ENERJİSA ÜRETİM SANTRALLERİ A.Ş.

AND ITS AFFILIATES

(“ENERJİSA” or the “COMPANY”)

SPECIAL CATEGORIES OF PERSONAL DATA PROTECTION AND PROCESSING POLICY

(“SPECIAL CATEGORY PDP POLICY”)

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

Enerjisa, which has adopted the utmost diligence in complying with the legal order throughout its history, establishes the necessary systems to carry out all activities required for compliance with the legislation on the processing and protection of personal data.

The Company's Personal Data Protection Policy ("Company PDP Policy") sets out the principles adopted by the Company in the protection and processing of personal data.

In line with the importance the Company places on personal data protection, the Company PDP Policy establishes the fundamental principles to ensure compliance of the Company's activities with the provisions of the Law No. 6698 on the Protection of Personal Data ("PDP Law"). The implementation of the provisions of the Company PDP Policy ensures the sustainability of the data security principles adopted by the Company.

The Company PDP Policy applies to natural persons whose personal data are processed by the Company through automatic means or by non-automatic means provided that they are part of a data recording system. However, matters concerning the protection of the personal data of Company employees are regulated separately under the "Company Employee Personal Data Protection and Processing Policy".

2. OBJECTIVE

The objective of the Company PDP Policy is to establish the necessary structure and regulations to ensure compliance with the legislation and raise awareness within the Company regarding the lawful processing and protection of personal data. In this context, the Company PDP Policy serves as a guiding document for the implementation of the provisions introduced by the PDP Law and relevant legislation.

3. DEFINITIONS

Şirket KVK Politikası' nda kullanılan ve önem teşkil eden tanımlar aşağıda yer almaktadır:

Explicit Consent	Consent that is related to a specific subject, based on information, and freely given.
Anonymization	Rendering personal data incapable of being associated with an identified or identifiable natural person, even by means of matching it with other data.
Communiqué on the Principles and Procedures to be Followed in	The communiqué published in the Official Gazette dated March 10, 2018 and numbered 30356.

Fulfillment of the Obligation to Inform	
Employee(s)	Company employee(s).
Employee PDP Policy	The "Company Employee Personal Data Protection and Processing Policy," which sets out the principles concerning the protection and processing of Company employees' personal data.
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDINGS S.A.R.L. (briefly referred to as "E.ON").
Regulation on Personal Health Data	The Regulation on Personal Health Data published in the Official Gazette dated June 21, 2019 and numbered 30808.
Personal Health Data	All kinds of information related to the physical and mental health of an identified or identifiable natural person, as well as information regarding the health services provided to such person.
Personal Data	Any information relating to an identified or identifiable natural person.
Data Subject	The natural person whose personal data are processed.
Personal Data Protection Committee	The internal Company committee responsible for ensuring, maintaining, and coordinating compliance with the personal data protection legislation.
Processing of Personal Data	Any operation which is performed on personal data, wholly or partly by automatic means, or otherwise as part of a data recording system, such as collection, recording, storage, preservation, alteration, reorganization, disclosure, transfer, acquisition, making available, classification, or preventing the use thereof.
PDP Law	The Law on the Protection of Personal Data No. 6698, published in the Official Gazette dated April 7, 2016 and numbered 29677.
PDP Board	The Personal Data Protection Board.
PDP Authority	The Personal Data Protection Authority.
PDP Compliance Program	The compliance program enacted by the Company for ensuring adherence to the legislation on the protection of personal data.
Special Categories of Personal Data	Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, health, sexual life,

	criminal convictions and security measures, as well as biometric and genetic data.
Company	Enerjisa Üretim Santralleri Anonim Şirketi and its affiliates.
Company Business Partners	Parties with which the Company forms business partnerships for various commercial purposes.
Company Personal Data Retention and Destruction Policy	The "Company Personal Data Retention and Destruction Policy," which serves as the basis for determining the maximum retention period of personal data processed for their intended purpose and for the deletion, destruction, or anonymization of personal data, in accordance with the Regulation on the Deletion, Destruction, or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017 and numbered 30224.
Company PDP Policy	The Company Personal Data Protection and Processing Policy.
Company Suppliers	Parties providing services to the Company based on contractual arrangements.
Company Data Subject Application Form	The application form to be used by data subjects in exercising their rights under Article 11 of the PDP Law.
Sabancı Group Employee PDP Policy	The "Sabancı Group Employee Personal Data Protection and Processing Policy," which sets out the principles adopted regarding the protection and processing of personal data of employees within the Sabancı Group.
Sabancı Group PDP Policy	The "Sabancı Group Personal Data Protection and Processing Policy," which sets out the principles adopted by the Sabancı Group regarding personal data protection and processing.
Sabancı Group Companies / Group Companies	All companies under the umbrella of the Sabancı Group.
Constitution of the Republic of Türkiye	The Constitution of the Republic of Türkiye dated November 7, 1982 and published in the Official Gazette dated November 9, 1982 and numbered 17863.
Turkish Penal Code	The Turkish Penal Code No. 5237, dated September 26, 2004 and published in the Official Gazette dated October 12, 2004 and numbered 25611.
Data Processor	The natural or legal person who processes personal data on behalf of the data controller based on the authorization granted by the latter.

Data Controller	The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.
Communiqué on the Principles and Procedures for Application to the Data Controller	The communiqué published in the Official Gazette dated March 10, 2018 and numbered 30356.

4. ROLES AND RESPONSIBILITIES AND THE PERSONAL DATA PROTECTION COMMITTEE

The "Personal Data Protection Committee" has been established within the Company to ensure, maintain, and coordinate compliance with the legislation on personal data protection. The Committee consists of at least four members, including the Group Director of People and Culture, the Group Director of Information Technologies, the Legal Counsel, and a Senior Legal Counsel. The Committee is responsible for ensuring consistency among Company units and departments, and for executing and improving the systems established to ensure compliance of the Company's operations with personal data protection legislation. The procedures of the Committee have been determined through internal regulations.

The primary duties of the Personal Data Protection Committee are as follows:

- To foster a corporate culture that supports the protection and processing of personal data,
- To prepare and enact fundamental policies on the protection and processing of personal data,
- To determine how the implementation and supervision of personal data protection policies will be carried out, assign internal roles accordingly, and ensure coordination
- To identify necessary measures to ensure compliance with the PDP Law and related legislation; monitor implementation and ensure coordination,
- To identify necessary measures to ensure compliance with the PDP Law and related legislation; monitor implementation and ensure coordination,
- To identify potential risks in the Company's data processing activities and ensure appropriate precautions are taken; propose improvements,
- To design and oversee training programs related to the protection and processing of personal data,
- To make final decisions on data subject applications at the highest level,

- To coordinate information and training activities to inform data subjects about the Company's data processing activities and their legal rights (These efforts are carried out in accordance with the "Personal Data Security Guide" published on the official website of the PDP Board),
- To prepare and enact amendments to core policies regarding data protection and processing,
- To monitor developments and regulations concerning data protection and provide guidance to senior management on necessary adjustments to Company operations,
- To manage relations with the PDP Board and PDP Authority,
- To carry out other duties assigned by Company management related to personal data protection.

Each business unit that processes personal data, particularly the People and Culture and Information Technologies departments, is responsible for ensuring the security, processing, erasure, and transfer of personal data, as well as compliance with obligations such as data security, information provision, and obtaining explicit consent imposed on data controllers. While the Personal Data Protection Committee is responsible for the implementation of the Company PDP Policy across all Company operations, activities, and processes, the Legal Department shall act as the advisor and guide for the implementation of regulations, procedures, guidelines, standards, and training activities aligned with the Company PDP Policy. All employees, stakeholders, visitors, and relevant third parties across the Company are obliged to comply with the Company PDP Policy and to collaborate with the Legal Department in order to mitigate legal risks and imminent threats. All departments and organs of the Company are responsible for ensuring compliance with the Company PDP Policy.

5. PRINCIPLES OF THE COMPANY PDP POLICY

5.1. Scope of the Company PDP Policy

Within the scope of the Company PDP Policy, the data subjects whose personal data are processed by the Company are categorized as follows:

- Company Job Applicants
  Individuals whose employment contracts have not yet been concluded with the Company but are under consideration for potential recruitment.
- Relatives of Employees
- Consultants
- Company Business Partners, Their Representatives, Employees

Natural person representatives, shareholders, and employees of entities with which the Company maintains commercial relations.

- Company Visitors

  Persons visiting the Company's premises or websites operated by the Company.

- Other Persons

  All individuals who are not covered under the Company Employee Personal Data Protection and Processing Policy.

5.2. LEGAL GROUNDS AND PURPOSES FOR PROCESSING PERSONAL DATA IN THE COMPANY'S BUSINESS ACTIVITIES

Pursuant to Articles 5(2) and 6(3) of the PDP Law, the Company processes personal data only based on the legal grounds specified therein. (See Section 6.1 for further detail.)

Before processing personal data, the Company verifies the existence of a legal basis. If no legal basis is found, the Company obtains explicit consent from the data subjects prior to processing.

Under the conditions stated above, the Company may process personal data for, but not limited to, the following purposes:

	PURPOSE
1	Conducting Training Activities
2	Managing Employee Applicant / Intern / Student Selection and Placement Processes
3	Handling Applicant Registration Processes
4	Performing Finance and Accounting Operations
5	Conducting Procurement of Goods/Services
6	Executing Contractual Processes
7	Disclosing Information to Authorized Persons, Agencies, or Institutions
8	Conducting Internal Audit / Investigation / Intelligence Activities
9	Implementing Audit / Ethics Activities
10	Ensuring Physical Facility Security
11	Ensuring the Security of Data Controller Operations
12	Carrying Out Occupational Health and Safety Activities
13	Performing and Auditing Business Operations
14	Ensuring Regulatory Compliance of Activities

15	Managing Information Security Processes
16	Recording and Tracking Visitor Entries
17	Managing Events and Organizational Activities
18	Carrying Out Business Continuity Measures
19	Conducting Communications Activities
20	Managing and Conducting Legal Affairs
21	Executing Emergency Management Processes
22	Receiving and Evaluating Suggestions to Improve Business Processes
23	Managing Requests and Complaints
24	Conducting Corporate Social Responsibility and Civil Society Activities
25	Managing Access Authorization Processes

6. PRINCIPLES ADOPTED BY THE COMPANY FOR THE PROCESSING AND PROTECTION OF PERSONAL DATA

6.1. Compliance of Personal Data Processing Activities with Legal Requirements

When processing personal data, the Company strictly adheres to: (i) general data protection principles, (ii) conditions for processing personal data, and (iii) conditions for processing special categories of personal data.

6.1.1. Compliance with Fundamental Principles

To ensure compliance with the personal data protection legislation and maintain such compliance, the Company adopts the following fundamental principles:

(1) Processing Personal Data in accordance with Lawfulness and Fairness

The Company processes personal data lawfully and fairly, in compliance with the Turkish Constitution and applicable data protection legislation.

(2) Ensuring Accuracy and Currency of Processed Personal Data

The Company takes all necessary administrative and technical measures to ensure the accuracy and currency of personal data, to the extent technically feasible. Mechanisms are in place to enable data subjects to request correction or verification of inaccurate information.

(3) Processing Personal Data for Specified, Explicit, and Legitimate Purposes

The Company processes personal data only for purposes that are specified, clear, and lawful prior to the commencement of the processing activity.

(4) Limiting Personal Data Processing to Purpose-Related, Adequate, and Proportionate Means

The Company processes personal data only to the extent necessary and in connection with the applicable legal grounds for processing and the fulfillment of the relevant services. In this context, the purpose of processing personal data is determined before initiating any data processing activity, and data are not processed based on the assumption that they may be useful in the future. Prior to initiating any personal data processing activity, the method set forth in the Personal Data Processing Necessity and Proportionality Test Procedure is followed to assess whether the processing is necessary, and if so, the required actions are identified and implemented according to the nature of the data.

(5) Retaining Personal Data Only for the Time Required by Law or Purpose

The Company retains personal data for the period stipulated under the applicable legislation, or if no such retention period is specified, for as long as is necessary in connection with the service provided at the time the data are processed, in accordance with Company practices, requests from relevant authorities due to the Company operating in a regulated sector, and commercial customs. In this regard, upon the expiration of the period prescribed by legislation or the elimination of the reasons requiring the processing of personal data, the data are deleted, destroyed, or anonymized by the Company. The rules governing this matter are set forth in the Company's Personal Data Retention and Destruction Policy.

6.1.2. Compliance with Personal Data Processing Requirements

The Company carries out its personal data processing activities in accordance with the data processing conditions set forth in Article 5 of the KVK Law. In this context, the personal data processing activities carried out are carried out in the presence of the personal data processing conditions listed below:

(1) Existence of the Explicit Consent of the Personal Data Owner

Personal data processing activities are carried out by the Company if the data owner consents to the processing of data related to him/her, freely, with sufficient knowledge on the subject, in a clear manner that leaves no room for hesitation and limited to that transaction only.

(2) Personal Data Processing Activity is Clearly Stipulated in the Laws

In the event that there is a clear regulation in the laws regarding personal data processing activity, personal data processing activities may be carried out by the Company limited to the relevant legal regulation.

(3 Failure to Obtain the Explicit Consent of the Data Owner Due to Actual Impossibility and Mandatory Personal Data Processing

In cases where the personal data owner cannot disclose his/her consent or his/her consent is not valid, if the processing of personal data is mandatory for the protection of the life or physical integrity of the persons, data processing activities are carried out by the Company in this context.

(4) Personal Data Processing Activity is Directly Related to the Establishment or Performance of a Contract

In cases that are directly related to the establishment or performance of a contract, if it is necessary to process the personal data of the parties to the contract, data processing activities are carried out by the Company.

(5) It is Mandatory to Carry Out Personal Data Processing Activities for the Company to Fulfill Its Legal Obligation

In the event that the Company, which has adopted the necessary sensitivity to comply with the law as the Company's policy, has a legal obligation, personal data processing activities are carried out in order to fulfill the legal obligation.

(6) Publicization of Personal Data by the Data Owner

Personal data made public (disclosed to the public in any way) by the company is processed by the person concerned in accordance with the purpose of making it public.

(7) Data Processing is Mandatory for the Establishment, Exercise or Protection of a Right

In the event that the processing of personal data is mandatory for the establishment, exercise or protection of a right, personal data processing activities are carried out by the Company in parallel with this obligation.

(8) Provided that it does not harm the fundamental rights and freedoms of the Data Owner, the Execution of Personal Data Processing Activity is Mandatory for the Legitimate Interests of the Company

In the event that personal data processing is mandatory for the legitimate interests of the Company, data processing activity may be carried out if the fundamental rights and freedoms of the data owner will not be harmed. In this context, in order to determine the existence of

the said condition, the "balance test" accepted by the Company in the regulation is carried out.

6.1.3. Compliance with Sensitive Personal Data Processing Requirements

The Company attaches special importance to the processing of sensitive personal data, which carries the risk of creating discrimination when they are processed unlawfully. In this context, in the processing of sensitive personal data by the Company, first of all, it is determined whether the data processing conditions exist, and the data processing activity is carried out after making sure that the condition of compliance with the law exists. The technical and administrative measures taken by our Company for the protection of personal data are taken within the scope described in the Policy on the Protection and Processing of Sensitive Personal Data within the framework of the adequate measures stipulated in the Board's Decision dated 31/01/2018 and numbered 2018/10 in terms of sensitive personal data, and the studies carried out in this direction are monitored and audited within the framework of the audits carried out within our Company.

Detailed rules on this subject are announced in the Policy on the Protection of Sensitive Personal Data.

Sensitive personal data can be processed by the Company in the following cases, provided that adequate measures determined by the KVK Board are taken:

a) Having the explicit consent of the person concerned,

b) It is clearly stipulated in the laws,

c) It is mandatory for the protection of the life or bodily integrity of the person who is unable to express his consent due to actual impossibility or whose consent is not legally valid.,

ç) Regarding the personal data made public by the person concerned and in accordance with the will to make it public,

d) It is mandatory for the establishment, exercise or protection of a right,

e) It is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and planning, management and financing of health services by persons or authorized institutions and organizations under the obligation of confidentiality.,

f) It is mandatory for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance,

g) Foundations, associations and other non-profit organizations or formations established for political, philosophical, religious or trade union purposes, provided that they comply with the legislation and purposes to which they are subject, limited to their fields of activity and not

disclosed to third parties; It is aimed at current or former members and members or persons who are in regular contact with these organizations and formations.

6.1.4. Compliance with Personal Data Transfer Terms

In the personal data transfers to be carried out by the company, we act in accordance with the personal data transfer conditions regulated in Articles 8 and 9 of the KVK Law.

(1) Domestic Transfer of Personal Data

Pursuant to Article 8 of the KVK Law, the Company acts in accordance with the data processing conditions and by taking the necessary security measures in the data transfer activities to be carried out in the country.

Even without the consent of the person concerned, if one or more of the following data processing conditions ("Data Processing Conditions") are present, personal data may be transferred to third parties by taking due care and taking all necessary security measures, including the methods stipulated by the Board:

- The relevant activities regarding the transfer of personal data are clearly stipulated in the laws,

- The transfer of personal data by the Company is directly related and necessary for the establishment or performance of a contract,

- The transfer of personal data is mandatory for our Company to fulfill its legal obligation,

- Provided that personal data has been made public by the person concerned, the transfer of personal data by our Company in a limited manner for the purpose of making it public,

- The transfer of personal data by the Company is mandatory for the establishment, exercise or protection of the rights of the Company or the person concerned or third parties,

- Provided that it does not harm the fundamental rights and freedoms of the person concerned, it is obligatory to carry out personal data transfer activities for the legitimate interests of the Company,

- It is mandatory for the protection of the life or physical integrity of the person who is unable to express his consent due to actual impossibility or whose consent is not legally valid,

(2) Transfer of Personal Data Abroad

In accordance with Article 9 of the KVK Law, one of the following situations must exist in order for personal data to be transferred abroad by the company;

1. In the event that at least one of the conditions for processing personal or sensitive personal data exists and there is an adequacy decision about the country to which the personal data will be transferred, the sectors within the country or international organizations, the transfer

abroad can be made by the data controllers and data processors. The adequacy decision will be made by the KVKK Board.

2. In the absence of a adequacy decision;

- ❖ The existence of at least one of the conditions for processing personal or sensitive personal data,
- ❖ Having the opportunity to exercise the rights of the person concerned and to apply for effective legal remedies in the country of transfer, and
- ❖ Provision of one of the appropriate safeguards

Must.

Appropriate Safeguards are listed below:

- ➢ Binding company rules approved by the Board, which include provisions on the protection of personal data, which are obliged to be complied with by the companies within the group of undertakings engaged in joint economic activities,
- ➢ Authorization of the transfer by the Board with a written undertaking containing provisions to provide adequate protection
- ➢ Existence of a standard contract announced by the Board,

The standard must be notified to the Board by the data controller or data processor within 5 working days from the signing of the contract.

Personal data may be transferred to Microsoft's data centers by taking the necessary security measures as a result of the use of Microsoft Office 365 applications by the Company. These data centers are located in the countries in the relevant link, especially in EU countries and the United States. [1] Data hosted in Microsoft datacenters is not technically accessible to third parties, including Microsoft, due to the encryption methods used. In the event that Microsoft engineers need access to data for any technical reason, it is not technically possible to access it in cases where Enerjisa Üretim does not allow it[2].

(3) Transfer of Sensitive Personal Data

Sensitive personal data may be transferred by our Company in accordance with the principles specified in this Policy and by taking administrative and technical measures with the methods

[1] Microsoft's datacenter location, country information and which of these data centers are used for access to Turkey can be found at https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations.

[2] Veri erişimi ihtiyacını, Enerjisa Üretim inisiyatifi ve iznine bağlı kılan Customer Lockbox özelliği platformumuzda aktif durumdadır. Teknolojinin detaylarına https://social.technet.microsoft.com/wiki/contents/articles/35748.office-365-what-is-customer-lockbox-and-how-to-enable-it.aspx adresinden ulaşılabilir.

described in the Policy on Protection and Processing of Sensitive Personal Data and in the presence of the following conditions:

- Having the explicit consent of the person concerned,
- It is clearly stipulated in the laws,
- It is mandatory for the protection of the life or bodily integrity of the person who is unable to express his consent due to actual impossibility or whose consent is not legally valid.,
- Regarding the personal data made public by the person concerned and in accordance with the will to make it public,
- It is mandatory for the establishment, exercise or protection of a right,
- It is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and planning, management and financing of health services by persons or authorized institutions and organizations under the obligation of confidentiality.,
- It is mandatory for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance,
- Foundations, associations and other non-profit organizations or formations established for political, philosophical, religious or trade union purposes, provided that they comply with the legislation and purposes to which they are subject, limited to their fields of activity and not disclosed to third parties; It is aimed at current or former members and members or persons who are in regular contact with these organizations and formations.

6.2. DISCLOSURE OF PERSONAL DATA OWNERS BY THE COMPANY

In accordance with Article 10 of the KVK Law and the Communiqué on the Procedures and Principles to be Followed in the Fulfillment of the Obligation to Inform, the Company carries out the necessary processes to ensure that data owners are informed during the acquisition of personal data. In this context, the information listed below is contained in the clarification texts submitted by the Company to the data owners:

(1) The title of our company,

(2) For what purpose the personal data of the data owners will be processed by the Company,

(3) To whom and for what purpose the processed personal data can be transferred,

(4) The method and legal reason for collecting personal data,

(5) Rights of the data subject.

6.3. FINALIZATION OF REQUESTS OF PERSONAL DATA OWNERS BY THE COMPANY

In the event that data owners submit their www.enerjisauretim.com.tr requests regarding their personal data to our Company in writing or by other methods determined by the KVK Board, the Company, as the data controller, carries out the necessary processes to ensure that the request is concluded as soon as possible and within thirty (30) days at the latest, in accordance with Article 13 of the KVK Law. Data owners should make their requests regarding their personal data in accordance with the Communiqué on the Procedures and Principles of Application to the Data Controller and the Procedure for Receiving, Evaluating and Responding to Data Owner Applications.

Within the scope of ensuring data security, the Company may request information in order to determine whether the applicant is the owner of the personal data subject to the application. Our company may also ask questions to the personal data owner about the application in order to ensure that the application of the personal data owner is concluded in accordance with the request.

The application of the data owner; In cases where there is a possibility of preventing the rights and freedoms of other persons, requiring disproportionate effort, and the information is public information, the request may be rejected by the Company by explaining the reason.

6.3.1. Rights of Personal Data Owners

Pursuant to Article 11 of the KVK Law, the data owner can apply to our Company with the Data Owner Application Form and make a request on the following issues:

(1) To learn whether your personal data has been processed,

(2) If your personal data has been processed, to request information about it,

(3) To learn the purpose of processing your personal data and whether they are used in accordance with their purpose,

(4) To learn the third parties to whom your personal data is transferred domestically or abroad,

(5) To request correction of your personal data in case of incomplete or incorrect processing and to request notification of the transaction made within this scope to the third parties to whom your personal data has been transferred,

(6) Although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, to request the deletion, destruction or anonymization of your personal data in the event that the reasons requiring its processing disappear, and to request that the transaction made within this scope be notified to the third parties to whom your personal data has been transferred,

(7) To object to the emergence of a result against you by analyzing your processed data exclusively through automated systems,

(8) To request the compensation of the damage in case you suffer damage due to the unlawful processing of your personal data.

6.3.2. Situations Outside the Rights of Personal Data Owners in Accordance with the Legislation

Pursuant to Article 28 of the KVK Law, since the following situations are not within the scope of the KVK Law, it will not be possible for personal data owners to assert their rights on the following issues:

(1) Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy or personal rights or does not constitute a crime.

(2) Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.

(3) Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.

(4) Processing of personal data by judicial authorities or enforcement authorities in relation to investigation, prosecution, trial or execution proceedings.

Pursuant to Article 28/2 of the KVK Law; In the following cases, it will not be possible for personal data owners to assert their rights, except for requesting the compensation of the damage:

(1) The processing of personal data is necessary for the prevention of crime or criminal investigation.

(2) Processing of personal data made public by the personal data owner.

(3) The processing of personal data is necessary for the execution of supervisory or regulatory duties and disciplinary investigation or prosecution by authorized and authorized public institutions and organizations and professional organizations in the nature of public institutions, based on the authority granted by the law.

(4) The processing of personal data is necessary for the protection of the economic and financial interests of the state in relation to budget, tax and financial issues.

6.4. CATEGORIES OF PERSONAL DATA AND RECIPIENT GROUPS PROCESSED AS A RESULT OF PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT BY THE COMPANY

6.4.1. Categories of Personal Data

The categories and descriptions of personal data processed within the scope of personal data processing activities carried out by the Company are regulated below:

CATEGORIES OF PERSONAL DATA	EXPLANATION
ID	It is personal data that contains information about the identity of the person; Documents such as driver's license, identity card and passport containing information such as name-surname, TR identity number, nationality information, mother's name-father's name, place of birth, date of birth, gender, tax number, SSI number, signature information, vehicle license plate, etc. information.
Contact Information	Contact information; Personal data such as telephone number, address, e-mail address, fax number.
Physical Space Security Information	Personal data regarding the records and documents taken at the entrance to the physical space, during the stay in the physical space; camera recordings and recordings taken at the security point, etc.
Transaction Security Information	Personal data such as IP address information, website login and exit information, password and password information processed to ensure the technical, administrative, legal and commercial security of both the data owner and the Company while carrying out the commercial activities of the Company.
Financial Datas	Personal data such as bank account number, IBAN number, credit card information, financial profile, asset data, income information
Personnel Information	All kinds of personal data processed to obtain information that will be the basis for the formation of the personal rights of company employees or real persons who have a working relationship with our Company.
Legal Action	Personal data processed within the scope of the determination and follow-up of the Company's legal receivables and rights, and the

	performance of its debts, as well as compliance with legal obligations and Company policies.
Association Membership	If it is included in the CV of the employee candidate
Foundation Membership	If it is included in the CV of the employee candidate
Trade Union Membership	If it is included in the CV of the employee candidate
Professional Experience	Personal data such as diploma information, courses attended, on-the-job training information, certificates, transcript information, etc.
Audiovisual Recordings	Audio/Visual Data Photo and camera recordings (except for records within the scope of Physical Space Security Information), audio recordings and data contained in documents that are copies of documents containing personal data
Philosophical Beliefs, Religions, Denominations and Other Beliefs	If an old identity card has been provided to the Company by the data owner for the purpose of company records, information about the religious affiliation written in the religion section of the identity card.
Criminal Conviction and Security Measures	Criminal record obtained for personnel file creation and internal audit processes
Vehicle Information	Vehicle information received by the company in order to keep visitor records and to ensure the security of the physical space
Health Data	Information on disability, blood group information, personal health information, device and prosthesis information used, etc.

6.4.2. Recipient Groups

In accordance with the principles contained in the KVK Law and in particular, in accordance with Articles 8 and 9 of the KVK Law, the Company may transfer the personal data of the data owners within the scope of the Company's KVK Policy to the groups of persons listed in the table below for the purposes specified:

RECIPIENT GROUPS	DEFINITION	PURPOSE OF DATA TRANSFER
Partner	Third parties with whom the	Limited to ensure the fulfillment of

	Company has established a business partnership for purposes such as carrying out its commercial activities	the purposes for which the business partnership was established
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. ("E.ON") are shareholders of the Company	For purposes such as planning and maintaining the Company's strategic measures regarding the Company's commercial activities, including board decisions and internal audit reporting,
Supplier	Parties that provide services to the Company in accordance with the Company's orders and instructions and on a contractual basis within the scope of the Company's commercial activities	Limited to the purpose of providing the Company with the services outsourced from the supplier and necessary to carry out the Company's commercial activities,
Affiliates	Companies in which the Company is a shareholder	Limited to ensuring the execution of the Company's commercial activities that require the participation of its subsidiaries
Sabancı Group Companies	All the companies that make up the Sabancı Group	Limited to purposes such as planning the Company's strategies regarding its commercial activities and maintaining its activities and auditing
Legally Authorized Public Institutions and Organizations	In accordance with the provisions of the relevant legislation, the Company's public institutions and organizations authorized to receive information and documents	Limited to the purpose requested by the relevant public institutions and organizations within the legal authority

6.5. ENSURING THE SECURITY AND CONFIDENTIALITY OF PERSONAL DATA BY THE COMPANY

In order to prevent unlawful disclosure, access, transfer of personal data or security deficiencies that may occur in other ways, the Company may, within the possibilities, according to the nature of the data to be protected, in accordance with Article 12 of the KVK Law. All necessary measures are taken in accordance with the article. The relevant rules are included in the Personal Data Retention and Destruction Policy.

In this context, all necessary (i) administrative and (ii) technical measures are taken by the Company, (iii) an audit system is established within the company, and (iv) in case of unlawful disclosure of personal data, it acts in accordance with the measures stipulated in the KVK Law.

(1) Administrative Measures Taken by the Company to Ensure the Lawful Processing of Personal Data and to Prevent Unlawful Access to Personal Data

– The Company educates its employees regarding the legislation on the protection of personal data and ensures that they are made aware.

– In cases where personal data is subject to transfer, it is ensured that records are added to the contracts concluded by the Company with the persons to whom the personal data is transferred, stating that the party to whom the personal data is transferred will fulfill its obligations to ensure data security.

– The personal data processing activities carried out by the company are examined in detail, and in this context, the steps to be taken to ensure compliance with the personal data processing conditions stipulated in the KVK Law are determined.

– The Company determines the practices that must be fulfilled in order to ensure compliance with the KVK Law and regulates these practices with internal policies.

(2) Technical Measures Taken by the Company to Ensure the Lawful Processing of Personal Data and to Prevent Unlawful Access to Personal Data

– Regarding the protection of personal data, technical measures are taken by the company to the extent permitted by technology, and the measures taken are updated and improved in parallel with the developments.

– Expert personnel are employed in technical matters.

– Inspections are carried out at regular intervals for the implementation of the measures taken.

– Software and systems are installed to ensure security.

– The authorization to access the personal data being processed within the company is limited to the relevant employees in line with the determined processing purpose.

(3) Conducting Audit Activities by the Company on the Protection of Personal Data

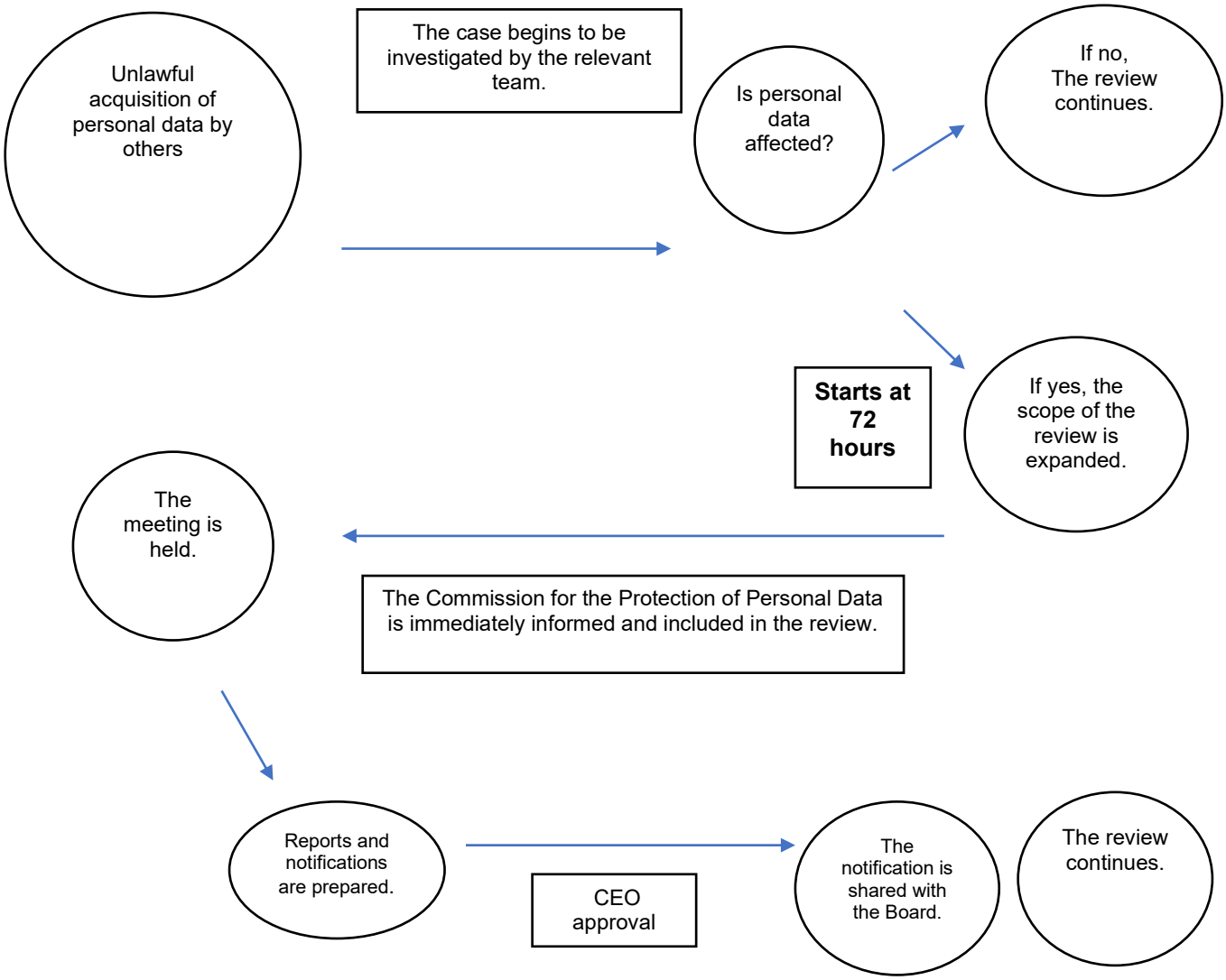
The compliance with the relevant legislation, policies, procedures and instructions of the technical measures, administrative measures and practices taken by the Company within the scope of protecting and ensuring the security of personal data are audited by the Company's Internal Audit Department. The Company's Internal Audit Department may carry out the audit activity in question through its own organization or outsourced audit firms when it deems necessary. The results of the audit activities carried out within this scope are reported to the Company's Internal Audit Committee, the Company's CEO and the relevant function managers. It is the responsibility of the process owners to regularly follow up the planned actions regarding the audit results. Process owners periodically report their follow-up and progress status to the Company's Internal Audit Department,

and the Internal Audit Department monitors the actions within the scope of this report, conducts verification tests and audits. Activities that will ensure the development and improvement of the measures taken regarding the protection of data, including but not limited to the results of the audit, are carried out by the relevant enforcement units.

(4) Measures to be Taken in Case of Unlawful Disclosure of Personal Data

In the event that the personal data processed by the Company is obtained by others illegally, this situation should be reported to the relevant persons and the Personal Data Protection Board (Board) as soon as possible. The said "shortest period" has been determined as 72 hours for the notifications to be made to the Board together with the decision of the Board.

In order to manage this process in the best way and to minimize the risks that may arise as a result of the Board's investigations, the relevant units must act quickly and in a coordinated manner. Therefore, in the event that a data breach occurs and is detected, the flowchart to be followed should be as follows:



In the event that the personal data of which the Company is the data controller is obtained by others illegally, it can first be determined by the Information Technologies unit. Such a violation can be detected as a result of the investigations carried out by the Internal Audit unit. In these cases, or if the breach is detected by different units, the data breach process described above

should be initiated immediately. When it is determined that personal data has been affected in the data breach, the Personal Data Protection Commission is immediately involved in the process and the kisiselveri@enerjisauretim.com address is immediately notified via e-mail.
At the meeting to be held by the Personal Data Protection Commission, the relevant issues are evaluated, especially the determination studies carried out, the number of people affected by the breach, the number of data affected by the breach, the after-effects of the breach and the measures to be taken. If the Commission deems it necessary, it may include managers and employees from the relevant units in the meeting. Information on data breaches, their effects and measures taken are recorded. The meeting and determination outputs are prepared as a report and submitted to the approval of the CEO together with the draft notification. After approval, the notification is shared with the Board.

If a notification cannot be made to the Board within 72 hours for a justified reason, the reasons for the delay shall be explained to the Board along with the notification to be made. In the notification to be made to the Board, the "Personal Data Breach Notification Form" on the Board's website is used. In cases where it is not possible to provide the information in the form at the same time, this information is provided gradually without delay.

Investigations into the violation continue within the company. Data owners who are found to be affected by the breach are contacted as soon as reasonably possible and informed. If the contact address of the person concerned cannot be reached, notification is made by appropriate methods such as publishing on the Company's own website. If deemed necessary, public disclosure and information activities are carried out by taking the opinion of the Corporate Communication unit.

6.6. PERSONAL DATA PROTECTION LAW COMPLIANCE PROCESS

The compliance process is carried out by the company in order to ensure the fulfillment of legal obligations within the scope of KVKK and the relevant legislation, to ensure that the activities carried out comply with the legislation on the protection of personal data, to execute and improve the established systems, to identify them in case of non-compliance, to determine the corrective actions to be taken and to increase awareness within the company by reporting all related issues. The rules regarding the harmonization process are determined in the Enerjisa Generation Compliance Booklet and the Compliance Policy and Procedure announced regarding this process.

7. REVIEW

The application rules, which will be regulated in accordance with this Policy and will specify how the matters specified in this Policy will be carried out in certain matters, will be arranged in the form of a procedure.

In any case, this Policy is reviewed once a year and updated if there are necessary changes.

In the event of a conflict between the legislation in force regarding the protection and processing of personal data and the Company's KVK Policy, the Company accepts that the legislation in force will be applied.

The Company's KVK Policy is published on the Company's website (www.enerjisauretim.com) and is accessible to personal data owners. In parallel with the changes and innovations to be made in the relevant legislation, the amendments to be made in the Company's KVK Policy will be made accessible to data owners in a way that data owners can easily access.