

PERSONAL DATA PROTECTION AND PROCESSING POLICY

Table of Contents

1. PURPOSE AND SCOPE.....	3
2. OBJECTIVE.....	3
3. DEFINITIONS	3
4. ROLES AND RESPONSIBILITIES AND PERSONAL DATA PROTECTION COMMITTEE	6
5. FUNDAMENTAL PRINCIPLES OF COMPANY PDP POLICY	8
5.1. SCOPE OF THE COMPANY PDP POLICY	8
5.2. CONDITIONS AND PURPOSES FOR PROCESSING OF PERSONAL DATA WITHIN THE SCOPE OF BUSINESS ACTIVITIES CONDUCTED BY THE COMPANY	8
6. PRINCIPLES ADOPTED BY THE COMPANY REGARDING THE PROCESSING AND PROTECTION OF PERSONAL DATA	9
6.1. PERFORMANCE OF PERSONAL DATA PROCESSING ACTIVITIES IN COMPLIANCE WITH DATA PROCESSING CONDITIONS.....	9
6.2. PROVISION OF INFORMATION BY THE COMPANY TO DATA SUBJECTS ...	15
6.3. FINALIZATION OF PERSONAL DATA SUBJECTS' REQUESTS BY THE COMPANY	15
6.4. CATEGORIES AND RECIPIENT GROUPS OF PERSONAL DATA PROCESSED AS A RESULT OF PERSONAL DATA PROCESSING ACTIVITIES CONDUCTED BY THE COMPANY	17
6.5. ENSURING THE SECURITY AND PRIVACY OF PERSONAL DATA BY THE COMPANY	20
6.6. PROCESS OF COMPLIANCE WITH THE PERSONAL DATA PROTECTION LAW	23
7. REVIEW	23

1. PURPOSE AND SCOPE

Having adopted the principle of paying utmost care to ensure compliance with the legal order from its past to the present, Enerjisa establishes systems for conducting any and all necessary activities in order to ensure compliance with the legislation on the processing and protection of personal data.

The Company's PDP (Personal Data Protection) Policy governs the principles adopted by the Company for the protection and processing of personal data.

In line with the emphasis placed by the Company on protection of personal data, the Company's PDP Policy sets forth the fundamental principles regarding the compliance of activities conducted by the Company with the regulations in the Personal Data Protection Law no. 6698 ("PDP Law"). The sustainability of data security principles adopted by the Company will be ensured with the implementation of the Company's PDP Policy regulations.

Although the Company's PDP Policy is intended for natural persons whose personal data are processed by the Company whether by automated means or non-automated means that are a part of any data recording system; the matters regarding the protection of the personal data of Company employees are set out separately in the "Company Employees Personal Data Protection and Processing Policy".

2. OBJECTIVE

With the Company's PDP Policy, it is aimed to establish necessary systems in line with the objective of raising awareness about the lawful processing and protection of personal data within the Company and to establish the necessary mechanism to ensure compliance with the legislation. In this context, the Company's PDP Policy is intended to provide guidance regarding implementation of the regulations stipulated by the PDP Law and relevant legislation.

3. DEFINITIONS

Important terms used in the Company PDP Policy are defined as follows:

Explicit Consent	Freely given, specific and informed consent related to a specific matter.
Anonymization	Rendering personal data impossible to link with an identified or identifiable natural person, even by matching them with other data.
Communiqué on Principles and Procedures to be followed in	The Communiqué on Principles and Procedures to be followed in fulfilment of the Obligation to Inform which entered into force upon its publication in the Official Gazette no. 30356 of 10 March 2018.

Fulfilment of the Obligation to Inform	
Employee(s)	Employee(s) of the Company.
Employee PDP Policy	“Company Employees Personal Data Protection and Processing Policy” setting forth the principles regarding the protection and processing of personal data of Company employees.
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDINGS S.A.R.L. (hereinafter referred to as “E.ON”)
Regulation on Personal Health Data	The Regulation on Personal Health Data published in the Official Gazette no. 30808 of 21 June-October 2019.
Personal Health Data	Any information regarding physical and mental health of an identified or identifiable natural person as well as information on healthcare services offered to such person.
Personal Data	Any information relating to an identified or identifiable natural person.
Data Subject / Personal Data Subject	Natural person whose personal data is processed.
Personal Data Protection Committee	The committee that will ensure necessary coordination within the Company in order to ensure, maintain and sustain compliance of the Company with the legislation on protection of personal data.
Processing of Personal Data	Any operation or set of operations performed on personal data, in part or in whole, whether by automated means, or non-automated means that are a part of any data recording system, such as collection, recording, storage, preservation, alteration, revision, disclosure, transmission, acquisition, retrieval, categorization or prevention of the use of such data.
PDP Law	Personal Data Protection Law no. 6698 dated 24 March 2016 as published in the Official Gazette no. 29677 of 7 April 2016.
PDP Board	Personal Data Protection Board.
PDP Authority	Personal Data Protection Authority.

PDP Compliance Program	The program implemented by the Company to ensure compliance with the legislation on protection of personal data.
Special Categories of Personal Data	Data relating to race, ethnic origin, political view, philosophical belief, religion, sect or other beliefs, clothing/dressing, association, foundation or trade-union membership, health, sexual life, criminal convictions and offences and related security measures as well as biometric and genetic data.
Company	means Enerjisa Üretim Santralleri Anonim Şirketi and its subsidiaries.
Company Business Partners	The parties with which the Company establishes business partnerships for various purposes while conducting its business activities.
Company Personal Data Storage and Destruction Policy	The “Company’s Personal Data Storage and Destruction Policy” constituting the basis for determination of the maximum storage period necessary for the purpose of processing of personal data as processed by the Company, and for erasure, destruction and anonymization of personal data pursuant to the By-Law on Erasure, Destruction and Anonymization of Personal Data as published in the Official Gazette no. 30224 of 28 October 2017.
Company PDP Policy	The Company’s Personal Data Protection and Processing Policy.
Company Suppliers	The parties providing services to the Company on a contractual basis.
Company Data Subject Application Form	The application form to be used by data subjects as they make applications to exercise their rights listed in article 11 of the PDP Law.
Sabancı Group Employee PDP Policy	The “Sabancı Group Employees Personal Data Protection and Processing Policy” setting forth the principles adopted for protection and processing of personal data pertaining to the employees of the companies within Sabancı Group.
Sabancı Group PDP Policy	The “Sabancı Group Personal Data Protection and Processing Policy” setting forth the principles adopted for protection and processing of personal data by Sabancı Group.
Sabancı Group Companies / Group Companies	All companies within the structure of Sabancı Group.
Constitution of the Republic of Türkiye	The Constitution of the Republic of Türkiye no. 2709 dated 7 November 1982 as published in the Official Gazette no. 17863 of 9 November 1982.

Turkish Criminal Code	Turkish Criminal Code no. 5237 dated 27 September 2004 as published in the Official Gazette no. 25611 of 12 October 2004.
Data Processor	The natural or legal person processing personal data on behalf of the data controller based on the authorization granted by the data controller.
Data Controller	The person determining the purposes and means of processing of personal data and responsible for the establishment and management of the data recording system.
Communiqué on Principles and Procedures for Application to the Data Controller	The Communiqué on Principles and Procedures for Application to the Data Controller which entered into effect upon its publication in the Official Gazette no. 30356 of 10 March 2018.

4. ROLES AND RESPONSIBILITIES AND PERSONAL DATA PROTECTION COMMITTEE

The “Personal Data Protection Committee” has been established by the Company to ensure necessary coordination within the Company in order to ensure, maintain and sustain compliance with the personal data protection legislation. The Committee is comprised of at least 4 persons, providing that its members include the People and Culture Group Manager, the Information Technologies Group Manager, the Legal Advisor and a Senior Lawyer. The Personal Data Protection Committee is responsible for ensuring uniformity among the units and departments of the Company, and for the maintenance and improvement of the systems established to ensure compliance of the activities conducted by the Company with the personal data protection legislation. The processes of the Committee have been set forth with a procedure.

In this context, the fundamental duties of the Personal Data Protection Committee are as follows:

- To establish a corporate culture supporting the rules regarding the protection and processing of personal data;
- To prepare the basic policies regarding protection and processing of personal data and to implement them upon the approval of the Executive Vice President for People and Culture;
- To decide on how personal data protection and processing policies will be implemented and audited, and to make internal assignments and to ensure coordination within the Company in this respect.
- To determine the actions to be taken to ensure compliance with the PDP Law and the relevant legislation; to supervise the implementation and to ensure the coordination of such actions;
- To increase awareness about the protection and processing of personal data both within the Company and at and before the agencies and institutions that the Company cooperates with;

- ❑ To identify the risks that may arise during the Company’s personal data processing activities and to ensure necessary measures are taken against such risks; and to offer recommendations for improvement;
- ❑ To design and ensure the performance of trainings on protection of personal data and implementation of policies;
- ❑ To conclude and resolve the applications of personal data subjects at the highest level;
- ❑ To coordinate the performance of information and training activities aimed at ensuring that personal data subjects are informed about the Company’s personal data processing activities and their legal rights (While conducting the relevant training and awareness-raising activities, the “Personal Data Security Guideline” published by the Board on its official website is taken as basis.);
- ❑ To prepare the amendments to the fundamental policies regarding the protection and processing of personal data and to implement them with the approval of the Executive Vice President for People and Culture;
- ❑ To monitor the developments and regulations on protection of personal data; and to make recommendations to the senior management with respect to necessary actions to be taken in the operations of the Company in line with these developments and regulations;
- ❑ To manage the relationships with the PDP Board and PDP Authority;
- ❑ To fulfil other duties to be assigned by the Company management regarding the protection of personal data.

All business units processing personal data, including, particularly, the People and Culture and Information Technologies department, are responsible for the practices such as protection, processing, erasure, and transfer of personal data, and for fulfilment of the obligations such as data security, disclosure, and explicit consent as stipulated in the legislation for the data controller, providing to be limited with the data retained and stored by them. Although the Personal Data Protection Committee is responsible for implementation of the Company PDP Policy in all of the Company operations, activities and processes; the Legal Consultancy department shall serve as a consultant, guide, and source of recommendations in the implementation of regulations, procedures, guidelines, standards and training activities prepared in line with the Company PDP Policy. All our employees, stakeholders, visitors and relevant third parties across the Company are obliged to cooperate with the Legal Consultancy department while ensuring compliance with the Company PDP Policy and preventing legal risks and immediate threats and hazards. All bodies and departments of the Company are responsible to observe compliance with the Company PDP Policy.

The Executive Vice President for People and Culture is authorized to change and implement the Policies as necessary, except for the revocation of personal data policies.

5. FUNDAMENTAL PRINCIPLES OF COMPANY PDP POLICY

5.1. SCOPE OF THE COMPANY PDP POLICY

Data subjects covered within the scope of the Company PDP Policy, whose personal data are processed by the Company, are grouped as follows:

- Company Employee Candidates
Individuals who have not made an employment contract with the Company, but are under evaluation by the Company to that effect.
- Relatives of employees
- Consultants
- Company Business Partners, Officials, Employees
Natural person officials, shareholders, and employees of the institutions that are in business relationships with the Company.
- Company Visitors
Natural persons visiting the Company buildings or websites operated by the Company.
- Other Natural Persons
All natural persons not covered by the Company Employees Personal Data Protection and Processing Policy.

5.2. CONDITIONS AND PURPOSES FOR PROCESSING OF PERSONAL DATA WITHIN THE SCOPE OF BUSINESS ACTIVITIES CONDUCTED BY THE COMPANY

Our Company processes personal data for the following purposes, limited to the personal data processing conditions as listed in paragraph 2 of article 5 and paragraph 3 of article 6 of the PDP Law (See Section 6.1.).

The Company firstly checks whether processing conditions exist when processing personal data. If such processing conditions do not exist, the Company obtains explicit consent from personal data subjects in order to conduct personal data processing activities.

Under the conditions specified above; our Company may process personal data for the purposes, including, but not limited to the following:

	<u>PURPOSES</u>
1	Conducting Training Activities
2	Conducting Employee Candidate / Intern / Student Selection and Placement Processes

3	Conducting Employee Candidate Application Processes
4	Conducting Finance and Accounting Activities
5	Conducting Goods / Services Procurement Processes
6	Conducting contract execution processes
7	Providing Information to Competent Persons, Agencies and Institutions
8	Conducting Internal Audit / Investigation / Intelligence Activities
9	Conducting Audits / Ethics-Related Activities
10	Ensuring Physical Location Security
11	Ensuring Security of Data Controller Operations
12	Conducting Occupational Health & Safety Activities
13	Conducting / Auditing Business Activities
14	Conducting Activities in line with the Legislation
15	Conducting Information Security Processes
16	Creating and Monitoring Visitor Records
17	Organization and Event Management
18	Conducting Business Continuity Activities
19	Conducting Communication Activities
20	Following up and Conducting Legal Affairs
21	Conducting Emergency Management Processes
22	Receiving and Evaluating Recommendations for Improvement of Business Processes
23	Follow-up of Requests / Complaints
24	Conducting Social Responsibility and Civil Society Activities
25	Executing Access Authorizations

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

6.1. PERFORMANCE OF PERSONAL DATA PROCESSING ACTIVITIES IN COMPLIANCE WITH DATA PROCESSING CONDITIONS

While conducting its data processing activities, the Company acts in compliance with (i) fundamental principles, (ii) personal data processing conditions, and (iii) special categories of personal data processing conditions.

6.1.1. Compliance with Fundamental Principles

The Company adopts the fundamental principles listed below within the scope of ensuring and maintaining compliance with personal data protection legislation:

(1) Processing personal data in compliance with the law and the rules of integrity

The Company conducts personal data processing activities in line with the personal data protection legislation and in compliance with the law and the rules of integrity, including, particularly, the Constitution of the Republic of Türkiye.

(2) Ensuring accuracy and currency of the processed personal data

While personal data processing activities are conducted by the Company, any and all necessary organizational and technical measures are taken to ensure the accuracy and currency of the personal data within technical means. In this context, our Company has established mechanisms to correct and verify the accuracy of personal data in cases where the personal data of personal data subjects are incorrect.

(3) Processing personal data for specified, explicit and legitimate purposes

The Company conducts personal data processing activities for specified and lawful purposes determined before the start of personal data processing activities.

(4) Processing personal data as relevant, limited and proportionate to the purposes of processing

The Company processes personal data as relevant with the data processing conditions and only to the extent necessary for provision of these services. In this context, personal data processing purpose is determined before the start of personal data processing activity; and data processing activities are not conducted with the assumption that the data might be used in the future. Before personal data processing activities, the need for data processing activity and, if necessary, actions to be taken according to the nature of the data, are determined and implemented by following the methods specified in the Personal Data Processing Necessity and Proportionality Testing Procedure.

(5) Storing personal data for the time period stipulated in the relevant legislation or required for their processing purposes

The Company stores personal data for the period stipulated in the relevant legislation; or if such a period is not stipulated for storage of personal data in the relevant legislation, for the necessary period required for processing of relevant data pursuant to the Company practices in connection with the services offered while processing such data, the requests of the relevant Authorities/Agencies due to operation in a regulated industry and relevant business practices. Accordingly, in cases where the period stipulated in the legislation expires or the reasons requiring the processing of personal data cease to exist, personal data are erased,

anonymized by the Company. The relevant rules are announced in the Personal Data Storage and Destruction Policy.

6.1.2. Compliance with the Conditions for Processing of Personal Data

The Company conducts personal data processing activities in compliance with the data processing conditions stipulated in article 5 of the PDP Law. In this context, personal data processing activities are conducted in case of existence of the following conditions for processing of personal data:

(1) Presence of the Explicit Consent of the Personal Data Subject

The Company conducts personal data processing activities if the data subject gives their consent for processing of their data freely, with adequate information about the matter, clearly without hesitation and limited to that relevant process only.

(2) Explicit Stipulation of Personal Data Processing Activity in the Laws

If there is an explicit provision in the law regarding the personal data processing activity, the Company may conduct personal data processing activity limited to the applicable statutory regulation.

(3) Failure to Obtain the Data Subject's Explicit Consent due to Actual Impossibility and the Requirement to Process Personal Data

In cases where personal data subjects cannot express their consents or their consents are rendered invalid and if it is required to process personal data in order to protect life or physical integrity of individuals, the Company conducts data processing activities in this context.

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

In cases where it is directly related with the execution or performance of a contract; the Company conducts data processing activities if it is required to process the personal data of the relevant contracting parties.

(5) If Personal Data Processing Activity is Required for Fulfilment of the Company's Legal Obligation(s)

In cases where there is a legal obligation to be fulfilled by the Company that has adopted the principle of paying due care and diligence to ensure compliance with the laws, the personal data processing activities are conducted in order to fulfil the relevant legal obligation.

(6) Public Disclosure of Personal Data by the Data Subject

The personal data made public (disclosed to the public in any manner whatsoever) by the relevant data subject are processed by the Company in accordance with the purpose of their public disclosure.

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

If the processing of personal data is required for establishment, exercise or protection of a right, the Company conducts data processing activities in parallel with this requirement.

(8) If it is required to conduct Personal Data Processing Activities for the Legitimate Interests of the Company without prejudice to the Data Subject's Fundamental Rights and Freedoms

In cases where it is required to process personal data for legitimate interests of the Company, data processing activities may be conducted without prejudice to the data subject's fundamental rights and freedoms. In this context, "balancing tests" recognized in the referenced regulation are applied by the Company to determine the existence of this condition.

6.1.3. Compliance with the Conditions for Processing of Special Categories of Personal Data

The Company pays special attention to the processing of special categories of personal data bearing the risk of leading to discrimination when processed unlawfully. In this context, when processing special categories of personal data, the Company firstly determines whether sensitive data processing conditions exist and then conducts data processing activities after making sure that the lawfulness condition is fulfilled. The technical and organizational measures taken by our Company for the protection of personal data are duly taken within the scope explained in the Special Categories of Personal Data Protection and Processing Policy within the framework of adequate measures stipulated in the Board's Decision no. 2018/10 dated 31/01/2018 in terms of special categories of personal data; and the activities conducted accordingly are monitored and audited within the framework of the audits conducted within the Company.

Detailed Rules on this matter are announced in the Special Categories of Personal Data Protection Policy.

Special categories of personal data may be processed by the Company in the following cases, providing that adequate measures determined by the PDP Board are duly taken:

- a) The existence of the explicit consent of the relevant person,
- b) It is explicitly stipulated by law,

- c) It is mandatory to protect the life or physical integrity of the person or another person who is unable to declare their consent due to actual impossibility or whose consent is not legally recognized,
- ç) It relates to personal data made public by the relevant person and is in line with their intent to make it public,
- d) It is necessary 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, as well as for the planning, management, and financing of healthcare services by persons or authorized institutions and organizations obligated to maintain confidentiality,
- f) It is necessary for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance,
- g) It is directed at current or former members or affiliates, or persons in regular contact with foundations, associations, or other non-profit organizations or entities established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with the legislation and purposes they are subject to, limited to their field of activity, and not disclosed to third parties.

6.1.4. Compliance with the Conditions for Transfer of Personal Data

Personal data transfer conditions as set forth in articles 8 and 9 of the PDP Law are followed in case of personal data transfers to be conducted by the Company.

(1) Domestic Transfer of Personal Data

In case of data transfer activities to be conducted at home, the Company acts in accordance with the data processing conditions and by taking necessary security measures pursuant to article 8 of the PDP Law.

Even in cases where there is no explicit consent of the data subject, personal data may be transferred by our Company to third parties by paying due care and diligence and taking all necessary security measures including the methods stipulated by the Board if one or more of the following data processing conditions (“Data Processing Conditions”) exist:

- If the relevant activities regarding transfer of personal data are explicitly stipulated in the laws;
- If the transfer of personal data by the Company is directly related to and necessary for execution or performance of a contract;

- If the transfer of personal data is required for fulfilment of our Company's legal obligation(s);
- If personal data are transferred by our Company limited to the purpose of public disclosure, providing that the relevant personal data have been made public by the relevant data subject;
- If the transfer of personal data by the Company is required for establishment, exercise or protection of the rights of the Company or the data subject or third parties;

- If it is required to perform personal data transfers for the Company's legitimate interests without prejudice to the fundamental rights and freedoms of the data subject;
- If it is required to protect the life or physical integrity of the data subject or another person who is incapable of giving consent due to actual impossibility or whose consent is rendered legally invalid.

(2) Transfer of Personal Data Abroad

For the transfer of personal data abroad by the company in accordance with Article 9 of the Personal Data Protection Law, one of the following conditions must be met:

1. If at least one of the conditions for the processing of personal or sensitive personal data is present and there is an adequacy decision regarding the country to which the personal data will be transferred, the sectors within the country, or international organizations, data controllers and data processors may transfer data abroad. The adequacy decision will be issued by the Personal Data Protection Board.
2. In the absence of an adequacy decision:
 - At least one of the conditions for the processing of personal or sensitive personal data must exist,
 - The transferred country must provide the data subject with the opportunity to exercise their rights and have access to effective legal remedies, and
 - One of the appropriate safeguards must be ensured.

The appropriate safeguards are listed below:

- Binding corporate rules that include provisions on the protection of personal data, which are approved by the Board and are mandatory for companies within a group of enterprises engaged in joint economic activities,
- Written commitments that include provisions ensuring adequate protection and permission for the transfer granted by the Board,
- The existence of a standard contract announced by the Board.

The standard contract must be notified to the Board by the data controller or data processor within 5 business days from the date it is signed.

Personal data can be transferred by the Company to Microsoft's data centers by taking necessary security measures as a result of the use of Microsoft Office 365 applications. Such data centers

are located in the countries listed in the relevant link¹, including, particularly, the EU countries and the United States of America. It is technically impossible for third parties, including Microsoft, to access the data hosted in Microsoft data centers due to the encryption methods used. If Microsoft engineers need to have access to such data for any technical reasons, access is technically impossible in cases where it is not permitted by Enerjisa Üretim².

(3) Transfer of Special Categories of Personal Data

Special categories of personal data may be transferred by our Company in accordance with the principles specified herein and by taking organizational and technical measures including the methods described in the Special Categories of Personal Data Protection and Processing Policy, in case of existence of the following conditions:

- The existence of the explicit consent of the data subject,
- It is explicitly stipulated by law,
- It is mandatory to protect the life or physical integrity of the person or another person who is unable to declare their consent due to actual impossibility or whose consent is not legally recognized,
- It relates to personal data made public by the data subject and is in line with their intent to make it public,
- It is necessary 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, as well as for the planning, management, and financing of healthcare services by persons or authorized institutions and organizations obligated to maintain confidentiality,
- It is necessary for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance,
- It is directed at current or former members or affiliates, or persons in regular contact with foundations, associations, or other non-profit organizations or entities established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with the legislation and purposes they are subject to, limited to their field of

¹ Microsoft's data center location country details and information about which of these data centers are used for access from Türkiye are available at <https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations>.

² Customer Lockbox feature, whereby the need to access data is subject to the initiative and permission of Enerjisa Üretim, is enabled on our platform. Further details of the technology are available at <https://social.technet.microsoft.com/wiki/contents/articles/35748.office-365-what-is-customer-lockbox-and-how-to-enable-it.aspx>.

activity, and not disclosed to third parties.

6.2. PROVISION OF INFORMATION BY THE COMPANY TO DATA SUBJECTS

The Company conducts necessary processes to ensure that data subjects are informed during collection of personal data in accordance with article 10 of the PDP Law and the Communiqué on Procedures and Principles to be followed in Fulfilment of the Obligation to Inform. In this context, the informative texts provided by the Company to data subjects contain the following information:

- (1) Trade-name of our Company;
- (2) The purposes for which data subjects' personal data will be processed by the Company;
- (3) The recipients to whom and the purpose for which the processed personal data may be transferred;
- (4) The method of and legal reasons for collection of personal data;
- (5) Data subject's rights.

6.3. FINALIZATION OF PERSONAL DATA SUBJECTS' REQUESTS BY THE COMPANY

If data subjects submit their requests about personal data to our Company in writing by using the Data Subject Application Form available at www.enerjisauretim.com.tr or via other methods determined by the PDP Board; the Company, acting in the capacity as the data controller, conducts the necessary processes to ensure that such requests are concluded and finalized in accordance with article 13 of the PDP Law as soon as possible and within thirty (30) days at the latest according to the nature of the request. Data subjects should make their requests about their personal data in accordance with the Communiqué on Principles and Procedures for Application to the Data Controller and the Procedure for Receiving, Evaluating and Responding to Data Subject Applications.

The Company may request information to determine whether the applicant is the owner of the personal data in question in terms of ensuring data security. Our Company may also address questions to the personal data subject about their applicant in order to ensure that the data subject's application is duly finalized in line with the request.

The company may decline requests by explaining their justification in cases where the data subject's application may prejudice the rights and freedoms of other persons, or requires disproportionate efforts, or involves publicly available information.

6.3.1. Rights of Personal Data Subjects

Pursuant to article 11 of the PDP Law, data subjects can apply to our Company using the Data Subject Application Form and thus file requests in relation to the following matters:

- (1) To find out whether your personal data have been processed or not;
- (2) If processed, to request information about such processing;
- (3) To learn the purpose of processing and whether your personal data have been used for intended purposes or not;
- (4) To find out the third parties to whom your personal data have been transferred at home or abroad;
- (5) To request for correction of your personal data if they have been processed incompletely or inaccurately, and to request for notification of the action taken accordingly to the third parties to whom your personal data have been transferred;
- (6) To request for erasure, destruction or anonymization of your personal data if the reasons requiring their processing cease to exist even though they were processed in accordance with the PDP Law and the provisions of other applicable laws, and to request for notification of the action taken accordingly to the third parties to whom your personal data have been transferred;
- (7) To object to any outcomes that may arise to your detriment through the analysis of your processed data exclusively via automated means;
- (8) To claim for compensation of any loss or damages that you may incur due to the unlawful processing of your personal data.

6.3.2. Cases Excluded from Data Subjects' Rights pursuant to Legislation

Pursuant to article 28 of the PDP Law, personal data subjects may not claim for their rights in respect of the following matters since the following cases are excluded from the scope of the PDP Law:

- (1) Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, providing that national defence, national security, public security, public order, economic security, privacy, or personal rights are not violated or the processing does not constitute a criminal offence.
- (2) Processing of personal data for official statistics and research, planning and statistical purposes through anonymization of such data.

(3) Processing of personal data within the scope of preventive, protective, and intelligence activities carried out by governmental authorities and agencies duly empowered and authorized by laws to ensure national defence, national security, public security, public order, or economic security.

(4) Processing of personal data by judicial authorities or enforcement authorities with regard to investigation, prosecution, adjudication or enforcement proceedings.

Pursuant to article 28/2 of the PDP Law; personal data subjects may not claim for their rights in case of the following circumstances, except for the right to claim for compensation in such cases:

(1) Personal data processing is required for the prevention of a crime or for conducting a criminal investigation.

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

(3) Personal data processing is required for performance of supervisory or regulatory duties, and for disciplinary investigation or prosecution by empowered and authorized governmental authorities and agencies as well as professional institutions bearing the status of governmental agencies, in accordance with the powers granted to them by the laws.

(4) Personal data processing is required for the protection of the state's economic and financial interests regarding budgetary, tax-related and financial matters.

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

6.4.1. Personal Data Categories

Categories of personal data processed within the scope of personal data processing activities conducted by the Company and their descriptions are as follows:

PERSONAL DATA CATEGORIES	DESCRIPTION
Identity data	Personal data containing information about the identity of the person; for example, documents such as driving license, identity card and passport containing information such as name-surname, Turkish identity number, nationality, mother's name and father's name, place of birth, date of birth, and sex as well as information such as tax ID number, SGK (Social Security Institution) number, signature details, vehicle license plate, etc.
Contact Data	Contact details; personal data such as telephone number, address, e-mail address, fax number, etc.
Physical Location Security Data	Personal data about the records and documents collected when entering and during the period of stay in physical premises; camera footage and records taken at the security checkpoint, etc.
Process/Transaction Security Data	Personal data such as IP address details, Website login and logout

	details, Password and code details, etc., which pertain to either the data subject or the Company and which are processed for technical, organizational, legal and commercial security of the Company while conducting the Company's activities.
Financial Data	Personal data such as bank account number, IBAN number, credit card details, financial profile, assets data, income details, etc.
Personnel Data	Any and all personal data processed to obtain information to serve as basis for establishment of personnel-related rights of Company employees or the natural persons having employment relationships with our Company.
Legal Action Data	Personal data processed for determination and follow-up of the Company's legal rights and receivables and discharge of its debts and those processed within the scope of compliance with legal obligations and Company policies.
Association Membership	If included in the CV of an employee candidate
Foundation Membership	If included in the CV of an employee candidate
Trade-Union Membership	If included in the CV of an employee candidate
Professional Experience	Personal data such as diploma details, courses attended, vocational training details, Certificates, Transcript details, etc.
Audio-Visual Data	Audio-Visual Data, Photographs and camera footage (except for footage included within the scope of Physical Location Security Data), audio records and data on the documents that are copies of the documents containing personal data
Philosophical Belief, Religion, Sect and Other Beliefs	Religious details stated in the religion field of the identity card if the data subject has submitted their old identity card to the Company for Company records.
Criminal Convictions and Security Measures	Criminal record obtained for creation of personnel file and internal audit purposes
Vehicle Data	Vehicle data collected by the Company to keep visitor logs and to ensure the physical premises security
Health Data	Data regarding disability status, blood type details, personal health details, data about the devices and prostheses used, etc.

6.4.2. Recipient Groups

Pursuant to the principles specified in the PDP Law and particularly, articles 8 and 9 of the PDP Law, the Company may transfer data subjects' personal data included within the scope of the Company PDP Policy to the recipient groups listed in the following table for specified purposes:

RECIPIENT GROUPS	DESCRIPTION	PURPOSE OF DATA TRANSFER
Business Partner	Third parties that the Company establishes business partnerships for the purposes such as conducting business operations	Limited to the purpose of accomplishing the objectives of the business partnership established
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (hereinafter “E.ON”) which are shareholders of the Company	For the purposes such as planning strategic measures about the Company’s business activities and maintaining the Company’s operations, including the Board of Directors’ resolutions and internal audit report.
Supplier	Parties providing services to the Company on a contractual basis and pursuant to the Company’s orders and instructions within the scope of conducting the business activities of the Company	Limited to the purpose of ensuring the provision for the Company of the necessary services outsourced by the Company from the supplier for performance of the Company’s business operations
Subsidiaries	Companies that the Company is a shareholder of	Limited to the purpose of ensuring performance of business operations which also require the participation of the Company’s subsidiaries
Sabancı Group Companies	All companies comprising Sabancı Group	Limited to the purposes such as planning strategies regarding the Company’s business activities and maintaining the Company’s operations as well as auditing
Legally Authorized Governmental Authorities and Agencies	Governmental authorities and agencies authorized to obtain information and documents from the Company pursuant to the provisions of the relevant legislation	Limited to the purposes as requested by relevant governmental authorities and agencies within the scope of their legal authorities

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

The Company takes any and all necessary measures according to the nature of the data to be protected as much as possible in accordance with Article 12 of the PDP Law in order to prevent unlawful disclosure, access, or transfer of or any other security deficits that may occur in relation to personal data. Related rules are provided in the Personal Data Storage and Destruction Policy.

In this context, the Company takes any and all necessary (i) organizational and (ii) technical measures; (iii) establishes an audit system within the company; and (iv) acts in accordance with the actions stipulated in the PDP Law in case of unlawful disclosure of personal data.

(1) Organizational Measures taken by the Company to ensure Lawful Processing of and to prevent Unlawful Access to Personal Data

- The Company trains its employees and raises their awareness about the legislation on protection of personal data.
- In case of any possible transfer of personal data, the Company ensures that clauses stipulating that the recipient of personal data will fulfil the obligations aimed at ensuring data security are incorporated into the contracts concluded with the parties to whom personal data are transferred by the Company.
- Personal data processing activities conducted by the Company are reviewed in detail; in this context, steps to be taken are identified to ensure compliance with the personal data processing conditions as stipulated in the PDP Law.
- The Company determines the practices to be implemented to ensure compliance with the PDP Law and regulates these practices by issuing internal policies.

(2) Technical Measures taken by the Company to ensure Lawful Processing of and to prevent Unlawful Access to Personal Data

- The Company takes technical measures, to the extent allowed by technology, for protection of personal data and the measures taken are revised and improved in parallel with the current developments.
- Specialized personnel are employed for technical issues.
- Audits regarding the implementation of measures taken are conducted at regular intervals.
- Software and systems are installed to ensure security.

- The authorization to access personal data processed within the Company is limited to the relevant employees according to the specified purpose of processing.

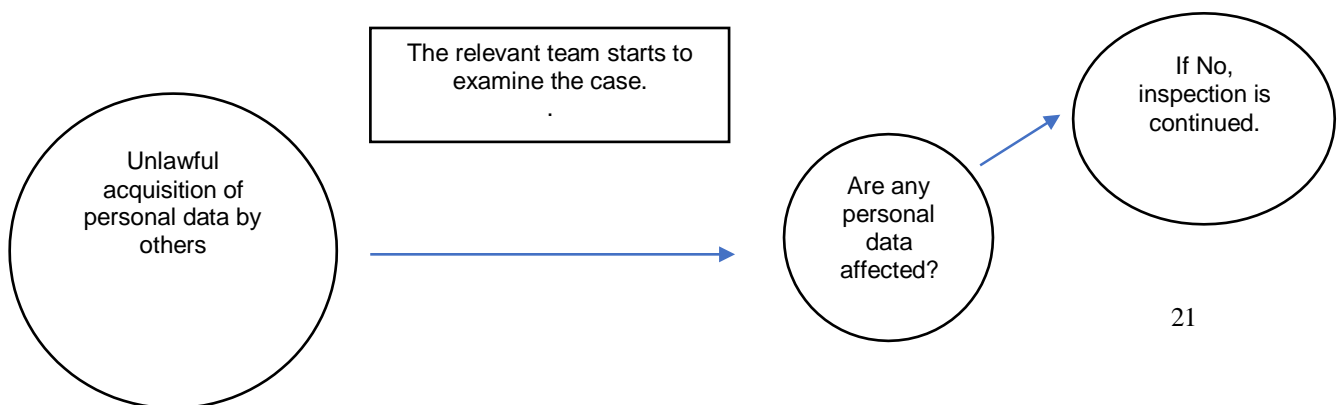
(3) Audits conducted by the Company for Protection of Personal Data

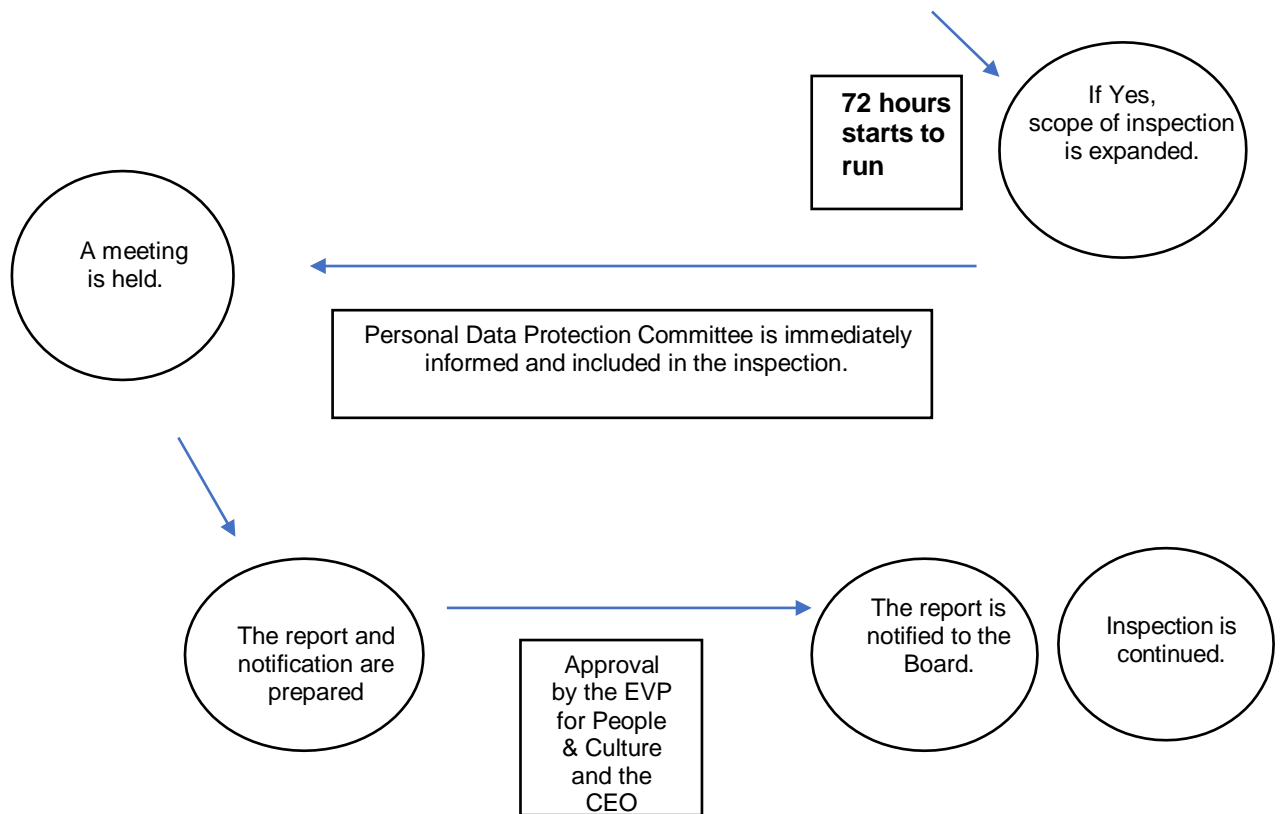
The Internal Audit Department of the Company audits the compliance of technical and organizational measures taken and the practices implemented by the Company to ensure the protection and security of personal data with the relevant legislation, policies, procedures and instructions, as well as their proper functioning and efficiency. The Internal Audit Department of the Company may conduct such audits either through its own organization or by commissioning external audit firms if and when deemed necessary. The results of audits conducted in this context are reported to the Internal Audit Committee, the CEO and the relevant function managers of the Company. Process owners are responsible for the regular follow-up of the actions planned in relation to such audit results. Process owners periodically submit follow-up and progress reports to the Internal Audit Department of the Company; and the Internal Audit Department conducts the follow-up, validation testing and audits for the actions included in such reports. Relevant executive units conduct the activities aimed at development and improvement of the measures taken for protection of data, without being limited to audit results.

(4) Actions to be taken in case of Unlawful Disclosure of Personal Data

In cases where any personal data processed by the Company are unlawfully accessed and acquired by others, this situation should be notified to the relevant persons and the Personal Data Protection Board (Board) within the shortest time possible. The said “shortest time” has been determined with a Board’s decision as 72 hours for notifications to be made to the Board.

Relevant units should act swiftly and in coordination with each other in order to manage this process in the best manner possible and to minimize the risks that may arise as a result of the Board inspections. Therefore, the flow chart to be followed in case of occurrence and identification of a data breach must be as follows:





Any unlawful acquisition by others of any personal data for which the Company acts as the data controller may primarily be determined by the Information Technologies unit. Such a breach may be identified as a finding as a result of the inspections conducted by the Internal Audit unit. In such cases or in case of identification of the breach by different units, the aforementioned data breach process must be initiated immediately. If it is identified that personal data have been affected by the data breach, the Personal Data Protection Committee is immediately included in the process and the situation is immediately notified to kisiselveri@enerjisauretim.com via e-mail.

Relevant matters, including, particularly, the assessments made, the number of people affected by the breach, the number of data affected by the breach, after-effects of the breach, and the measures to be taken are evaluated in the meeting to be held by the Personal Data Protection Committee. The committee may also include the officials and employees from the relevant units in the meeting, if deemed necessary. The information on data breaches, their effects and the measures taken are recorded. Meeting and assessment outputs are issued as a report; and submitted together with the draft notification to the Executive Vice President for People and Culture and the CEO for approval. After obtaining the said approvals, the report is shared with the Board.

In case of failure to notify the Board within 72 hours for justifiable reasons, the reasons for the delay are also explained to the Board together with the notification to be made. The “Personal Data Breach Reporting Form” which is available on the Board’s website is used for notifications to be made to the Board. If the information specified on the form cannot be provided at the same time, such information is gradually provided without delay.

Investigations about the breach are continued within the Company. Data subjects who are found to have been affected by the breach are contacted and informed within the shortest reasonable period possible. If the relevant person's contact address cannot be reached, notification is made using suitable methods such as posting on the Company's own website. If deemed necessary, public disclosure and information activities are carried out by obtaining the opinion of the Corporate Communications unit as well.

6.6. PROCESS OF COMPLIANCE WITH THE PERSONAL DATA PROTECTION LAW

The Company conducts a compliance process to ensure fulfilment of legal obligations under the PDP Law and relevant legislation and the compliance of the conducted activities with the legislation on protection of personal data, the maintenance and improvement of the established systems, identification of potential nonconformities, and determination of corrective actions to be taken and to increase awareness within the company by reporting all relevant issues. The rules regarding the compliance process have been specified in Enerjisa Üretim Compliance Manual and Compliance Policy and Procedure announced in relation to this process.

7. REVIEW

This Policy document enters into effect upon its approval by the Company's executive vice president for People and Culture. The Company's executive vice president for People and Culture is responsible for amendments to be made in the Policy and how it will be implemented, except for the revocation of the Policy. Amendments to this Policy can be made and implemented with the approval of the executive vice president for People and Culture.

Implementing rules to be issued in connection with this Policy, which will specify how the matters specified herein will be enforced with respect to specific issues shall be issued as a procedure. Procedures shall be issued and enforced upon their approval by the executive vice president for People and Culture.

This Policy is, in any event, reviewed at least once a year, and updated and revised with necessary changes, if any, after they are submitted to the approval of the executive vice president for People and Culture.

The Company acknowledges that applicable legislation shall prevail in case of any discrepancy between applicable legislation on the protection and processing of personal data and the Company PDP Policy.

The Company PDP Policy is published on the Company's website (www.enerjisauretim.com) and is accessible to personal data subjects. The amendments to be made in the Company PDP Policy in parallel with the amendments to be made in and new regulations to be issued under the relevant legislation shall be made available to and easily accessible by data subjects.

This Policy may not be copied or distributed without the written permission of the Company.