1. PURPOSE AND SCOPE

This Policy's purpose is to ensure the effective implementation of the regulations within the framework of the fundamental principles set forth by the Law on the Protection of Personal Data ("LPPD") no. 6698, by Fiba Yenilenebilir Enerji Holding A.Ş. and all its affiliates (hereinafter referred to as the "Company").

Planning will be carried out to take the administrative and technical measures set forth by the applicable legislation for the processing and protection of the personal data within the company, the necessary information will be provided to raise awareness and it will be ensured that the necessary measures are taken within the scope of LPPD so that the employees and business partners are able to adapt the LPPD processes.

2. DEFINITIONS

The definitions set forth in the Law on the Protection of Personal Data, which we will use within the scope of certain subjects in this procedure, are as follows:

Personal Data: 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 as to, who, for what purpose and for how long can the different personal data in different categories be processed.

Sensitive Personal Data: 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 of persons.

Processing of Personal Data: 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.

Explicit consent: Freely given, specific and informed consent.

Verbis: Data controllers' registry information system.

Data Controller: 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.

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

Contact Person: The personnel who is responsible for establishing and managing the communications between the Personal Data Protection Authority and the Data Controller, monitoring the processes and conducting other operations.

Data subject: The natural person, whose personal data is processed.

Data Registry System: The recording system in which personal data is configured and processed according to certain criteria.

Recording Medium: Any medium that contains personal data that is processed fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.

Personal Data Processing Inventory: An inventory that the Company creates and details by associating the personal data processing operations carried out by the Company in relation to business processes with; the purposes of processing the personal data, data categories, the recipient group to whom the data is transferred, and the group of data subjects.

Disposal: The erasure, destruction or anonymization of the personal data.

Erasure of the Personal Data: The process of rendering the personal data that is processed fully or partially through automatic means inaccessible and non-reusable for Human Resources.

Destruction: The process of rendering all the recording mediums suitable for data storage, in which the personal data is stored, inaccessible, irretrievable or non-reusable.

Anonymization: The process of rendering the personal data impossible to be linked with an identified or identifiable natural person, even by matching them with other data.

The processing and protection of the personal data and sensitive personal data of our company's natural and legal person clients, legal person business partners, shareholders, directors or employees, company advisors, consultants, solution partners, guests and company personnel will be taken into consideration by our Company within the scope of the LPPD and the Policy.

The process of implementing the decisions and regulation of the Personal Data Protection Board; court verdicts, changes in technical infrastructure and legislation and the personal data protection, processing, storage and disposal processes within the company are monitored by the Human Resources Department. To ensure compliance with the statutory legislation, coordination is established with the Department of Legal Affairs, and planning is carried out with the Department of Data Processing within the scope of technical measures.

3. PRINCIPLES IN PROCESSING OF PERSONAL DATA

The Company agrees to process the personal data under this procedure as per the following principles, in accordance with Article 4 of the LPPD:

- Lawfulness and conformity with rules of bona fides

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 LPPD.

- 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 LPPD, insofar as circumstances permit.

- 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.

- 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.

- 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 erased, 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.

4. CONDITIONS FOR PROCESSING OF PERSONAL DATA

Article 5 of the LPPD, 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 LPPD:

4.1. 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 case of 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 LPPD, upon clarification of the intended purpose for the avoidance of any doubt.

4.2. Data Processing Due to Legal Requirements

Pursuant to the LPPD, data processing activities shall be deemed to be in accordance with the law, provided that other required criteria are fulfilled in cases where it is mandatory to process the personal data in accordance with the provisions of the legislation, even if the data subject does not give their explicit consent.

4.3. It is 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 LPPD 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 the

personal data in accordance with and in cases stipulated in the aforementioned regulation.

4.4. 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 fulfilment of the contract.

4.5. It is Mandatory for the Controller to be Able to Perform His/Her Legal Obligations

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

4.6. The Data Concerned is Made Available to the Public by the Data Subject Himself/Herself

If the personal data is made available to the public by the data subject, the personal data shall be processed by the Company in proportion to the purposes of making it available to the public.

4.7. 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.

4.8. Processing of Personal Data is Mandatory for the Legitimate Interests of the Data Controller

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 expression of the Company's legitimate interests, cannot in any way be in contradiction with the principles of the LPPD as well as the purpose of processing such personal data and, it cannot interfere with the essence of the rights guaranteed by the Constitution.

5. TRANSFER OF PERSONAL DATA

Article 8 of the LPPD regulates the domestic transfer of personal data to third parties. The personal data is shared with the consulting firms, suppliers and business partners with whom the company executes contracts, by obtaining the explicit consent of the personnel. To keep the data confidential, a protocol is drawn up with the relevant consulting firms, suppliers and business partners; and their commitment is obtained not to transfer the data to third parties or organizations or use them for any other purpose, except for the conditions that meet the criteria for transfer as provided for in the main service agreement.

With respect to 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 future legislation.

5.1. Conditions for the Processing of Sensitive Personal Data

Unless required to exercise certain rights or fulfill certain obligations arising from the labor codes or legislation,

and except for the cases authorized and permitted under the applicable legislation, it is always necessary to obtain the explicit consent and permission of the data subject before processing the Sensitive Personal Data.

5.2. Domestic Transfer of Personal Data

5.2.a Explicit consent of the data subject is obtained for the transfer of personal data

Pursuant to Article 8 of the LPPD, 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, by carefully determining and entering into the data inventory the groups of persons to whom the personal data of the data subject will be transferred, and the specific data categories to which the data subject gives consent for domestic transfer to third parties.

5.2.b. Personal data may be transferred without explicit consent of the data subject provided that conditions concerning the 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 LPPD and as defined in the articles 4.2., 4.3., 4.4., 4.5., 4.6., 4.7. and 4.8. of this Procedure regarding the processing requirements of personal data.

5.3. The Rules to be Followed in Processing the Personal Data of the Personnel and Candidate Personnel

In order for the personal data of the Company personnel to be processed in accordance with the Labor Code and other relevant legislation, all the personnel have already signed the "FEH.DD.04 Personal Data Protection Protocol".

By quoting the relevant clause of the Law on the Protection of Personal Data no. 6698 in FEH.FR.22 Job Application Form, it was guaranteed that the personal data relating to the candidates who are in the process of recruitment will be kept confidential by our Company.

5.4. Guidelines for the Processing and Use of the Personal Data of Customers for Marketing Purposes

In order to directly or indirectly acquire and process the personal data of customers, the explicit consent of the customer is obtained before the acquisition of personal data. In the absence of explicit consent, it is possible to process the personal data under the terms of Article 5, paragraph 2 of the LPPD and as defined in the articles 4.2., 4.3., 4.4., 4.5., 4.6., 4.7. and 4.8. of this Procedure regarding the processing requirements of personal data.

6. LEGAL REASONS THAT REQUIRE RETENTION

Fiba Yenilenebilir Enerji Holding and affiliates store the personal data processed within the framework of business activities for the retention periods stipulated in the relevant legislation.

- Labor Code no. 4857
- Turkish Code of Obligations no. 6098
- Social Security and General Health Insurance Law no. 5510
- Occupational Health and Safety Code no. 6361
- Turkish Code of Commerce no. 6102
- Consumer Protection Law no. 6502

6.1. Purposes of Processing That Require Retention

The personal data acquired directly or indirectly for the purposes of conducting the Company's following operations may be saved, retained, updated within the framework of the following conditions or disclosed, transferred to 3rd parties to the extent allowed by the legislation, classified and processed as provided for in the LPPD.

- Managing Human Resources processes,
- Ensuring the organization's security,
- Legal reporting,
- Conducting the wholesale and retail sales activities for electricity

The Company may collect personal data from parties such as customers, employees, candidate employees, business partners and suppliers, in categories such as identification, contact information, customer information, customer transaction information, transaction security information, legal transaction and compliance information.

The personal data collected will be processed within the framework of the conditions and purposes of processing of personal data as specified in articles 5 and 6 of the Law no. 6698, in line with the purposes listed below:

- Fulfilling the purposes of processing as stated in the clarification text and providing services to customers, fulfilling obligations towardsthe customers, organizing records and documentation, complying with the information retention, reporting, briefing, auditing and other obligations stipulated by the local and international statutory legislation,

- Data processing requirements, system infrastructure, the necessity of the data processing services and communicating for the purpose of transmitting the necessary information to the data subjects in connection with these services and products,

- Measuring and increasing customer satisfaction, managing complaints, obtaining your opinions and suggestions regarding the services, obtaining issue-error notifications, providing information on the products and services, complaints and requests,

- Carrying out payment transactions, ensuring that the information texts are transmitted by establishing a logistics cooperation with 3rd parties,

- Reviewing, evaluating and responding to the requests received from official authorities or data subjects.

7. THE COMPANY'S OBLIGATIONS AS THE DATA CONTROLLER

7.1. Obligation to Inform

While collecting the personal data, the Company shall inform the data subject about the following matters in accordance with article 10 of the LPPD:

a. The identity of the 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 were reviewed, identified issues were subjected to a classification and transferred to the inventory. Necessary briefing plans were created so that the data subjects can exercise their rights of application related to their personal data.

7.2. Obligation to Secure Personal Data

7.2.1. Obligation to prevent the unlawful processing of personal data

The Company takes the necessary technical and administrative measures to ensure the security of the personal data. In addition, the company will ensure planning to take the necessary measures for the purpose of preventing the processing of personal data in violation of the obligations set forth in the LPPD and this procedure.

7.2.2. TECHNICAL AND ADMINISTRATIVE MEASURES

The Company takes technical and administrative measures pursuant to the Law on the Protection of Personal Data to ensure the storage of personal data in a secure manner, prevent the unlawful processing of and access to personal data and ensure lawful disposal of the personal data.

7.2.2.1 Technical Measures

- ✓ Network security and application security is ensured.
- ✓ A closed-circuit line is used between the Istanbul office and the data center.
- ✓ Firewall, Ips, Ddos and waf services are used against possible external attacks.
- ✓ The necessary software is used for end-user PC security.
- ✓ A firewall structure is available in the central office for Internet traffic and access rules.
- ✓ If the sensitive personal data is to be communicated via electronic mail, they are always sent in encrypted form and using the KEP or corporate e-mail account.
- ✓ Studies are conducted through the Holding in order to identify the existing risks and threats.
- ✓ Studies for pentest are conducted.
- ✓ Data loss prevention software is used.

The Company will conduct planning to take measures that are suitable for the technological developments and if the system is installed, it will update and upgrade the system periodically, organize efforts to test the system's reliability by way of pentests and other methods. If the Company installs this system, and the Personal Data Protection Board sets forth regulations in relation to such pentests and other security measures or refers to technical standards, necessary efforts to ensure compliance with these new requirements will be planned out. The Company will plan out the provision of necessary hardware and software to prevent penetration into the systems that store personal data and to monitor potential risks.

7.2.2.2 Administrative Measures

- ✓ There is a "Personal Data Protection Protocol" that contains data security provisions for the employees.
- ✓ Planning is being done for informative mails that will raise awareness among the personnel regarding data security on a periodic basis.
- ✓ The contracts signed include data security provisions.
- ✓ For personal data transmitted through print media, extra security measures are taken and the relevant documentation are transmitted in the form of classified documents.

- ✓ The personal documents, medical documents or any kind of documents containing personal data are stored in password-protected and locked cabinets by the Human Resources department.
- ✓ Access to documents stored on digital environments is not possible without a password. The password is controlled only by the Human Resources department.
- ✓ The data processing Human Resources personnel undertake that they will process the data in accordance with the laws by signing the "Letter of Commitment to be Signed by Critical Personnel" as prepared by the Personal Data Protection Board.

In order for all the personnel to be informed regarding the processing of personal data according to the law and the LPPD, the Company will draft this procedure and then the documents that will be necessary in the future, and will send them to each employee via the QDMS system or an information e-mail. The current version of this procedure is kept on the QDMS portal, which is open for access by all the personnel.

Any changes in the legislation, and changes that may occur due to the decisions of the Board or court verdicts as notified to the Company, are monitored by the Contact Person. The necessary changes are implemented as promptly as possible after the occurrence of said change.

8. RIGHTS OF THE DATA SUBJECT

Pursuant to Article 11 of the LPPD, the "data subject" has the following rights against the Company in the capacity of Data Controller:

a. To learn whether his/her personal data are processed or not, and to request information if his/her 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/her personal data is transferred,

ç. To request the rectification of the incomplete or inaccurate data, if any, and if the conditions are fulfilled, to request the erasure of his/her personal data and the forwarding of this request to third parties,

d. To object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavorable consequence for the data subject,

e. To claim compensation for any losses which may result from unlawful processing.

If the data subjects communicate their requests in connection with the rights listed above to the company, the Company must finalize this request as soon as possible depending on its nature pursuant to article 13 of the LPPD.

9. PERSONAL DATA BREACH AND STEPS TO BE TAKEN IN CASE OF A BREACH

9.1. Personal Data Breach

Notwithstanding whether the data is kept on manual or automatic systems, circumstances that will lead to unauthorized persons accessing personal data that requires authorization to access, removing the Company's control on such data, making such data inaccessible by the Company, sending the data to another location, copying, erasing or subjecting the data to similar actions or other actions that will lead to the possibility of these actions being performed, and the loss of data or the data being acquired by unauthorized persons as a result of the omissions and negligence of the authorized persons.

The following examples can be given for such actions:

- Computers, tablets, memory cards or other devices that contain personal data being stolen or getting lost
- Theft of data due to the use of a simple/unsecure password
- The personal data of the customers mistakenly being sent to an unauthorized person
- Access by persons who are not authorized to access data processing systems, an unauthorized person being granted access authorization

9.2. Steps to be Taken in Case of Data Breach

An actual, suspected or potential Personal Data Breach must be reported by the person who first realized situation, depending on the contents of the data, to the Human Resources Directorate in case of Personnel data, or directly to the Directors of the relevant Departments in case of customer data and other personal data and/or to the Data Processing Department and the Department of Legal Affairs.

The department directors as data subjects will evaluate the Personal Data Breach and the degree of risk associated with such breach. As a result of this evaluation, following a risk assessment to be carried out in consideration of the scale and sensitivity of the breach, the number of the data subjects affected and similar matters, a report will be submitted to the relevant management regarding the internal measures to be taken in connection with the breach, and similarly as a result of the risk assessment, if a decision is made to submit the necessary warnings, notifications and applications to the prosecutor's office, to the Personal Data Protection Board or to other judicial authorities and administrative authorities, the matter will be referred to the office of the legal counsellor, accompanied by all the relevant evidence and the necessary legal and administrative applications will be filed.

Following these steps, the directors of the relevant departments will prepare and submit a report to the management in regard to the technical and administrative measures to be taken and the changes to be made to the contents of the procedure to prevent the reoccurrence of the breach in the future.

9.3. Recording Data Loss Events

All personal data breaches will be recorded. This record will contain information such as the date and time of the event, a description of the breach, the location of the breach, the personal data affected by the breach and the scale of the breach. The recorded information will be retained by the relevant Department.

10. ERASURE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

At the end of the retention period stipulated by the relevant legislation or required for the purposes of processing, the personal data is disposed of according to the periodic disposal periods or as per the application of the data subject, similarly in accordance with the provisions of the relevant legislation.

9.1. Destruction of Personal Data

a. Erasure/Destruction of Personal Data on Electronic Media: The personal data on electronic media, for which the requisite retention period has expired, will be erased in a way that renders them inaccessible and non-reusable by any means.

b. Erasure/Destruction of Personal Data on Physical Media: The personal data on physical media, for which the requisite retention period has expired, are rendered inaccessible and non-reusable by any means.

After destroying the data on digital and physical media, the relevant Disposal Reports are signed by the officials named on the report and this report is retained by Human Resources for a period of 3 years.

Following the notification of the board or a court, regardless of the periodic auditing intervals, the Human Resources department complies with the decision/notice. The decisions on the warrants served by the board or the court are implemented immediately, or the possibility of exercising legal remedies such as going for an appeal or raising objections are taken into consideration and actions are taken accordingly.

9.2. Anonymization of Personal Data

Anonymization is the process of rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.

To anonymize the personal data, personal data shall be rendered impossible to relate to identified or identifiable person, even through using appropriate techniques in respect of the recording medium and relevant field of activity, such as recovery of data by the data controller or third parties and/or matching the data with other data.

11. DUTIES AND RESPONSIBILITIES OF THE PERSONS WHO ARE INVOLVED IN THE RETENTION AND DISPOSAL OF PERSONAL DATA

Human Resources, which is responsible for the retention and disposal process of the personal data of the Company personnel and the officials of the relevant Departments, who are responsible for the customer data, are responsible for performing the following duties:

- Ensuring and monitoring the implementation of this procedure,
- Monitoring changes that may occur in the legislation and circumstances such as court verdicts,
- Monitoring and reviewing the work schedules created for data retention and disposal, auditing the compliance of actions performed within the framework of the work schedules with this procedure, and in case non-conformities are detected, ensuring that they are aligned with this procedure,
- Receiving or accepting the notices or correspondences sent by the organization on behalf of the data controller,
- Receiving the requests forwarded by the organization to the data controller on behalf of the data controller and conveying the replies to the Organization,
- In the absence of any other guidelines set by the Board, receiving the applications to be directed by the data subjects towards the data controller on behalf of the data controller as per the first sub-paragraph of article 13 of the Law,
- In the absence of any other guidelines set by the Board, conveying the replies of the data controller to the data subjects as per the third sub-paragraph of article 13 of the Law,
- Carrying out the processes and procedures related to the Registry on behalf of the data controller,
- Entering the contact person information into the registry during the registration process on behalf of the data controller,

The Contact Persons who are responsible for processing, retaining and disposing of customer data are obligated to comply with the foregoing duties and responsibilities.

11. PERSONAL DATA RETENTION AND DISPOSAL PERIODS

❖ The medical and safety records of the Company personnel must be retained for 15 years, pursuant to article 7/1-b of the Regulation on Occupational Health and Safety Services. With this said, pursuant to the relevant provisions of the Social Security and General Health Insurance Law no. 5510, other personal data of the Company personnel aside from medical and safety records are retained for 10 years. The personnel records are retained throughout the term of their employment. Documents related to candidate employees such as job application forms etc. are retained for 2 years.

❖ The Company is obligated to present all kinds of information and documents to be requested during the audits within the framework of the Commercial Code and relevant regulations, submit books and documentation and make them available for inspection, and retain all the information and documentation relating to the Company's transactions for 10 years.

❖ With this said, as the receivables are subject to a statute of limitations for 10 years pursuant to article 146 of the Code of Obligations no. 6098 and since there is a 10-year mandatory retention period for the documents pursuant to article 82 of the Turkish Code of Commerce no. 6102, the personal data is retained for a period of 10 years starting from the date of the last transaction in order to allow the Data Controller to fulfill their legal obligations, protect their legitimate interests and to present the documents to the judicial authorities if the need arises.

❖ Personal data obtained from support services companies, corporate customers and suppliers is retained for a period of 10 years starting from the date of the last transaction, in order to allow the Corporate Customer / Company in the capacity of Data Controller to fulfill their legal obligations, protect their legitimate interests and to present the documents to the judicial authorities if the need arises, as the receivables are subject to a statute of limitations for 10 years pursuant to article 146 of the Code of Obligations no. 6098 and since there is a 10-year mandatory retention period for the documents pursuant to article 82 of the Turkish Code of Commerce no. 6102.