data perpetually so that the data shall no longer be identified as personal data. E.g. masking, consolidation, data disintegration and similar methods used for making it impossible for personal data to be associated with a natural person.

Application form: refers to the "Application Form to be Used for Applications to be Filed to Data Controller by Data Subjects as per the Personal Data Protection Law no. 6698" with a view to exercising the rights related to the personal data.

Job applicant: refers to natural persons who apply for a position in the Company by any means or submit their resumes and relevant information to be reviewed by the Company.

Employees, shareholders and officers of business partners: refers to natural persons who work for the companies having a business partnership with the Company (including without limitation business partners and suppliers) including the shareholders and officers of those companies.

Business partner: refers to the parties with which the Company forms any business partnership for undertaking projects, receiving services etc. while conducting its commercial operations.

Personal data processing: refers to any operation which is performed upon personal data by automatic means completely or partially or through non-automated methods as part of any data recording system such as collection, recording, storage, retention, alteration, adaptation, disclosure, transfer, acquisition, making available, classification or blockage of the data.

Data subject: refers to natural persons whose personal data are processed. E.g. job applicants.

Personal data: refers to any information relating to an identified or identifiable natural person. Therefore, data related to legal entities are not governed by the Law. E.g. name and surname, Turkish ID number, e-mail, address, date of birth, credit card number etc.

Company: Akmerkez GYO A.Ş.

PDP Law: refers to Personal Data Protection Law no. 6698 of March 24, 2016 which was published in the Official Gazette no. 29677 of April 7, 2016.

PDP Board: Personal Data Protection Board

PDP Authority: Personal Data Protection Authority

Special categories of personal data: refers to personal data revealing racial or ethnic origin, political opinions, philosophical convictions, religious, sectarian or other beliefs, appearance, membership to associations, foundations or trade unions, health, sexual life, conviction and security measures as well as biometric and generic data.

Policy: Akmerkez GYO A.Ş. Personal Data Processing and Protection Policy

Company Shareholder: refers to natural persons who hold shares in the Company.

Company Officer: refers to natural persons who act as directors of the Company and assume other executive positions.

Supplier: refers to the parties who provide any service to the Company based on an agreement executed in line with the orders and instructions of the Company for facilitating its commercial operations.

Third Person: refers to natural persons with personal data processed under the personal data protection policy but not identified in a different manner under the policy (E.g. guarantor, attendant, family members and relatives, former employees).

Data processor: refers to the natural and legal person processing the personal data on behalf of the data controller based on the applicable authorization. E.g. cloud IT company keeping the data of the Company, call-centre company making phone calls based on scripts etc.

Data controller: refers to the person determining the purposes and means of the processing of personal data with the responsibility to manage the site where the data are kept systematically (data recording system).

Representative of data controller: refers to the person assigned by the data controller in order to deliver or receive notices and correspondences made by PDP Authority on behalf of the data controller, ensure that the requests of the PDP Authority are transferred to the data controller, inform the PDP Authority of the response to be given by the data controller, receive the applications of data subjects made under article 13.1 of the Law and submit them to the data controller unless otherwise required by the PDP Board, and perform the registration processes and procedures on behalf of the data controller.

Visitor: refers to natural persons who enter the physical campuses of the Company or visit its websites for any purpose.

3. SCOPE, POLICY and RESPONSIBILITIES

3.1. SCOPE

This Policy:

a) Applies to the entire Company for the purpose of processing personal data.

b) Is applicable for the natural person customers of the Company as well as other natural persons who do not enter into any framework agreement with the Company.

c) Does not apply to anonymized or unidentifiable data such as information obtained for statistical evaluations or studies as well as data of legal person since such data are not considered to be personal data.

3.2. POLICY

This Personal Data Protection Policy shall enter into force upon the approval of the Board of Directors. The policy shall be reviewed regularly and updated in line with the requirements.

Legal regulations in force concerning the processing and protection of personal data shall take precedence over this policy. The policy has been drafted by means of adaptation of the relevant legislative provisions to the corporate practices of the Company.

The following categories of personal data shall be processed by duly informing the data subjects under article 10 of PDP Law to be limited to the duration provided herein with due regard for the general principles indicated in PDP Law including article 4 regarding processing of personal data and in compliance with the all of the obligations specified in PDP Law based on the lawful and legitimate personal data processing purposes of the Company provided that any such processing shall be based on and limited to one or a few of the personal data processing conditions indicated in article 5 of PDP Law.

3.2.1. CATEGORIES OF PERSONAL DATA

The following personal information relating to customers, job applicants, employees, company shareholders, company officers, visitors, employees, shareholders and officers of business partners and third persons are regarded personal data.

3.2.1.1. Identity Details

Identity details are defined as the data which clearly relate to an identified or identifiable natural person, processed by automatic means completely or partially or through non-automated methods as part of any data recording system and are comprised of the information about the identity of the data subject.

E.g. name, surname, Turkish ID number, nationality, mother's name, father's name, place of birth, date of birth, gender and similar details available in driving license, identity card and passport as well as information such as tax number, SGK number, signature etc.

3.2.1.2. Contact Information

Contact information is the data which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system.

E.g. phone number, address, e-mail address, fax number, IP address etc.

3.2.1.3. Information about Family Members and Relatives

This refers to the data about the family members and relatives of the data subject which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system so that the legal and other benefits of the data subject may be protected in relation to the products and services under the operations conducted by the business divisions of the Company.

E.g. spouse, mother, father, children and other people to be contacted in case of emergency.

3.2.1.4. Location Data

This refers to the data which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system and used for determining the location of the data subject while using the products and services or using the corporate applications of the employees of business partners in line with the operations conducted by the business divisions of the Company.

E.g. GPS location etc.

3.2.1.5. Physical Space Security Information

This refers to the data such as records and documents taken at the entrance or inside a physical space which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system.

E.g. CCTV footage, fingerprint database, records of the security check point etc.

3.2.1.6. Financial Information

This refers to the data about the information, documentation and records displaying all kinds of financial results created according to the type of legal relationship between the Company and data subject which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system.

E.g. Bank account number, IBAN number, credit card information, financial profile, asset data, income details etc.

3.2.1.7. Personnel Information

This refers to all kinds of data which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system in order to obtain the information that shall form the basis for establishing the personnel rights of natural persons employed by the Company.

3.2.1.8. Visual/Audio Data

This refers to the data which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system;

E.g. Photograph and camera footage (excluding those regarded as Physical Space Security Information), voice records and data provided in the copies of the documentation containing personal data.

3.2.1.9. Special Categories of Personal Data

This refers to the data provided in article 6 of PDP Law which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system.

E.g. health information including blood type, biometric data, religion, membership to associations etc.

3.2.1.10. Demand/Complaint Management Data

This refers to the data used for receiving and evaluating all kinds of demands or complaints submitted to the Company which clearly relate to an identified or identifiable natural person; are processed by automatic means completely or partially or through non-automated methods as part of any data recording system.

3.2.2. PERSONAL DATA PROCESSING POLICY

The Company shall adopt and implement the following measures regarding the processing of personal data:

a) The Company shall perform personal data processing activities in line with the principles provided in article 4 of PDP Law and retains the personal data as required for the purpose of processing or in line with the duration specified in the law.

b) The Company shall process personal data based on one or a few of the conditions specified in the legal provision regarding processing of personal data pursuant to article 5 of PDP Law.

c) The Company shall inform data subjects as provided in article 10 of PDP Law in addition to giving information when required by data subjects.

d) The Company shall act in line with the requirements for processing of special categories of personal data in line with article 6 of PDP Law.

e) The Company shall act in line with the principles set forth by PDP Board as provided in the law regarding transfer of personal data pursuant to article 8 and 9 of PDP Law.

The Company shall act in line with the following principles while processing personal data:

a) Compliance with Law and Principle of Integrity

The Company shall conform to the legal principles as well as the rule of general trust and integrity while processing personal data. In that respect, the Company shall take into consideration the requirements of proportionality and use the personal data only to the extent of the relevant purpose.

b) Accuracy and, Where Necessary, Up-to-dateness of Personal Data

The Company shall ensure that the personal data remain accurate and up-to-date while processing them in line with the fundamental rights of data subjects and its own legitimate interest. It shall adopt necessary measures to that end.

c) Processing for Specific, Explicit and Legitimate Purposes

The Company shall define legitimate and lawful processing purposes specifically and explicitly. The Company shall process personal data to the extent required for and related to its commercial operations. The Company shall clearly explain the purpose of processing before commencing any such processing activities.

d) Being Relevant, Limited and Proportionate to the Purpose of Processing

The Company shall process personal data conveniently for furthering the relevant purposes in that it avoids processing personal data which are not related to or required for the purpose.

e) Retention for the Period Specified in the Relevant Law or Required for the Purpose of Processing

The Company shall retain the personal data only to the extent provided in the law or required for the relevant purpose. In that respect, the Company shall primarily determine if the relevant law provides for any duration for retention of personal data and comply with the duration if any. Otherwise, it shall retain the personal data as required for the purpose of processing. The Company shall delete, destroy or anonymize the personal data upon expiration of the duration or conclusion of the processing conditions. The Company shall retain any personal data in case they are needed in the future.

3.3. PURPOSES FOR PROCESSING OF PERSONAL DATA

The Company shall process personal data for the purpose of:

a) Fulfilment of corporate services,

b) Planning and implementing corporate sustainability activities,

c) Event management,

d) Management of relations with business partners or suppliers,

e) Fulfilment of personnel recruitment processes,

f) Performance/follow-up of financial reporting and risk management processes of the Company,

g) Performance/follow-up of legal processes for the Company,

h) Planning and implementing corporate communication activities,

i) Implementing corporate management activities,

j) Performance of processes under corporations law,

k) Demand and complaint management,

l) Conducting activities for maintaining the good standing of the Company,

m) Management of investor relations,

n) Providing information to authorized organizations under the law,

o) Improving and customizing corporate services, and

p) Creation and follow-up of visitor records.

In the event that the processing activity conducted for the purposes provided above does not meet any one of the requirements indicated in the PDP Law, the Company shall receive explicit consent from data subjects for the relevant processing activity.

3.4. PROCESSING OF PERSONAL DATA

Special categories of personal data and other personal data may also be processed in case of availability of one or more than one of the following conditions.

a) Availability of Explicit Consent of Data Subject

One of the conditions for processing personal data is the explicit consent of the data subject. A data subject shall be expected to provide explicit consent for any specific purpose with freewill based on the information provided about the processing activity. Any processing activity which is outside the purpose of processing related to the reason for acquisition of personal data (primary processing) shall be considered as secondary processing which requires minimum one of the conditions provided in paragraphs (b), (c), (d) (e), (f), (g) and (h) of this section. If any of those conditions is not satisfied, the Company shall process the personal data by receiving explicit consent from the data subject.

b) Express Permission in Law

Personal data may be processed lawfully where expressly permitted in the law. E.g. driver information as per Highway Traffic Law.

c) Physical Incapability to Receive Explicit Consent from Data Subject

Personal data may be processed where it is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent.

E.g. informing hospital of identity details of an employee who suffers from an occupational accident.

d) Direct Relevance to Execution or Performance of a Contract

Personal data may be processed where it is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract.

E.g. receiving the data concerning a customer/employee for fulfilling the requirements of a contract executed with that customer/employee.

e) Compliance with Legal Obligations

Personal data may be processed where it is necessary for the Company to perform its legal obligations as a data controller. E.g. submitting information required under a court order.

f) Personal Data Made Public by Data Subject

Personal data may be processed where the relevant data are made public by the data subject.

E.g. a job applicant disclosing the contact details on employment websites.

g) Obligation to Establish or Protect Any Right

Personal data may be processed where it is establishing, using or protecting any right.

E.g. retention of data constituting proof (e.g. agreement and addenda) to be used when necessary.

h) Obligation to Preserve Legitimate Interests of the Company

Personal data may be processed where it is necessary for the legitimate interests of the data controller, provided that such processing is not detrimental to fundamental rights and freedoms of the data subject.

E.g. CCTV footage taken in buildings and offices of the Company for security purposes.

The Company shall process "specific categories" of personal data determined in PDP Law in line with the requirements provided in the same law.

The Company shall process specific categories of personal data based on the explicit consent of the data subject by taking adequate measures to be designated by PDP Board in line with PDP Law or under following conditions where explicit consent is not received from the data subject:

i. Specific categories of personal data other than health and sexual life may be processed as provided in the law,

ii. Personal data relating to health and sexual life may only be processed to the extent required for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorized institutions and organizations,

iii. Regarding private healthcare insurance taken out for employees, specific categories of personal data may be processed in case of any requirement for exchange of healthcare data between the private healtcare insurance company and healthcare institutions providing health services in order to ensure that employees may benefit from those services effectively.

3.5. INFORMING PERSONAL DATA SUBJECT

Data subjects shall be entitled to "request information" as per article 11 of PDP Law. Accordingly, the Company shall give necessary information in case any such request is made by a Data Subject under article 11 of PDP Law.

The Company informs data subjects as necessary during the collection of personal data in line with article 10 of PDP Law. In that respect, the Company explains the identity of representative, if any, purposes for processing of personal data, recipients of personal data and purpose of transfer, methods of collecting personal data, legal justification and rights of data subjects.

3.6. TRANSFER OF PERSONAL DATA

The Company may transfer personal data to third persons based on legitimate and lawful processing purposes. The Company shall perform transfer activities based on the following requirements:

- Through adoption of necessary security measures,

- Based on and limited to one or more than one of the processing conditions provided in article 5 of PDP Law, and

- In compliance with the transfer requirements provided in article 8 of PDP Law.

The Company may transfer personal data to foreign countries which are certified to ensure sufficient protection by PDP Board (a "Foreign Country with Sufficient Protection"). In case of lack of sufficient protection, personal data may be transferred to foreign countries based on the permission of PDP Board if the data controllers in Turkey and abroad issue a written covenant to undertake sufficient protection (a "Foreign Country with a Data Controller Undertaking Sufficient Protection"). The Company shall observe the principles of article 9 of PDP Law in that regard.

Third Persons Receiving Personal Data and Transfer Purposes:

The Company shall inform data subjects of third persons and groups to whom personal data are transferred in line with article 10 of PDP Law. For the purposes designated in articles 8 and 9 of PDP Law, the Company may transfer personal data belonging to data subjects based on this Policy to:

a) Business partners to be limited to the purpose of fulfilling the objectives of the business partnership,

b) Suppliers to be limited to the purpose of providing the Company with the outsourced services required for the corporate operations,

c) Company shareholders to be limited to the purpose of fulfilling the objectives of corporate activities conducted under corporations law, event management and corporate communications processes in line with the provisions of applicable regulations,

d) Company employees and officers to be limited to the purpose of determining strategies for corporate operations of the Company, ensuring highest level of managerial effectiveness and conducting audits under the provisions of applicable regulations,

e) Competent public authorities and organizations to be limited to the purpose of meeting the legitimate requests of the relevant authorities and organizations,

f) Private legal persons that hold legal power to be limited to the purpose of meeting the legitimate requests of the relevant private legal person.

3.7. RETENTION OF PERSONAL DATA AND RETENTION PERIOD

The Company shall inform data subjects of the personal data subject to processing activities, processing purposes and retention periods in line with the disclosure obligation provided in article 10 of PDP Law.

The Company shall retain the personal data for the period of time specified in the relevant laws and regulations, if applicable. If, on the other hand, the regulations do not provide for a retention period, the Company shall process the personal data for the period of time required under the corporate practices and commercial principles in relation to the activity making it necessary to process the personal data after which it shall delete, destroy or anonymize them.

After processing purpose is fulfilled and retention period which is provided in relevant regulations and designated by the Company is concluded, personal data may only be retained only if they constitute evidence for potential legal disputes or for the purpose of making any claim or defence with the use of the personal data. Retention period shall be determined with due regard for the prescription time as well as the previous demands made from the Company on the same subject notwithstanding the expiration of the prescription time provided for making claims in relation to the relevant rights. In that case, it shall not be possible to have access to the personal data that are retained for any other purpose and they shall be accessible only if required for settlement of a legal dispute. Personal data shall be deleted, destroyed or anonymized following the expiration of the relevant period.

3.8. DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Personal data shall be deleted, destroyed or anonymized as per the decision of the Company or based on the request of the data subject upon the fulfilment or conclusion of processing purposes after the personal data is processed in line with the legal requirements as provided in article 7 of PDP Law. The Company shall perform this obligation by means of the methods explained in this section.

The Company shall delete or destroy personal data by using the following methods:

a) Physical Destruction

Personal data may be processed through non-automated methods as part of any data recording system. Such data shall be deleted/destroyed through physical destruction so that they shall not be used in the future.

b) Secure Deletion from Software

If personal data are processed by automatic means completely or partially and retained in digital media, they shall be deleted/destroyed with the use of methods for deleting the data from the software to prevent its retrieval from the system in the future.

c) Secure Deletion by Experts

In some cases, the Company may outsource the deletion tasks from experts on the subject. In that case, personal data shall be deleted/destroyed with the use of secure methods so that they shall not be retrieved in the future.

The Company may anonymize personal data upon the conclusion of legitimate processing purposes. Anonymized personal data may be processed for research, planning and statistical purposes etc. in line with article 28 of PDP Law. Such processing activities shall be under the scope of PDP Law according to which it shall not be necessary to seek for explicit consent from the data subject.

The Company shall use the following anonymization methods.

a) Masking

Data masking is defined as anonymization of personal data by removing the fundamental distinctive features of personal data from the data set. E.g. removing the data subject's name, Turkish ID no etc. in order to derive a data set where the data subject is unidentifiable.

b) Blending

Data blending is used for merging loads of data into a single set of data so that the personal data shall no longer be associated with a specific person. E.g. calculating that the number of employees at the age of X is Z without indicating the age of each employee.

c) Data Derivation

Data derivation method is used for creating a more overarching content than that of personal data so that the personal data shall no longer be associated with a specific person. E.g. referring to ages instead of dates of birth or area of domicile instead of full address.

d) Data Mixing

Data mixing method is used for mixing the values of personal data set in order to dissociate values from persons. E.g. modifying features of voice records so that the voice of a data subject shall no longer be identified.

3.9. PERSONAL DATA PROCESSING ACTIVITIES RELATED TO VISITORS

The Company shall perform personal data processing activities to promote security in line with PDP Law and relevant regulations.

3.9.1. Monitoring Buildings and Offices with CCTV Systems

The Company shall use CCTV systems in order to ensure security and protect interests of the company and other persons. Those activities shall be performed in line with the requirements of PDP Law in terms of privacy and fundamental rights of individuals.

The Company shall use two methods to inform data subjects of monitoring activities performed with the use of CCTV systems. A notice shall be published on the corporate website under the principles of Protection of Personal Data in addition to a bulletin available in the areas where monitoring activities are conducted (onsite information).

The monitoring areas, number of cameras and timing of monitoring activities shall be determined in a manner that shall be adequate for and limited to security purposes. CCTV systems shall not be available in areas where personal privacy may be violated in a manner that shall invalidate security purposes.

Personal data derived from the systems shall be processed as provided in the relevant sections of this policy.

Live CCTV footage and records stored in digital media shall be accessible solely to a limited number of employees of the Company and, if necessary, the employees of the security company acting as the provider of security services. The employees who have access to the records shall sign a confidentiality undertaking to confirm that they shall observe the confidentiality rules regarding the relevant data.

3.9.2. Monitoring Entrances-Exits of Buildings and Offices

The Company performs personal data processing activities comprised of the follow-up of visitors' entrance to and exit from the buildings and offices of the Company in order to promote security and fulfil the objectives specified herein. Information shall be provided to data subjects verbally while they are asked to give their full names upon entering the buildings of the Company as visitors or by means of texts displayed or rendered accessible to the visitors otherwise. Such data shall only be processed and stored for the purpose of monitoring visitors' entrance to and exit from the building.

3.9.3. Internet Access for Visitors

The Company may provide internet access to visitors, upon request, in the buildings and offices in order to ensure security and fulfil the objectives indicated in this Policy. In such cases, log sheets concerning internet access of visitors shall be recorded in line with the mandatory provisions of the Law no. 5651 and the relevant regulations provided that those records shall only be processed in case of demand of competent public authorities and organizations or for the purpose of fulfilling a legal obligation arising from audits conducted inj the Company.

In that sense, solely a limited number of corporate employees shall be entitled to have access to log sheets and generate reports thereunder. The permitted employees shall have access to the logs B in case of demand of competent public authorities and organizations or for the purpose of audits and disclose them to legally authorized individuals. The employees who have access to the logs shall sign a confidentiality undertaking to confirm that they shall observe the confidentiality rules regarding the relevant data.

3.9.4. Website Visitors

The Company may record the actions performed on its websites by using suitable technical means (e.g. cookies) to ensure that visitors of websites can achieve the aim of visit, to display customized contents to visitors and to perform online advertising activities. The disclosures available on the websites shall contain detailed explanation about the protection and processing of personal data arising from the activities performed by the Company.

3.10. RIGHTS OF DATA SUBJECTS AND USE OF RIGHTS

The Company shall inform data subjects of their rights under article 10 of PDP Law in addition to offering guidance on how to exercise those rights. The Company shall keep in charge of the necessary channels, internal functioning, administrative and technical regulations for evaluating the rights of data subjects and informing them as necessary under article 13 of PDP Law.

3.10.1. Rights of Data Subjects

Data subjects shall be entitled to:

a) learn whether or not your personal data have been processed,
b) request information about the processing, if any,
c) request information about the processing purpose whether or not the use of the data is fit for the purpose,
d) receive information about the recipient domestic/foreign third parties,
e) ask for correction in case of incomplete / incorrect processing and notification of third persons to whom the personal data are transferred,
f) ask for deletion or destruction of personal data by duly informing the third persons receiving the personal data of this fact in the event that the causes for processing are no longer applicable even though the personal data are processed in line with PDP Law and other legal provisions and request notification of third persons to whom the personal data are transferred about the deletion,
g) object to any unfavourable result arising from analysis of processed data with automated systems exclusively, and
h) demand indemnification against losses, if any, incurred as a result of processing activities in violation of the law.

Data subjects may not make any claims for the following cases which remain outside the scope of PDP Law under article 28 of the same law:

a) Processing of personal data for the purposes of official statistics and, through anonymization, research, planning, statistics.

b) Processing of personal data for the purposes of art, history, and literature or science, or within the scope of freedom of expression, provided that national defence, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated.

c) Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized for providing national defence, national security, public safety, public order or economic safety.

d) Processing of personal data by judicial authorities and execution agencies with regard to investigation, prosecution, adjudication or execution procedures.

Pursuant to article 28/2 of PDP Law, data subjects may not make any claims other than the claim for indemnification against losses in following cases:

a) Processing of personal data which is required for prevention of crime or investigation of a crime.

b) Processing of personal data revealed to the public by the data subject.

c) Processing of personal data which is required for performance of supervision or regulatory duties, or any disciplinary investigation or prosecution, by competent and authorized public institutions and organizations and professional organizations which are considered to function as public institutions.

d) Processing of personal data which is required for the protection of economic and financial interests of the state related to budget, tax, and financial matters.

3.10.2. Use of Data Subject Rights

Data Subject may submit their requests to exercise the rights provided in this section to the Company free of charge by completing and delivering the Application Form to the Company with the following methods or any other method to be specified by Personal Data Protection Board along with the information and documentation proving their identity.

The Application Form should be delivered to:

a) Nispetiye Caddesi Akmerkez Ticaret Merkezi E-3 Blok Kat:1 Etiler-Beşiktaş / İstanbul by mail or in person,
b) akmerkez@akmerkez.hs02.kep.tr via registered electronic mail after scanning the form.

Any person to file an application on behalf of a data subject must submit a statutory power of attorney attested by a notary. The Company shall respond to all such requests within maximum thirty days free of charge according to the particulars of the request. Nevertheless, the Company shall charge the fee provided in the applicable tariff to the applicants if the Personal Data Protection Board provides for any fee for the relevant request. An application may be filed to the Company only if it is regarded a data controller under PDP Law. The Company may request the applicant to provide additional information in order to ascertain that the applicant is the data subject. The Company may also ask questions to the data subject in order to clarify the points available in the application.

The Company may deny an application in following cases by explaining the justification for denial:

a) If the request of the data subject has the potential to obstruct the rights and freedoms of other persons,
b) If the request necessitates disproportionate efforts,

c) If the information request is related to publicly disclosed information.

If any application is denied, replied insufficiently, or not replied in due time, the data subject may file a complaint with the PDP Board within 30 days following the date of receiving the reply of the Company and in any event, within 60 days following the date of application.

3.11. RESPONSIBILITIES

3.11.1. Personal Data Protection Committee

The Company has established a Personal Data Protection Committee to ensure that the requirements of PDP Law are duly observed and to enforce the Personal Data Protection and Processing Policy effectively. The Personal Data Protection Committee shall fulfil the following tasks:

a) Prepare and enforce the fundamental policies and, if necessary, amendments regarding the protection and processing of personal data.

b) Determine the methods to be used for implementing and supervising the policies regarding the protection and processing of personal data, assign tasks within the Company and ensure necessary coordination to that end.

c) Determine the actions required to be taken for ensuring compliance with PDP Law and relevant regulations, monitor the implementation process and ensure necessary coordination.

d) Raise awareness in the Company as well as its business partners regarding the protection and processing of personal data.

e) Determine the potential risks related to the personal data processing activities of the Company and ensure that necessary measures are duly taken.

f) Organize training programmes in order to ensure that data subjects are duly informed of personal data processing activities and their legal rights arising from those activities with respect to the implementation and dissemination of personal data protection policies.

g) Ensure that applications filed by data subjects are handled and concluded at the highest level.

h) Monitor and keep up with the developments and regulations regarding protection of personal data; make suggestions about the activities to be performed by the Company to comply with those developments and regulations and take necessary actions.

i) Steer and manage the relations with PDP Board and Authority.

3.11.2.IT Systems Committee

IT Systems Management shall:

a) Adopt measures required for protection of personal data under PDP Law.

b) Take measures and provide infrastructure for making sure that the personal data shall be retained for the period of time specified in the relevant legislation.

3.11.3. IT Systems and Business Continuity Management Committee

a) The Committee shall ensure that policies required for protection of personal data shall be developed pursuant to PDP Law.

b) The Committee shall ascertain the potential risks which may arise under PDP Law and ensure that necessary measures are adopted accordingly.

3.11.4. IT Security and Risk Management Officer (BGRSY)

a) The Officer shall promote coordination for development of policies required for protection of personal data under PDP Law.

b) The Officer shall promote coordination for providing information in order to raise awareness of the employees under Personal Data Protection Law.

c) The Officer shall coordinate periodical training sessions to be offered to employees about protection of personal data and information security.

3.11.5. Division Managers

Regarding protection of personal data under PDP Law, division managers shall:

a) Ensure that both managers and employees shall comply with the requirements of this document and other documents prepared and approved in relation to information security and risk management (e.g. policies, procedures, standards, directives etc.).

b) Undertake necessary adaptations in the tasks of the division with due regard for the provisions of PDP Law.

c) Ensure that employees shall be informed about the importance and necessity of PDP Law as well as protection of personal data and information security and attend training about the policies, procedures, standards, directives etc. of the Company.

3.11.6. Human Resources Division

In addition to the responsibilities assumed by Division Managements regarding protection of personal data and promotion of information security pursuant to PDP Law, Human Resources Division shall:

a) Make coordination with the division managers to ensure that responsibilities of employees shall also include responsibilities for protection of personal data.

b) Ensure that new hires are duly informed of the documents and responsibilities regarding protection of personal data and promotion of information security (e.g. policies, standards, procedures etc.) and record the information processes accordingly.

c) Act in coordination with the IT Security and Risk Management Officer in order to ensure that the relevant employees attend periodical training programmes about protection of personal data and information security and keep records of the training activities.

3.11.7. Personnel/User

In order to protect personal data and promote information security, each employee shall:

a) Comply with the approved policies and procedures regarding protection of personal data and promotion of information security.

b) Remain responsible for protecting personal data and promoting information security in relation to their own responsibilities / tasks.