FİBA HOLDİNG A.Ş.

POLICY ON THE PROTECTION AND PROCESSING OF PERSONAL DATA

1. INTRODUCTION ---------- 5

2. PURPOSE AND SCOPE ---------- 5

3. DEFINITIONS---------- 6

4. POLICY IMPLEMENTATION AND RESPONSIBILITIES ---------- 7

5. PRINCIPLES OF PROCESSING OF PERSONAL DATA ---------- 8

5.1. General Principles of Processing of Personal Data ---------- 8
5.1.1. Lawfulness and conformity with rules of bona fides---------- 8
5.1.2. Accuracy and being up to date ---------- 8
5.1.3. Being processed for specific, explicit and legitimate purposes---------- 8
5.1.4. Being relevant with, limited to and proportionate to the purposes for which they are processed---------- 8
5.1.5. Processing for the period of time stipulated by relevant legislation or the purpose for which they are processed ---------- 8

6. CONDITIONS FOR PROCESSING OF PERSONAL DATA---------- 9

6.1. Explicit consent of the data subject ---------- 9

6.2. Data Processing Due to Legal Requirements ---------- 9

6.3. Mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid ---------- 9

6.4. Processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfillment of that contract------- 9

6.5. Mandatory for the controller to be able to perform his legal obligations---------- 9

6.6. Data concerned is made available to the public by the data subject himself----------10

6.7. Data processing is mandatory for the establishment, exercise or protection of any right ----------10

6.8. Mandatory for the legitimate interests of the controller to process data ----------10

7. CONDITIONS FOR PROCESSING OF SENSITIVE PERSONAL DATA----------10

7.1. Processing the sensitive personal data with explicit consent of the data subject ----10

7.2. Processing sensitive personal data without seeking explicit consent of the data subject, in the cases provided for by laws ---- 10

7.3. Processing of sensitive Personal data relating to health and sexual life for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing under confidentiality obligation ---- 11

7.4. Adequate measures to be taken while processing the sensitive personal data ---- 11

8. TRANSFER OF PERSONAL DATA ---- 11

8.1. Transfer of Personal Data ---- 11

8.1.1. Explicit consent of the data subject for the transfer of personal data ---- 11

8.1.2. Personal data may be transferred without explicit consent of the data subject provided that conditions concerning processing of personal data are ensured ---- 12

8.1.3. Sensitive Personal data may be transferred without explicit consent of the data subject provided that the transfer conditions has been ensured and it is required by law --- 12

8.2. Cross-border Transfer of personal data ---- 12

8.2.1. Explicit consent of the data subject for the cross-border transfer of personal data --- 12

8.2.2. Personal data may be transferred without explicit consent of the data subject provided that conditions concerning processing of personal data are ensured ---- 12

9. ERASURE, DESTRUCTION OR ANONYMIZING OF PERSONAL DATA ---- 13

10. OBLIGATIONS OF THE COMPANY IN THE CAPACITY OF DATA CONTROLLER ---- 13

10.1. Obligation to Inform ---- 13

10.2. Obligation to Secure Personal Data ---- 14

10.2.1. Obligation to prevent unlawful processing of personal data ---- 14

10.2.1.2. Technical measures for lawful processing of personal data ---- 14

10.2.1.2. Administrative measures for lawful processing of personal data ---- 14

10.2.2. Obligation to prevent unlawful access to personal data ---- 15

10.2.2.1. Technical measures to be taken for the lawful access and protection of personal data ---- 15

10.2.2.2. Technical measures to be taken for the lawful access and protection of personal data ---- 15

10.2.3. Control of measures to protect personal data ---- 16

11. THE RIGHTS OF DATA SUBJECT ---- 16

12. ENFORCEMENT AND UPDATES ---- 17

1. INTRODUCTION

The Turkish Data Protection Act (“KVKK"), which was prepared by studying for many years within the frame in compliance with the criteria of the European Union, entered into force with the publication in the Official Gazette dated 07.04.2016.

Turkish Data Protection Act contains regulations in the same direction with the Directive 95/46/EC of the European Union and, with the entry into force of the Turkish Data Protection Act, the protection of the personal data of individuals within an integrated system, has been organized under legislative regulation.

Due the fact that the data of legal entities are already protected by the applicable laws, together with the Turkish Data Protection Act, the concept of personal data, is organized in line with the European Union regulations to provide protection for natural persons only.

With the Turkish Data Protection Act, the protection of personal data subject and to use also his/her rights defined in Article 11 of the Law has been regulated, and as the content it is forming the subjects such as identification and classification of personal data, processing of personal data, obligation to inform, Explicit consent and exceptions, determination of obligations of natural and legal persons processing personal data, constituting the Personal Data Protection Authority, complaint application procedures and sanctions.

One of our Company's priority is to form the internal operations of our Company within the scope on the Turkish Data Protection Act, secondary regulations, Decision of Personal Data Protection Authority, final court orders and other relevant regulations in accordance with the new regulations stipulated by the Turkish Data Protection Act, within the frame of the principles of superior service quality, respect for individuals' rights, transparency and honesty adopted by our company.

For this reason, this Policy has been put into effect in order to let the personal data owners utilize from the rights of the Turkish Data Protection Act and to ensure the process of the adaptation to the Law.

2. PURPOSE AND SCOPE

2.1. With the policy, it is aimed to implement the regulations in order to comply effectively by the Company employees and business partners with the Turkish Data Protection Act, to be taken by the company within the framework of the basic principles explained above.

2.2. With this policy, administrative and technical measures introduced in the current legislation will be taken in line with the envisaged basic regulations, necessary internal procedures will be formed in order to process and protect personal data within the scope of the Company's operation, all necessary training will be performed to raise awareness, all necessary measures will be taken in accordance with the Turkish Data Protection Act for the adaptation of the employees and business partners to the process of Turkish Data Protection Act and, technological infrastructure, administrative and legal system will be established together with appropriate and affective control mechanism.

2.3. In accordance with the basic principles to be taken into consideration during all these processes and as per the regulations set forth in the Turkish Data Protection Act, the matters that our Company is liable to regulate internal operations are formed. With the internal procedures to be formed within the framework of the Turkish Data Protection Act and the relevant legislation, compliance activities of our Company regarding the protection of personal data will be formed. When performing their duties, all employees of our Company are obliged to act in accordance with the provisions of this Policy and the provisions of the Turkish Data Protection Act and all other relevant legislation.

2.4. In case of failure to comply with the policy and the relevant legislation, according to the nature of the event within the framework of the legislation regulating the business life, sanctions will be applied within our company in addition to the criminal and legal liability stipulated by the provisions of the legislation, which may result with the termination of the employment contract under justified reason.

3. DEFINITIONS

3.1. Explicit consent: Means freely given, specific and informed consent.

Due the reason that the burden of proof that the data subject has been informed and clarified will be on the responsibility of the Controllers, the storage and protection of the data subject's explicit consent and information records shall be made according to the internal procedures of the company.

3.2. Anonymizing: Means, rendering personal data impossible to link with an identified or identifiable natural person, even by matching them with other data.

It is possible to anonymize personal data with a variety of purposes and methods which do not violate the Turkish Data Protection Act and the scope of the Explicit Consent granted by the data subject. Necessary measures shall be taken within the company, in order not to render the personal data that is anonymized by making the data subject identifiable through various methods.

3.3. Data subject: Means, the natural person, whose personal data is processed.

Processing and protection of personal data of the natural or legal person customers of our company, the shareholders, managers or employees of the legal entity business partners, the company consultants, the advisors, the solution partners, the guests and the employees of our company, as well as sensitive personal data, shall be dealt with by our Company within the scope of the Turkish Data Protection Act and the Policy.

3.4. Personal Data: Means, all the information relating to an identified or identifiable natural person.

All information that makes the person identifiable is evaluated as personal data. i.e. T.R. ID No, Name-Surname, e-mail address, telephone number, address, date of birth, bank account number. Within our Company, these data have been classified and the personal data

processing is regulated by the Personal Data Processing Inventory in such a way that, who, for what purpose and for how long can process the different personal data in different categories.

3.5. Processing of personal data: Means, any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.

3.6. Sensitive Personal Data: Means, personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or their belief, appearance, membership to associations, foundations or trade-unions, health, sexual life, criminal convictions and security measures, and the biometric and genetic data are deemed to be sensitive personal data

3.7. Data Processor: Means, the natural or legal person who processes personal data on behalf of the controller upon their authorization.

With the internal procedures, it has been determined by departments upon that, who are authorized to access personal data and who processes this data within the meaning of the Turkish Data Protection Act, and that for what extent, for what purpose, for how long they can access the data.

3.8. Data Controller: Means the natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

4. POLICY IMPLEMENTATION AND RESPONSIBILITIES

4.1. As Data controller, the Company is responsible for the implementation of this Policy in terms of the formation of all internal processes and procedures.

4.2. In order to implement within the Company the regulations, procedures, guidelines, standards and training activities to be prepared in accordance with this Policy, a governance model shall be established and implemented by the Company.

4.3. All employees, business partners, guests and all related third parties throughout the Company, are obliged to cooperate with the Company in the prevention of legal responsibilities, risks and emergencies arising in accordance with the relevant legislation together with the compliance with the Policy.

4.4. All employees of all departments and bodies of the Company are obliged to act in accordance with the Policy and ensure compliance with the provisions of the Policy.

4.5. This Policy shall be announced within the Company and shall be available at all times by loading it into common information systems. In addition, this Policy shall be published on the Company's website. The changes in the policy shall be added to the information processing system and to the web site, and this will enable the data owners to reach the principles stipulated by the Policy.

4.6. In the event of a conflict between the policy and the provisions of the applicable legislation, the Company as the data controller agrees that the provisions of the legislation will be prevail.

5. PRINCIPLES OF PROCESSING OF PERSONAL DATA

5.1. General Principles of Processing of Personal Data

The Company agrees to process the personal data under this Policy as per the following principles, in accordance with Article 4 of the Turkish Data Protection Act:

5.1.1. Lawfulness and conformity with rules of bona fides

As data controller, the Company accepts that, it will conduct personal data processing activities in accordance with all applicable and future legislative provisions and in compliance with the provisions of Article 2 of the Turkish Civil Code, in particular the Constitution and the Turkish Data Protection Act.

5.1.2. Accuracy and being up to date

In the activities of processing personal data, to ensure the accuracy and up to date of personal data, the company takes all necessary measures under the Turkish Data Protection Act, insofar as circumstances permit. In accordance with the requests to be notified to the Company by the person in the capacity of data controller, and in cases where the Company deems it necessary, the administrative and technical mechanisms established by the Company will be processed in order to correct and crosscheck the incorrect or outdated personal data.

5.1.3. Being processed for specific, explicit and legitimate purposes

The personal data of the Company are processed in accordance with the law within the limitations of the services rendered or to be presented under the requirements of the relevant legislative provisions and the purpose of processing personal data is clearly and precisely determined before the processing of data.

5.1.4. Being relevant with, limited to and proportionate to the purposes for which they are processed

The personal data of the Company are processed in the limitations in connection with the purposes of processing and to the extent necessary to achieve this objective. In this context, it is essential to avoid the processing of personal data that is not related to the purpose of processing the data and which is not needed.

5.1.5. Processing for the period of time stipulated by relevant legislation or the purpose for which they are processed

Personal data is stored for the period stipulated in the relevant legislation provisions or for the period for which the data are intended to be processed. At the end of the period stipulated by the provisions of the legislation or at the end of the period required for the purpose of processing the data, personal data is deleted, destroyed or anonymized by the Company.

Necessary administrative and technical measures shall be taken to prevent data from being stored at the end of the required period.

6. CONDITIONS FOR PROCESSING OF PERSONAL DATA

Article 5 of the Turkish Data Protection Act, regulates the processing conditions of personal data. The process of processing personal data by the Company is carried out in accordance with the following conditions specified by the Turkish Data Protection Act.

6.1. Explicit consent of the data subject

The main rule in the processing of personal data is the explicit consent of the data subject in the processing of his/her data in the absence of other data processing conditions. The Company, shall carry out data processing activities for the transactions covered by the consent in accordance with the explicit consent of the data subject, as provided for by the Turkish Data Protection Act, upon clarification of the intended purpose and without and lack.

6.2. Data Processing Due to Legal Requirements

As a requirement of the Turkish Data Protection Act, data processing activities shall be deemed to be in accordance with the law, provided that other required criteria are ensured in cases where it is mandatory to process the personal data in accordance with the provisions of the legislation, even if the data subject do not have explicit consent.

6.3. Mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid

In the event that it is not possible for the data subject to disclose his/her consent in accordance with the Turkish Data Protection Act and if it is necessary to process personal data in order to protect the life or body integrity of the data subject or someone else, processing of personal data can be possible. The Company, shall process personal data in cases stipulated in aforementioned regulation.

6.4. Processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfillment of that contract

The personal data of the parties to the contract shall be processed by the Company, provided that it is directly related to the conclusion or fulfillment of the contract.

6.5. Mandatory for the controller to be able to perform his legal obligations

In accordance with the Turkish Data Protection Act, in order to be able for the Company with the capacity of data controller to fulfill its obligations arising from the provisions of the legislation, personal data shall be processed by the Company, depending on the limits of the said liability.

6.6. Data concerned is made available to the public by the data subject himself

If the personal data, made available to the public by the data subject, the personal data shall be processed by the Company in proportion to the objectives to make it public.

6.7. Data processing is mandatory for the establishment, exercise or protection of any right

Personal data shall be processed by the Company to the extent necessary for the establishment, exercise or protection of a right.

6.8. Mandatory for the legitimate interests of the controller to process data

Personal data may be processed in accordance with the legitimate interests of the Company in the capacity of data controller, provided that it does not harm the fundamental rights and freedoms of the data subject. However, the expressions of the Company's legitimate interests, cannot in any way be in contradiction with the principles of the Turkish Data Protection Act as well as the purpose of processing personal data and, it cannot interfere with the essence of the right guaranteed by the Constitution.

7. Conditions for processing of sensitive personal data

Article 6 of the Turkish Data Protection Act, regulates the processing conditions of sensitive personal data. In accordance with the subject article, sensitive personal data may relate to persons' ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures as well as biometric and genetic data. All business processes within the company, were examined and the data in this status were determined and classified and transferred to personal data inventory. The process of processing of sensitive personal data by the Company is carried out in accordance with the following conditions specified in the Turkish Data Protection Act.

7.1. Processing the sensitive personal data with explicit consent of the data subject

As a rule, according the Turkish Data Protection Act it is forbidden to process sensitive personal datawithout the explicit consent of the data subject. In this context, in order to be able to process sensitive personal data, the Company shall seek to provide explicit consent of the data subject. Data processing activities shall be carried out in accordance with the scope of the consent of the data subject for the processing of sensitive personal data.The provisions stipulated by the Turkish Data Protection Act, are reserved for the processing of sensitive personal data, without explicit consent. The Company shall conduct data processing activities in the processing of sensitive personal data, firstly by checking whether the data processing requirements are available.

7.2. Processing sensitive personal data without seeking explicit consent of the data subject, in the cases provided for by laws

In cases where it is foreseen that sensitive personal data may be processed under the provisions of the legislation, the personal data of the data subject other than his/her health and sexual life, may be processed in accordance with the provisions of Article 6/3 of the Turkish Data Protection Act. In this case, the data processing activities to be performed by the Company, shall be limited to the requirements of the underlying legislation provision.

7.3. Processing of sensitive Personal data relating to health and sexual life for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing under confidentiality obligation

Pursuant to the Turkish Data Protection Act, the processing of the personal data of the data subject's health and sexual life, is subject to the condition of the explicit consent of the data subject, and in cases where there is no explicit consent, it has been regulated that the subject personal data can be processed by the persons who have confidentiality obligation in cases the implementation of preventive medicine, medical diagnosis, treatment and care services and the financing of health services. The persons with confidentiality obligation will be able to process the personal data in accordance with the provisions of the legislation about the health and sexual lives of the data subject as required by the provisions of this legislation.

7.4. Adequate measures to be taken while processing the sensitive personal data

Pursuant to the Turkish Data Protection Act, in order to process sensitive personal data, it is mandatory to take the measures determined by the Turkish Data Protection Act. The Company shall process sensitive personal datain accordance with the measures to be determined by the Authority.

8. TRANSFER OF PERSONAL DATA

With the Article 8 of the Turkish Data Protection Act, the transfer of personal data to third parties in domestic is regulated. In the process of transferring personal data, the following criteria shall be complied with. As regards the transfer of personal data, it is the Company's responsibility to act in compliance with all applicable legislation and to adapt the transfer processes in accordance with applicable or further legislation.

8.1. Transfer of Personal Data

8.1.1. Explicit consent of the data subject for the transfer of personal data

Pursuant to Article 8 of the Turkish Data Protection Act, the main rule for the transfer of personal data to third parties is defined as the existence of the explicit consent of the data subject. The personal data of the data subject shall be transferred by the Company to which personal data of the data subject consent to be transferred to third parties in domestic and, the groups of persons to whom the personal data of the data subject will be transferred, shall be carefully determined and processed in the data inventory.

8.1.2. Personal data may be transferred without explicit consent of the data subject provided that conditions concerning processing of personal data are ensured

Where there is no explicit consent of the data subject to transfer their personal data domestically, Personal data can be transferred to third parties under the terms of Article 5, paragraph 2 of the Turkish Data Protection Act defined in the articles 6.2., 6.3., 6.4., 6.5., 6.6., 6.7. and 6.8. of this Policy upon the processing requirements of personal data.

8.1.3. Sensitive Personal data may be transferred without explicit consent of the data subject provided that the transfer conditions has been ensured and it is required by law

Transfer of sensitive personal data other than health and sexual life of to third parties, is possible only as it is foreseen in the legislation and legislative provisions that the processing of personal data can be processed, even if the data subject does not have explicit consent. In this case, the Company may transfer sensitive personal data to third parties by determining that the conditions set out in Article 7 of this Policy have been met. Obligation to take necessary measures for the processing of sensitive personal data is also foreseen for the transfer of these data and, these measures shall be taken by the Company.

8.2. Cross-border Transfer of personal data

8.2.1. Explicit consent of the data subject for the cross-border transfer of personal data

Pursuant to Article 9 of the Turkish Data Protection Act, personal data cannot be transferred cross-border without the explicit consent of the data subject. For this reason, obtaining the explicit consent of the data subject by the Company for the cross-border transfer of personal data , will be applied as the basic principle. The consent of the data subject to which the personal data is allowed to cross-border transfer to third parties, shall be carefully determined by the Company and shall be transferred to the list of safe countries to be published by the Personal Data Protection Authority.

8.2.2. Personal data may be transferred without explicit consent of the data subject provided that conditions concerning processing of personal data are ensured

Where there is no explicit consent of the data subject to cross-border transfer their personal data , Personal data can be cross-border transferred to third parties in under the terms of Article 5, paragraph 2 of the Turkish Data Protection Act defined in the articles 6.2., 6.3., 6.4., 6.5., 6.6., 6.7. and 6.8. of this Policy upon the processing requirements of personal data providing to act in accordance with the list of safe countries to be published by the Personal Data Protection Authority and other methods.

Pursuant to Article 9 of the Turkish Data Protection Act, to cross-border transfer personal, it is necessary to have adequate protection in the country where the data will be transferred. The list of safe countries to be announced by the Authority shall be follow-up by the Company and shall be included in the Company's internal processes. If the personal data should be

transferred cross-border prior the publication of the list of safe countries by the Authority, providing that the Company in the capacity of data controller and person cross-border to whom the data will be transferred are committing to provide sufficient protection and with the approval of the Authority, the personal data shall be transferred cross-border by the company.

In case if there is not sufficient protection in the country where the data will be transferred after the announcement of the list of safe countries published by the Authority, the personal data shall be transferred by the company cross-border providing that the company in the capacity of data controller and the third person to whom the data will be transferred cross-border shall commit to provide sufficient protection and with the approval of the Authority.

9. ERASURE, DESTRUCTION OR ANONYMIZING OF PERSONAL DATA

Even the personal data has been processed in accordance to the Turkish Data Protection Act and other legislative provisions; it shall be erased, destroyed or anonymized by the Company upon the removal of the reasons for processing the data, or at the request of the data subject. The Company, shall establish an administrative and technical structure suitable for all applicable legislative provisions, that will be effective or in force in respect of the erasure, destruction or anonymization of the data.

10. OBLIGATIONS OF THE COMPANY IN THE CAPACITY OF DATA CONTROLLER

10.1. Obligation to Inform

Whilst collecting personal data, the company shall inform the data subject about the following in the direction of Turkish Data Protection Act:

a) The identity of the data controller and of his representative, if any,

b) The purpose of data processing;

c) To whom and for what purposes the processed data may be transferred,

ç) The method and legal reason of collection of personal data,

d) Other rights of the data subject

In order for the Company to fulfill its subject obligations in a lawful manner, business processes and data collection channels are reviewed, identified issues were subjected to a classification and transferred to inventory, necessary regulations have been made in order to make able the data subject to their application rights related to their personal data and, communication channels have been formed.

10.2. Obligation to Secure Personal Data

10.2.1. Obligation to prevent unlawful processing of personal data

In addition to the processing of personal data under the Turkish Data Protection Act and other legislative provisions as well as the principles and conditions set forth in this Policy, the Company is also obliged to take the technical and administrative measures introduced by the legislation in order to prevent the processing of personal data against such obligations.

In this context, the Company has established systems in order to prevent unlawful processing of personal data and have identified the relevant personnel and established their procedures to oversee these systems. The Company shall make updates of the system by following up the up to dates that may occur due to technical reasons as well as for legal reasons.

10.2.1.2. Technical measures for lawful processing of personal data

The personal data processing activities carried out by the Company departments, were analyzed and “Personal Data Processing Inventory" was issued. The administrative structure and hardware and software infrastructure, necessary for the monitoring and control of all processes from collection of personal data to erase, are being established.

10.2.1.2. Administrative measures for lawful processing of personal data

a. In order to inform all personnel about the processing of personal data in accordance with the Turkish Data Protection Act, the Company shall issue and submit the documents and the following documents to all personnel required by this Policy and shall arrange the necessary training activities and keep the participation certificates in their personal files.

b. The Company has added records for all kinds of documents regulating the relationship with its personnel and containing personal data in accordance with the law that it is necessary to comply with the obligations stipulated in the Turkish Data Protection Act, that personal data should not be disclosed, that personal data should not be used illegally and that the obligation of confidentiality pertaining to personal data continues even after the termination of the employment contract with the Company, and the fact that the personnel do not comply with these obligations will subject to sanction to termination.

c. Within the scope of personal data inventory to be created and authorization matrices, the Company restricts access to personal data to the intended personnel for the purpose of processing. All of the Company's personnel shall not be able to access all of the personal data processed by the company in the capacity of data controller, it shall be transacted within the frame of the access power regulated for departments.

ç. All activities of the company were analyzed and personal data processing activities specific to departments were determined. The Company has conducted policies, procedures and other internal regulations to ensure that the operations of the departments are carried out in a manner that fulfills the obligations under the Turkish Data Protection Act and this Policy, and that any updates shall be communicated to the personnel by using all communication

channels. Upon the publication of the update, new procedures and policies come into force and it is not necessary for the updates to be notified to the staff to be binding on them.

10.2.2. Obligation to prevent unlawful access to personal data

10.2.2.1. Technical measures to be taken for the lawful access and protection of personal data

a. The Company will take measures in accordance with technical developments and periodically update and renew the measures taken depending on the speed of development of the technology and test the reliability of the system with penetration tests and other methods. The Company shall undertake all necessary procedures to ensure compliance with these new requirements if the Personal Data Protection Authority makes regulations for such penetration tests and other security measures or refers to technical standards.

b. Access and authorization technical solutions shall be put into use by the Company in accordance with the legal compliance criteria determined by the department and, software and hardware solutions shall be put into practice in order to fulfill the requirements of the measures given in the table of administrative and technical measures issued by the Personal Data Protection Authority.

c. The technical measures taken shall be periodically reported to the related party as per the internal audit mechanism. Risky issues shall be re-evaluated and necessary technical solutions shall be produced.

ç. Including software and hardware, virus protection systems and firewalls, the company shall install all relevant security software and systems to all systems used during the operation and which have access to personal data.

d. The company shall employ technical staff in terms of data security.

e. In order to access personal data in accordance with the law, access rights shall be defined in accordance with the criteria to be taken on the basis of department, access and authorization of user accounts for systems to which personal data will be accessed shall be restricted, and devices that can access the systems shall be restricted.

f. The Company shall ensure that the necessary software and hardware are installed in order to prevent leakage of external data and to monitor potential risks, perform infiltration tests, take the same security measures in terms of backups to prevent data loss, make the necessary agreements to take the security measures brought by third parties and legal persons working under disaster planning and keep the data in accordance with the Turkish Data Protection Act.

10.2.2.2. Technical measures to be taken for the lawful access and protection of personal data

a. All Company personnel shall be provided with training in relation to personal data and technical measures to prevent unlawful access.

b. In line with the personal data processing inventory to be formed, the Company shall limit access to personal data to relevant personnel in line with the purpose of processing. All personnel of the Company shall be prevented from accessing all of the personal data processed by the company in the capacity of data controller, and access privileges should be regulated by taking into account the purpose of data processing.

c. The Company has added to all kinds of documents regulating the relationship with its personnel that, it should be complied with the obligations stipulated in the Turkish Data Protection Act in order to process the personal data in accordance with the law, that personal data should not be disclosed, that personal data should not be used illegally and that the confidentiality obligation pertaining to personal data continues even after the termination of the employment contract with the Company.

d. The Company shall prepare all necessary documents and procedures for access to personal data and submit it to all personnel.

10.2.3. Control of measures to protect personal data

In terms of the technical and administrative measures to be taken by the Company, the Company shall establish systems to carry out the necessary audits regarding the operation of the measures. The results of these audits should be reported to the relevant department within the scope of the Company's internal operation and, necessary actions shall be taken to improve the measures.

Necessary processes should be formed by the company in order to increase awareness and control of departments, business partners and suppliers about the protection and processing of personal data, follow-up of periodic reporting and actions under reports and verification tests and audits shall be performed.

The Company is liable under Article 12 of the Turkish Data Protection Act to ensure that the third parties to whom the personal data was transferred shall lawfully process, maintain and access the personal data in accordance with the provisions of this Policy and Turkish Data Protection Act. For this reason, the Company shall obtain commitments to provide these conditions in all agreements upon transfer of personal data and in all regulations related to the transfer of personal data while transferring personal data to third parties. Again the Company should inform all its personnel in terms of the responsibilities arising from the transfer of personal data to third parties.

11. The Rights of Data Subject

Pursuant to Article 11 of the Turkish Data Protection Act, the data subject has the following rights to the Company in the capacity of data controller:

a) To learn whether his personal data are processed or not, and to request information if his personal data are processed,

b) To learn the purpose of his data processing and whether this data is used for intended purposes,

c) To know the parties to whom his personal data is transferred,

ç) to request the rectification of the incomplete or inaccurate data, if any, and if the conditions are not realized. to request to delete his personal data and to forward this claim to third parties

d) To object for any opposite result against him resulting by analyzing the personal data through individual automatic systems

e) To claim compensation for any losses which may result as unlawful processing

In the event that data subject submits their requests regarding the rights listed above in writing or by other methods determined by the Authority, pursuant to Article 13 of the Turkish Data Protection Act, the Company shall finalize the relevant request as soon as possible and no later than thirty days, depending on the nature of the request. If the demand also requires a cost, the fee to be determined by the Authority will be charged. If it is understood that the application is caused by the Company's fault, the fee shall be returned to the person.

When the related application is finalized by the company, information should be given in a language and format that the data subject can understand and shall be sent to the data subject in writing or electronically in accordance with the person's request, and in absence of such request, in accordance with the method chosen by the Company.

According to the nature of the request, the Company may accept the application of the data subject or reject it by explaining its justification. In case the application is accepted, the Company shall do the required action without delay.

In case the application of the data subject has been refused, or the reply is found to be inadequate or the application is not responded within the deadline, all personnel within the Company should be warned and informed about that he has the right to complain to the Authority within 30 days.

12. ENFORCEMENT AND UPDATES

This Policy shall enter into force on the date of its approval by the Board of Directors of the Company. The necessary changes to be made in the policy and the implementation of these changes shall be made by a governance model to be formed and, the amendments shall enter into force upon the approval of the General Manager.

The policy shall normally be reviewed and updated once a year. However, in case of legislative changes, changes to a referenced technical standard, procedures and/or decisions of the Personal Data Protection Authority and in accordance with court decisions, the Company reserves the right to revise this Policy and, where necessary, to update, change or eliminate and to issue a new policy.

The Board of Directors is authorized to decide on the repeal of the policy.