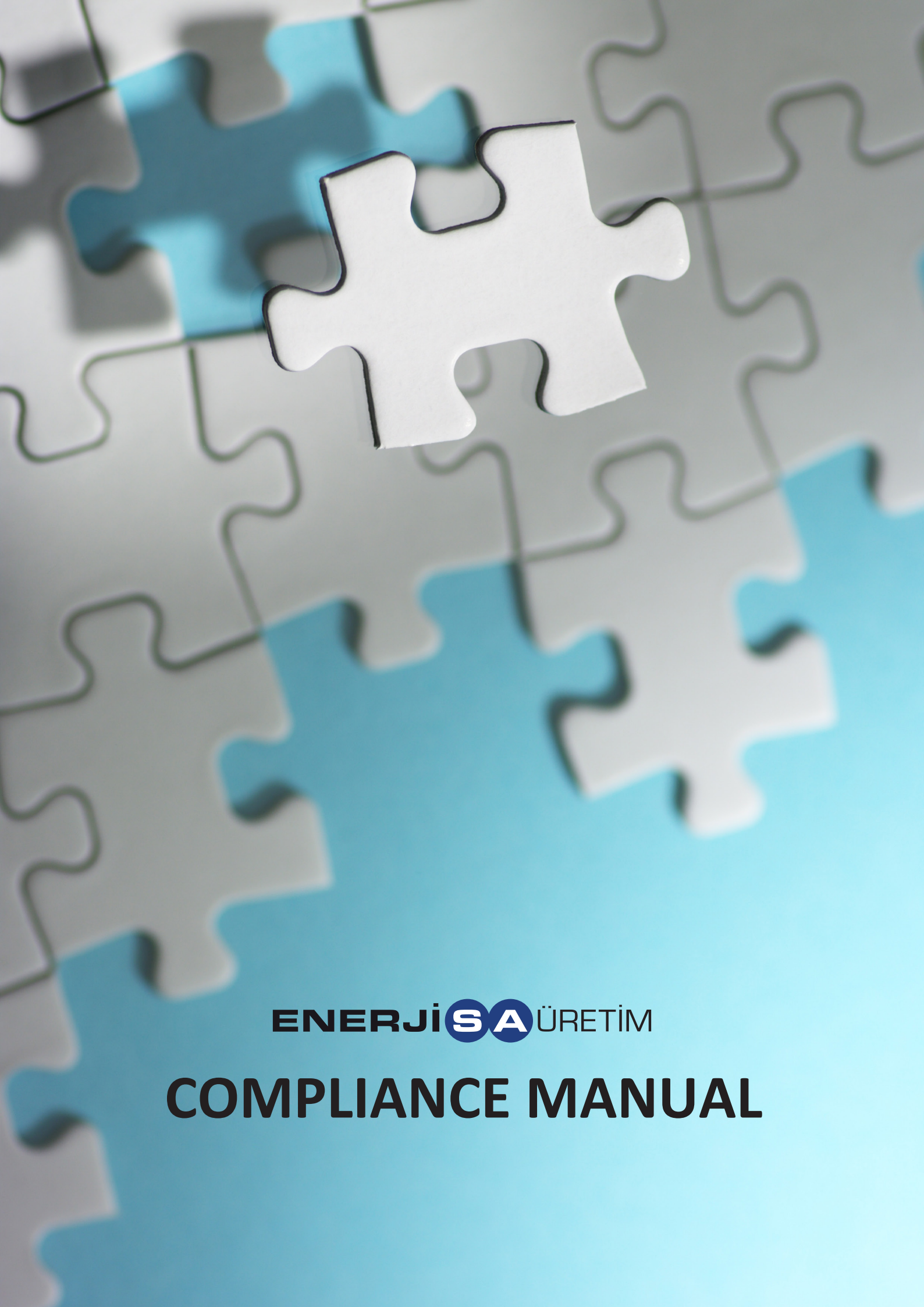


ENERJİSA ÜRETİM

COMPLIANCE MANUAL

TABLE OF CONTENTS

INTRODUCTION

Enerjisa Üretim Compliance Rules define compliance rules that should be observed by all employees within Enerjisa Üretim Santralleri A.Ş. organization and its subsidiaries*, rights of employees in this regard, and compliance criteria (values) and fundamental principles of the company. This document reflects Hacı Ömer Sabancı Holding (H.Ö. Sabancı Holding/SAHOL) Ethics Code (SA-Ethics) and common values of E.ON Compliance Rules, and complies with the applicable legislation (e.g. Competition Law, Energy Market Regulatory Authority, and Personal Data Protection Laws).

* Enerjisa Üretim Santralleri A.Ş. and subsidiaries shall hereinafter be referred to as the "Company".

Fundamental Principles of the Compliance Manual Rules

Compliance Principles

One of the principal compliance objectives of the Company is to implement Enerjisa Üretim Compliance Rules within the company and to ensure functionality of these rules. In this context, managers and employees have separate obligations to create a compliance culture and to ensure sustainability of this culture, and they all act in line with their respective obligations.

Confidentiality Principle

One of the objectives of the Company is to act with the awareness that information that would weaken competitive edge, employee rights and details, and agreements made with business partners are within the scope of "confidentiality", and to protect and keep these confidential, being aware of the importance and value of strategic and commercial secrets belonging to Enerjisa Üretim.

Legal Compliance

The company conducts all of its activities, both domestic and abroad, pursuant to both the legislation in force and international norms, and cooperates with competent public authorities and organizations if/when necessary in all of its activities and operations. In this sense, employees are prohibited from engaging in unlawful activities under any name whatsoever, including money laundering, as they fulfill their duties.

Compliance within the Scope of Competition Law

The company acts with the awareness of protecting market balance in the country and performs its activities pursuant to the principle of protecting fair trade and competition

between the actors in energy generation market. In this sense, the company avoids behaviors and actions disrupting competition, under any name whatsoever, outside the limits permitted by the legislation, including the Law no. 4054 on Protection of Competition.

Compliance within the Scope of Protection of Personal Data

The company places emphasis on the privacy of employees, as well as other employees, stakeholders, business partners, suppliers, and their employees to effectively protect personal data, the confidentiality of personal data belonging to these people, and aims to protect such data. In this sense, the Company processes personal data in a limited and reasonable manner in connection with legitimate purposes, pursuant to the applicable legislation, particularly the Law on Protection of Personal Data, and policies and procedures issued by the Company for protection of personal data.

Sustainability

The company operates in awareness of its responsibilities towards the society and the environment, with a holistic sustainability vision in line with global objectives, and with the purpose of continuous improvement as it fulfills these responsibilities. It evaluates economic, environmental, and social impacts of all activities and monitors preventive policies determined for prevention of issues and steps to be taken in this direction in regular intervals.

Internal and External Relationships

The Company:

- Creates a work environment for the employees, where there is equal opportunity, discrimination is prevented at all stages beginning from recruitment stages, which is open to full communication, increases diversity, and is respectful, thoughtful, and understanding.
- Treats all public institutions and organizations, administrative establishments, non-governmental organizations, and political parties equally, without expecting any benefit, as it conducts its activities.
- Conducts all activities with its customers with a proactive understanding focused on customer satisfaction to create mutual value, and aims to fully meet the expectation for uninterrupted and high-quality products and services.
- Conducts its relationships with suppliers within the scope of mutual diligence and good will, aiming for long-term cooperation based on solid foundations.

- Competes with other actors in the market only within legal and ethical areas, appreciates working in an honest and respectful work environment away from unfair competition, and conducts its activities in this direction.
- Maintains its relationships with the media on the basis of integrity and honesty by means of the Corporate Communications Department. In this sense, employees avoid making statements that would harm the reputation of the Company, lead to unfair competition, or provide personal benefit.
- Avoids taking unnecessary or unmanageable risks with an awareness of its responsibility towards its partners, ensures management within the scope of trust and honesty principles, aims for sustainable growth and profitability and manages company sources, assets, and work time with an awareness of efficiency.
- Within the scope of their responsibilities towards the society and humanity, they act sensitively by leading the way in social issues, and try to take part in non-governmental organizations, services in the interest of the public, and suitable activities.
- Conducts its activities within the scope of professional standards and ethical rules to uphold the reputation of the Company with an awareness of responsibility towards the names "Sabancı", "EON", and "Enerjisa Üretim".

Conflict of Interest

Employees act with the awareness that "avoiding conflicts of interest" is the primary principle that they should observe as they fulfill their duties and responsibilities. In this sense, employees shall not obtain personal benefit from individuals and organizations in business relationships with the Company by taking advantage of their offices or positions, or use name and reputation of the Company for personal benefit personally or through their relatives.

Other Rules and Responsibilities

- Representation of the Company: Employees may attend organizations, where they represent the Company, only if authorized to do so; and donate gifts and fees offered in these organizations to uphold the reputation of the Company.
- Political Activities: Employees cannot join any political organization using the name of the Company. In their personal memberships, they avoid attitudes that would harm the reputation of the Company or lead to conflicts of interest.
- Club, Association, and Cooperative Memberships: Employees cannot join any club, association, or cooperative using the name or sources of the Company, and avoid

attitudes that would harm the reputation of the Company in their personal memberships.

- Receiving and Giving Gifts/Donations/Sponsorships/Loans: The main principle for the Company is to avoid accepting gifts or benefits that could affect impartiality, decisions, and behavior of individuals, and preventing Company employees from making any attempt to this end. Gifts can be offered or received only in compliance with the Principles for Accepting/Offering Gifts, provided that such gifts are not in violation of morality, integrity, general customs, and the framework of business relationships of Enerjisa Üretim. Donation and sponsorship activities can be made only upon approval of senior management.
- Intellectual Property: The Company respects intellectual property rights of third parties during its activities and ensures that necessary procedures are carried out to protect the products subject to intellectual property rights that it develops.
- Working Outside the Company: Employees cannot accept any duty within any public or private organization or engage in any commercial affair directly or indirectly, other than their duties assumed in the Company under their contracts of employment, even outside working hours, without approval of relevant managers.
- Dress Code: Employees pay attention to their clothing and looks so that they will reflect the corporate culture.
- Hiring Relatives: Rules in Enerjisa Üretim Hiring Procedure are observed in this regard.
- Occupational Health and Safety: The Company is aware that its most valuable asset is "people" and, with this awareness, adopts all improvements, required to create a healthy and safe work environment and to minimize occupational accidents and diseases that might occur in this regard, as its primary objective.
- Substance Abuse: Employees are prohibited from being under the influence of substances such as alcohol and drugs during business hours, and disciplinary action is taken if such a situation is determined.
- Misconduct: Employees cannot gain benefits for themselves or their relatives by taking advantage of their titles and authorities, and obtain personal gains during activities of the company.
- Resource Utilization: The principle of "economy in every respect" was adopted regarding utilization of company resources, and the employees should use their time optimally in line with the same principle.

- Confidentiality of Rights Granted to Employees: Employees are aware that there are liable to keep all kinds of information confidential, including those regarding material benefits required by Human and Culture department to be kept confidential.

Anti-Money Laundering, Corruption, and Bribery

The Company adopts "zero tolerance" policy against bribery and any form of corruption, upholds the awareness that all kinds of bribery act defined as crime in the law cause irrecoverable and irreparable damages in reputation and standing of the company. In this sense, no Enerjisa Üretim employee or executive at any level may directly or indirectly offer, give, or authorize giving anything of material value to public servants in order to provide improper benefits to the Company. Company resources cannot be involved in acts of corruption, including money laundering.

Prohibition of Insider Trading

Company employees are aware that attempting to obtain any commercial benefit by using any information that is not disclosed to the public or providing such information to third parties, including direct or indirect trading on the stock market, (insider trading) is a crime under the law, and strictly avoid situations that might lead to insider trading.

Offering a Suitable Work Environment

The Company ensures that all employees work in an equal, fair, safe, and healthy work environment, without being exposed to discrimination for any reason whatsoever, and that differences co-exist in harmony. It respects private lives, personal spaces, material and moral assets of employees, observes their emotional, sexual, and physical immunity, is aware that violation of immunity is a crime, and does not tolerate such violence in any way.

Compliance Process and Resolution of Non-Conformities

Compliance process is conducted by Compliance-Legal department within the Company. Compliance Officer, determined by the Legal Advisor, offers guidance to be needed by employees in the course of compliance with the Compliance Rules and the principles set forth herein, reports situations that might lead to violations in the process to job owners together with the Legal Advisor, and follows up developments.

In this sense, employees and other stakeholders can notify situations, which they consider to be involving violations of compliance rules, to the Company by means of compliance reporting lines. Notifications are received by the Chief Legal Counsel and Compliance

Officer and submitted to the Compliance Board, established to resolve non-conformities. Notifications are resolved by the Compliance Board.

- Compliance Violation Notification E-mail: uyum.ihbar@enerjisauretim.com
- Compliance Violation Notification Line: (0216) 512 40 60
- Internal Extension: 4060

I. ENERJİSA ÜRETİM COMPLIANCE POLICY

As the Company, we commit to the highest standards of compliance with the laws, regulations, rules, and policies applicable to us. We aim to establish a structure involving measures and key processes required to ensure compliance and, accordingly, achieve the following fundamental objectives:

- Clear identification of responsibilities within the scope of compliance,
- Determination and evaluation of compliance liabilities,
- Encouragement of behaviors that ensure establishment and reinforcement of compliance, and showing no tolerance for behaviors that compromise on compliance,
- Performance of compliance analyses to check our fundamental compliance liabilities besides standard audits,
- Increasing awareness of employees, determination of their training needs, and organization of trainings for them within the scope of compliance,
- Monitoring our compliance activities and reporting performance,
- Regular review and continuous improvement of our compliance approach and tools.

II. ENERJİSA ÜRETİM COMPLIANCE PRINCIPLES

Enerjisa Üretim Compliance Board is responsible for ensuring an environment that will enable implementation of Enerjisa Üretim Compliance Rules.

Chief Legal Counsel and Compliance Officer, to be determined by the Chief Legal Counsel, are responsible for establishment of compliance rules, performance of analyses, and reporting non-conformities.

Enerjisa Üretim Compliance Board, Human and Culture, Compliance-Legal, and Internal Audit Departments are responsible for guaranteeing confidentiality of reports concerning violations in Enerjisa Üretim Compliance Rules, protection of employees against

harassment following relevant reports, ensuring job security of employees that submit notices, and ensuring work safety.

In addition to the obligation to observe the rules defined within the scope of Enerjisa Üretim Compliance Rules, all managers are responsible for fulfillment of the following additional obligations;

- Establishment of a corporate culture that supports Enerjisa Üretim Compliance Rules;
- Acting in line with the legislation and the Law on Protection of Personal Data,
- Acting in line with the Competition Law and applicable legislation;
- Serving as a model for employees regarding observance of Compliance Rules;
- Performance of their duties so that reputation of the company is kept at the highest level;
- Conducting instructive and informational activities regarding Enerjisa Üretim Compliance Rules, and guiding employees by offering full support in case of compliance complaints;
- Improving owned processes and resolving contradictions, if any, in accordance with Enerjisa Üretim Compliance Rules;
- Observing policies regarding occupational health and safety, and the protection of environment and nature against potential damages, and ensuring that the personnel work in compliance with these rules; and
- Denying any discrimination (religion, ethnicity, gender, political matters, native language, etc.) between the employees for any reason whatsoever.

Company employees are responsible for fulfillment of the following obligations;

- Acting in line with Enerjisa Üretim Compliance Manual;
- Acting in line with the legislation and the Law on Protection of Personal Data;
- Acting in line with the Competition Law and applicable legislation;
- Performing their duties pursuant to fundamental moral and humane values;
- Acting in accordance with procedures, policy documents, and workplace practices that regulate work flows and practices of the Company;
- Upholding reputation of the Company;
- Not gaining improper benefits, accepting and offering bribes by any means from individuals and organizations, for any purpose whatsoever;

- Not engaging in any behavior, declaration, or correspondence that would bind the company, unless explicitly authorized;
- Not engaging in behaviors that would disturb and/or harm other employees, not disrupting harmony in the workplace;
- Taking care of all tangible and intangible properties of the Company, including information and information systems, as if these were their personal property; protecting these against potential loss, damage, misuse, abuse, theft, and sabotage;
- Not utilizing work time or company resources directly or indirectly for personal gains and/or political activities and interests;
- In case of any actual or suspected violation of Enerjisa Üretim Compliance Rules, reporting the matter to the Chief Legal Counsel and Compliance Officer in writing or through Compliance Violation Notification Channels;
- Working in cooperation with Enerjisa Üretim Internal Audit Department personnel and Compliance-Legal department during compliance-related investigations.

In this scope, Employees are responsible for taking swift and consistent action against Enerjisa Üretim Compliance Manual violations. This can be ensured only by correctly assessing the situation. As it is not possible to forecast every situation, it is quite important to have a method for approaching how to resolve a new question or issue that might arise. Employees consider the following matters in the presence of a new question or issue:

- Employees should obtain all data regarding the situation. Employees should obtain all kinds of data to the highest extent possible to be able to make a correct decision in a situation regarding compliance.
- Employees should identify exactly what is expected of them, and whether there is a situation that might cause non-compliance. Employees can focus on the correct question, and therefore the most suitable alternate solutions for the question, upon making a correct identification in this regard.
- Employees should always adopt a prudent approach in resolution of issues.
- As there might be joint roles and responsibilities in some cases, Employees should determine whether they have authority concerning the present question or issue.
- Employees may consult their unit manager regarding the situation.
- If employees believe that it would not be appropriate to consult with their unit manager regarding the situation or if they feel uncomfortable about referring the situation to the unit manager, they may refer the situation to the Chief Legal

Counsel and the Compliance Officer or notify the situation by means of the Compliance Violation Notification Channels specified in the Compliance Procedure. This is a free hotline, which is accessible 24/7. (See Compliance Procedure)

It is ensured for Employees to make Compliance Violation Notifications safely and without any fear of sanctions. Notifications to be made through any of these channels are protected in strict confidentiality. If the situation requires concealing identity of the employee, the Employee's identity is kept confidential. The Company does not permit any sanction or retaliation against the Employee due to Compliance Violation Notifications made in good faith.

- The Employee may direct any question regarding implementation and interpretation of the Enerjisa Üretim Compliance Manual to the Chief Legal Counsel and the Compliance Officer.
- In case of Employees have doubts about what do to regarding the situation, they should always receive guidance/assistance from the Compliance Officer or their unit manager before acting.

III. ENERJİSA ÜRETİM COMPLIANCE RULES AND PRINCIPLES

1. CONFIDENTIALITY PRINCIPLE

Confidential information involves information that might lead to competitive disadvantage for the Company and its shareholders, trade secrets, financial and other information that have not been disclosed to the public yet, information pertaining to personal rights of the personnel, personal data of our employees, customers, and stakeholders, as well as information that we are obliged to protect pursuant to the "confidentiality agreements" made with third parties.

Employees of the company take care to protect confidentiality and private data of customers, employees, and other relevant individuals and organizations in relationships with the Company. They protect confidential information regarding activities of the Company, use such information only in line with the purposes of the Company, and disclose such information only to relevant parties within the scope of determined authorities. Such information cannot be disclosed to third parties, unless required to be disclosed to Public Authorities and in accordance with the Legislation.

Such information cannot be modified, copied, and destroyed. Necessary measures are taken to strictly retain, store, and prevent revelation of information. Modifications on the information are logged by the retaining department/unit with a modification history.

Employees of the Company cannot remove any written, visual, or verbal information, document, and work such as projects, software, reports, procedures, including financial data and confidential information of the Company, from the company or disclose these to third parties. Authorization of Information Security Department and relevant deputy general manager must be obtained with regard to confidential information that should be removed from the Company.

Every employee observes the policies and procedures announced by the Information Technologies Office.

In this context; employees are obliged to avoid responding to requests for information received from third parties, categorized as confidential data, without approval of the relevant deputy general manager, and show due diligence to ensure truthfulness of declarations made and reports submitted by the Company.

Confidential information of the Company cannot be discussed in dining halls, cafeteria, elevator, shuttle buses, and similar public locations, or shared on social media accounts and mobile phone apps. Information can be shared on social media accounts and mobile applications of the Company only by authorized personnel, within the scope and on time permitted in Enerjisa Üretim Social Media Procedure.

Confidential information is classified by the degree of confidentiality, which is clearly indicated in the contents of information. Employees of the Company know the degrees of confidentiality of information obtained as part of their jobs, and act in line with such degrees of confidentiality. In case of any doubt regarding the degree of confidentiality, the highest degree of confidentiality is assumed and opinion of relevant manager is taken when necessary.

If confidential information is kept on digital environment, relevant document should be labeled with a data label indicating required confidentiality level. If it is necessary to communicate these documents by e-mail, it is recommended to label the relevant e-mail at least at the level of the document with the highest degree of confidentiality among attached documents.

Passwords for computers, telephones, tablet PCs, as well as all kinds of data storage devices and software should not be shared with internal or external parties. Every employee is responsible for data security of desktop and/or laptop computers, mobile phones, and tablet PCs allocated and entrusted to them. Accessible personal data should be used in accordance with the LPPD and Company policies and procedures. Passwords,

user codes, and similar identifier information used to access company information are kept confidential, and these are not disclosed to any person other than authorized users.

Automobiles allocated to employees for only business purposes and devices such as computers, tablet PCs, radios, and mobile phones allocated to employees cannot be used in violation of activities of the Company and the rules set forth in the Compliance Manual. Every employee is liable to show utmost care to protect these devices, entrusted to them, against situations such as loss/theft/damage, to protect data security of these, and to report unwanted incidents primarily to their line manager and IT department, and then security authorities (in case of theft and loss).

Internal Audit Department is exclusively authorized to inspect relevant personnel, as well as the logs of devices and software (laptop computer, external data storage device, mobile phone, tablet PC, e-mail, Skype, SMS) allocated by the company for use by the personnel in question if deemed necessary within the scope of compliance investigation activities. These records can be inspected upon a written request to be submitted by the department in question to the Information Security Department. This authorization can by no means be delegated to another unit and data cannot be disclosed to internal/external third parties. In this regard, Internal Audit Department is exclusively authorized pursuant to the precedents of the Constitutional Court and the Supreme Court, applicable articles of Enerjisa Üretim Information Security Commitment Letter, LPPD, and applicable legislation.

Employees of the Company cannot share personal and/or financial data of customers, suppliers, and other company employees for purposes that are not related to business and/or with unauthorized third parties. During this process, LPPD and applicable Company policies and procedures are considered together. This obligation is valid also for former employees of the company, during the period after leaving the company.

If information is shared with third party individuals and / or organizations for the interests of the Company, a confidentiality agreement is signed or written confidentiality commitment is obtained beforehand from the other party with regard to information sharing to guarantee security and protection of information shared with these individuals and organizations, and understanding of relevant responsibilities.

Personal information such as wages and side benefits, which reflect company policy and which are private, are confidential and they cannot be disclosed to any party other than the authorities. Information belonging to the personnel are sent privately. The personnel cannot disclose such information to other parties or pressure other employees to disclose the information.

Abovementioned obligations concerning confidentiality remain in force for employees, who quit their jobs for any reason, during the period after leaving the company.

2. LEGAL COMPLIANCE

All employees of the company must work in full compliance with international norms and the provisions of national laws, including anti-money laundering, and cooperate with competent authorities if/when necessary. They must fulfill their obligations in compliance with both applicable laws and general practices. They are by all means prohibited from getting involved in any illegal activity as they fulfill their responsibilities or perform their daily jobs, and act, in any way, in violation of the legislation. Any violation of the legislation, corporate regulations and principles, or Compliance Rules can be subject to a compliance violation investigation and sanctions set forth in applicable laws and regulations.

Legislative compliance process is conducted diligently and in detail within the Company. It is aimed to conduct any follow-up with regard to the legislation, to notify amendments to the legislation to relevant departments, to identify potential non-conformities, to determine corrective actions to be taken, and to increase awareness within the company by reporting any relevant matter.

This process aims to prevent any sanction and risk that might arise from non-conformity with the legislation.

Compliance-Legal Department is responsible for the implementation of Legislative Compliance Process.

Changes in the legislation are currently monitored by the Compliance-Legal Department by means of both the Official Gazette and official websites of Regulatory Bodies. Monitored regulations are circulated as main titles weekly by e-mail to all Enerjisa Üretim employees. Besides regulatory changes that are circulated on a weekly basis, regulations that significantly and primarily affect the company are separately notified on the date of issuance in the Official Gazette.

A separate regulation meeting is held every week to conduct legislation monitoring process better, and matters concerning changes in the legislation and the effects of changed legislation on our company are evaluated and discussed weekly with relevant business unit managers. During such meetings, the matter is escalated to senior executives and it is ensured that action is taken regarding the process to reflect recently introduced regulation in the legislation or legislative changes to operations of the company.

Regulatory practices are monitored and implemented in respective fields of business of every department.

A list of all regulations that must be observed and that affect business processes was drawn by the Compliance-Legal Department. Compliance-Legal Department demand all business units to file semi-annual reports on Compliance Catalog within the scope of regulatory compliance to determine that applicable regulations are implemented correctly. This catalog contains company details, compliance definition, details of department and manager affiliated with compliance owner, relevant law and legislation details, affected procedure details, monitoring interval, definition of present non-compliance, if any, and actions to be taken, as well as details on deadline of these actions and sanctions to be imposed.

Compliance-Legal Department collects the information, provided in the abovementioned compliance catalog, from relevant departments in every six months. As a result of this analysis, Chief Legal Counsel and Compliance Officer report existing or potential non-conformities, sanctions, and actions to be taken to the CEO and affiliated deputy general managers in ELT or Compliance Board meetings.

Compliance-Legal Department inquires relevant business units whether departments have taken the actions that should be taken in this process, and checks implementation thereof. In case of non-compliance, the situation is reported again to the Compliance Board.

All details regarding Legislative Compliance process are given in Enerjisa Üretim Compliance Policy and Compliance Procedure given in Annex-1.

If the Company operates in international markets, operations of the company may be subject to the laws and regulations of different countries. In case of uncertainties regarding business values in different countries, established regulations in the relevant country should be observed in the first place. If regulations in the country and/or countries, where business shall be conducted, might lead to undesirable consequences on the activity to be performed on international arena in terms of the values specified in this manual, it should be attempted to find solutions pursuant to the compliance rules and procedures.

3. COMPLIANCE WITH COMPETITION LAW AND APPLICABLE LEGISLATION

Law no. 4054 on the Protection of Competition and all applicable regulations are observed with regard to full compliance concerning competition, which is one of the fundamental principles of our Company.

Rules of the competition law are strictly observed, also in consideration of economic foundations and practical applications, in relationships with our competitors and suppliers,

particularly in communication and interactions with companies within the scope of wholesale of electricity, to protect the reputation of the Company, which is the joint responsibility of employees.

Action is taken with the awareness that potential violations of competition would have serious consequences for reputation and brand value of the Company, taking into account that companies face hefty fines and damage claims due to violations of the competition law, while individual administrative fines can be imposed on employees as well.

All employees should fulfill their duties and act fully in compliance with the rules to prevent consequences in violation of competition and sanctions. All employees are responsible for the implementation of the Procedure for Compliance with Competition Law, given in Annex-2, required to uphold corporate culture and reputation of the Company.

4. COMPLIANCE WITH THE LAW ON PROTECTION OF PERSONAL DATA (LPPD) AND APPLICABLE LEGISLATION

The Company acts in compliance with the legislation concerning the Law on Protection of Personal Data.

In accordance with the applicable legislation and policies;

- Processing purposes are explained to relevant person before processing personal data, and explicit consent of relevant person is obtained if it is legally required.
- Administrative and technical measures, stipulated in the legislation, are taken by relevant departments to ensure confidentiality and safety of personal data and to prevent unlawful use.
- Processed personal data are stored for the period stipulated by the applicable legislation or the period required for the purpose for which the personal data are processed.
- Personal data are deleted, destroyed, or anonymized if stipulated period expires or processing purpose ceases to exist or upon request of the relevant person.
- Employees of the company are obliged to perform their jobs in compliance with these rules and measures.

Relevant rules are given in detail in the Policy for Protection and Processing of Personal Data of Employees, Personal Data Protection and Processing Policy, Personal Data Storage and Destruction Policy, and Private Personal Data Protection Policy. (Annex 3: Policies for Protection of Personal Data)

Personal Data Protection Committee ("Committee") was established to ensure necessary coordination within the Company to ensure, maintain, and sustain compliance with the personal data protection legislation. Personal Data Protection Committee is responsible for ensuring uniformity between units of the Company, as well as maintenance and improvement of systems established to ensure compliance of conducted activities with the personal data protection legislation:

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

- To prepare and implement essential policies regarding protection and processing of personal data of employees,
- To resolve on how implementation and inspection of policies on protection and processing of personal data of employees shall be performed and, accordingly, to make internal assignments and ensure coordination,
- To determine steps that should be taken to ensure compliance with the LPPD and applicable legislation, to observe implementation and ensure coordination,
- To increase awareness within the Company and before institutions, with which the Company cooperates, regarding protection and processing of personal data,
- To identify risks that might arise in personal data processing activities of the Company, to ensure that necessary measures are taken, and to offer recommendations for improvement,
- To design and ensure performance of trainings on protection of personal data and implementation of policies,
- To resolve on applications of personal data subjects at the highest level,
- To coordinate performance of information and training activities aimed at ensuring that relevant parties are informed about personal data processing activities of the Company and their legal rights,
- To prepare and implement amendments to essential policies regarding protection and processing of personal data,
- Monitoring developments and regulations on protection of personal data, making recommendations to the senior management in respect of necessary actions to be taken in operations of the Company in line with these developments and regulations,
- To manage relationships with the Personal Data Protection Board and Personal Data Protection Authority,

- To fulfill other duties to be assigned by Company management with regard to the protection of personal data.

5. COMPLIANCE IN SUSTAINABILITY PROCESSES

The Company addresses sustainable energy generation and trade at top level and considers it to be central to all of its activities, in line with its mission of "generation of energy for a better future by respecting lift". Sustainability approach of the Company is to consistently offer the value, created for its stakeholders, not only today, but also in the future. Therefore, resources, investments, operations, and goals for change are managed so as to ensure long-term continuity. The Company manages all positive or negative environmental, social, and economic effects that might arise in areas where it operates, with this sustainability approach. Sustainability approach is a holistic approach that should be integrated by the Company in decision-making and working manners of all employees. Accordingly, it is important for all employees to adopt and follow all studies conducted with regard to sustainability. In this context, relevant policies and rules to be determined by the Environment and Sustainability Department should be observed.

6. INTERNAL/EXTERNAL RELATIONSHIPS

6.1. **Relationships with Employees:** An environment where employees are treated respectfully, considerately, and tolerantly, and which contributes to ensuring full communication at all levels, is created. Common goals of the Company include developing team spirit within the Company and protecting its corporate identity. The Company ensures that personal rights of employees are fully and correctly exercised, treats employees honestly and fairly, and commits to a non-discriminatory, safe, and healthy work environment. The Company makes necessary endeavors for personal improvement of employees, support them in volunteering for social activities in which they will participate with a sense of social responsibility, and observes the balance between work life and private life.

6.2. **Relationships with Public Institutions:** The Company treats all public institutions and organizations, administrative establishments, non-governmental organizations, and political parties equally, without expecting any benefit, as it conducts its activities and operations, and fulfills its obligations with this sense of responsibility. In this sense, relationships established and maintained by the Company with the state, political organizations, unions, and other organizations should be based on the principles of maximum integrity, honesty, equality, and independence. Every employee should avoid all kinds of behavior that could make an impression that favors or direction of decisions of the other party are requested or offered. They should perform their representation duties as deemed proper for

Enerjisa Üretim, E.ON and SAHOL brands, regardless of their own political views, in relationships with public authorities. Maximum attention should be paid to this matter, particularly in relationships with public authorities and institutions (e.g. Ministry of Energy and Natural Resources, Energy Market Regulatory Authority, Turkish Electricity Transmission Corporation, etc.) that are of great significance for the business of the Company.

6.3. Relationships with Customers, Suppliers, Consultants, and Competitors: Employees of the Company are liable to avoid any action and behavior that would have negative impact on the corporate image in relationships conducted on behalf of the Company with customers, shareholders, subsidiaries, and other companies. Especially employees, who need to conduct direct relationships within the scope of their job definitions, should pay maximum attention to this matter.

In parallel with this, maximum attention should be paid to using the standard contractual texts of our Company, which are prepared by the Compliance-Legal Department and which protect the interests of the Company in the broadest sense, in relationships conducted on behalf of the Company. In case of any change (addition/deletion/modification) in these texts, opinion of Compliance-Legal Department must be obtained. Opinion of Compliance-Legal Department must be obtained in respect of all contracts other than the standard contractual texts of our Company, and contracts should be adjusted in line with such opinion.

Relationships with Customers: The Company conducts all of its activities with a proactive approach that is focused on customer satisfaction and that responds to needs and requests of customers as soon and as accurately as possible. It offers services on time and under promised conditions, and approaches customers pursuant to the rules of respect, honor, fairness, equality, and courtesy. It acts fairly and respectfully as expected from a good business/service provider, and exercises due diligence to fulfill our obligations on time. It diligently protects the confidential information of individuals and organizations in business relationships with the Company, as well as our business partners.

Relationships with Suppliers: It is a priority for the Company to develop effective and efficient relationships with its suppliers. The Company observes Company policies and procedures, professional standards, commitments, and ethical rules in selection of suppliers. Cost, delivery dates, flexibility, high quality, OHS and Environment approach, and diversity of additional services were determined as important criteria in selection of suppliers. Suppliers that harm public morality, environment and public health are not dealt with.

Relationships with Consultants: Terms of confidentiality should be clearly defined with an agreement in relationships with individuals or companies, from whom consultancy services are received. On the other hand, the personnel, whose assignment by the Company has expired, can be temporarily appointed in the capacity of consultant only upon proposal of the relevant Deputy General Manager, and approval of Human and Culture Deputy General Manager and CEO.

Relationships with Competitors: The Company effectively competes in only legal and ethical areas, avoids unfair competition, and supports activities aimed at achieving the competitive structure targeted within the community. The Company is liable to provided necessary trainings in this regard to all employees, and the employees are obliged to fully attend relevant trainings and take all kinds of relevant measures.

All employees of the Company must avoid any act, activity, and practice that might violate the Competition Law. Policies and rules regarding the Competition Law are announced by the legal office of the Company. Relevant rules are set forth in policies within the scope of the Competition Law.

Accordingly, the Company;

- Cannot make agreements or display behavior, which directly or indirectly aim to prevent, disrupt, or restrict competition, or which have or might have this effect, with competitors or other individuals or organizations, beyond the limitations stipulated by the legislation.

- Cannot abuse its dominant position in case it is dominant in a certain market alone or together with other enterprises.

- Cannot engage in discussions and information exchange aimed at determining market and/or competition conditions together with competitors. Cannot conduct discussions and procedures that might lead to the abovementioned situations or that might be characterized as such in association, assembly, chamber, professional society etc. meetings, as well as other private or professional meetings and discussions attended in representation of the Company.

6.4. Relationships with Other Individuals and/or Organizations in Business Relationships with the Company

Private business relationships cannot be established with customers, subcontractors, or suppliers of the Company, as well as other individuals and/or

organizations in business relationships with the Company, no personal loan, money, and/or goods/services can be received from these, and no loan and/or goods/services can be offered to other individuals and/or organizations in business relationships with the Company. No action can be taken beyond the knowledge of customers, even if such actions might be in favor of customers, weaknesses of customers cannot be taken advantage of, and no profit can be sought by providing incomplete or inaccurate information to customers in relationships with customers.

Board members, managers, executives, or representatives of the Company cannot be the target of and/or subject to any international or local economic or commercial sanction by institutions such as US Department of Treasury Office of Foreign Assets Control (OFAC), US Department of State, United Nations Security Council, European Union, Her Majesty's Treasury, Hong Kong Monetary Authority, Central Bank of the Republic of Turkey, Banking Regulation and Supervision Agency, Capital Markets Board and Republic of Turkey Ministry of Treasury or Ministry of Finance Financial Crimes Investigation Board, or be a shareholder of entities subject to sanctions, or managed by such entities, or be the target of and/or subject to economic or commercial sanctions of their governing jurisdiction. The Company cannot engage in any commercial and economic relationships with a country associated with economic or commercial sanctions imposed by the institutions specified in this article.

6.5. **Relationships with Printed/Visual Media and Social Media:** All relationships with press and media are conducted by Enerjisa Üretim Corporate Communications Department. Our employees must avoid any situation that might lead to any speculation or negative consideration about the company or any practice and behavior that could negatively impact the reputation and stability of the company (including posts on social media regarding the Company) in relationships of the Company with press and media. Furthermore, Enerjisa Üretim Social Media Procedure is considered to be fundamental in representation of the corporate structure on social media. Approval of senior management of the Company must be obtained before making any statement to any broadcast corporation, having an interview, participating as speakers in seminars, conferences, etc. No personal gain can be obtained from these activities.

6.6. **Responsibilities Towards Our Partners:** Sustainability of the Company is prioritized and sustainable profitability is aimed in line with the goal of the Company to create value for our partners. Financial discipline and accountability are taken into consideration in activities of the Company, and resources and assets, as well as work time of the Company, are managed with the awareness of efficiency

and economy. The Company pays attention to increasing competitive strength and investing in areas which have growth potential and which would offer the highest yield for invested resources. Timely, accurate, complete, and understandable information is provided with regard to financial statements, strategies, investments, and risk profile in disclosures to the public and the shareholders.

6.7. Responsibilities Towards the Society and Humanity: Our Company is sensitive about protection of democracy, human rights, and environment, educational and charitable works, and prevention of crime and corruption. The Company acts sensitively by leading the way in social issues, and tries to take part in non-governmental organizations, services in the interest of the public, and suitable activities. The Company acts sensitively in line with traditions and cultural aspects in Turkey and countries where it conducts international projects.

The Company acts sensitively by leading the way in respect of its responsibilities towards the society and humanity, and takes all kinds of measures stipulated by the legislation to prevent its fundamental activities from having negative impacts on the environment. It improves awareness and sensitivity of its employees in this regard.

6.8. "Responsibilities Towards the Names "Sabancı", "Eon", and "Enerjisa Üretim": The Company acts with the awareness of upholding its reputation. The Company offers its services pursuant to the policies of Sabancı/EON/the Company, professional standards, its commitments, and ethical rules, and commits to the fulfillment of its obligations. It pays attention to offering services in areas where the Company is professionally competent and it is expected to be competent, it aims to work with customers, business partners, and personnel that conform to the criteria of legitimacy. Employees state only views of the Company rather than their own opinions in respect of every matter for which Sabancı/EON/the Company is represented before the public. Employees act with the awareness that their opinions can be identified with Sabancı/EON/Company when they state their opinions regarding their duties and/or based on their personal preferences in relationships with the media or on social media platforms.

7. CONFLICT OF INTEREST

Conflict of interest means a situation where personal interests or an employee and/or one or several family members and corporate interests may affect each other positively or negatively. In this sense, employees shall by no means engage in business relationships that provides reciprocated or unreciprocated benefits with their family members, friends,

or other parties with whom they have relationships. One of the most important responsibilities of all employees is to avoid using resources, name, identity, and power of the company for personal benefit, and to avoid situations that might have a negative impact on the name and reputation of the company. Employees must commit to avoiding any situation and relationship that involves any potential or actual conflict of interest. Company employees are liable to avoid any act which could provide interest for them, their relatives, and/or any third party in vendor selection processes.

Any situation that poses the risk of conflict of interest should be notified by the relevant employee to their direct supervisor and to the Company via Compliance Violation Notification channels.

8. OTHER RULES AND RESPONSIBILITIES

8.1. Representation of the Company: Employees may give speeches or write professional articles about matters that are not related to the company, its activities, and its policies. Approval of relevant deputy general manager and Chief Legal Counsel must be obtained to use the name of the Company in any activity that is not led by the Company.

Any fee to be received as a result of duties performed in any association, employers' union, and similar non-governmental organization in representation of the Company shall be donated to the relevant institution or channels to be indicated by the relevant institution. Payments made by third parties to a Company employee as a seminar speaker fee or against similar services shall likewise be donated to the relevant institution or channels to be indicated by the relevant institution. These individuals may receive awards, plates, and similar gifts other than cash, given as a token of that day and of symbolic value.

8.2. Political Activities: Employees of the Company should not join political organizations using name of the company, their position within the company, their title, and resources belonging to the company when they are performing their jobs. Managers cannot ask their personnel to perform a political task or join a party. However, in case of personal membership, they are obliged to avoid any activity that might be against interests and reputation of the Company. Employees cannot engage in any political activity during work hours and they cannot occupy their colleagues with these activities. Such activities should not affect work hours and schedule; there should not be any conflict of interest with their duty performed in the Company and practices and approaches of other Sabancı/EON companies.

8.3. Club, Association, and Cooperative Memberships: Employees of the Company cannot join any club, association, or cooperative in the name and on behalf of the company or by using their position or title within the company and resources belonging to the company. However, in case of personal membership, they are obliged to avoid any activity that might be against interests and reputation of the Company. Such activities should not affect work hours and schedule; there should not be any conflict of interest with their duty performed in the Company and practices and approaches of other Sabancı/EON Group companies.

8.4. Receiving and Giving Gifts/Donations/Sponsorships/Loans:

Receiving Gifts and Donations:

It is essential for the Company and its employees not to accept gifts or benefits that might affect their objectivity, decisions, and behaviors, and to avoid offering gifts and benefits that might have such effects on third party individuals and organizations.

No gifts or other benefits can be accepted from existing and/or potential customers / vendors partners, and/or other individuals and organizations in business relationships with our Company, except for the circumstances specified in the Compliance Manual. Company employees cannot accept unreciprocated money or loans, or have their travel expenses, event expenditures, or other payments covered inexpediently by sub-employers, suppliers, consultants, competitors, or customers. No gifts or benefits, which are indirectly or explicitly contingent on a reciprocation, can be accepted. Accepting, giving, or offering bribe and/or commission is unacceptable under any circumstances.

Employees may accept and/or offer gifts;

- In line with the business objectives of the Company,
- In compliance with applicable legislation, and
- As outlined below by the "Principles for Accepting / Offering Gifts" permitted / determined by the Compliance Board, or they may accept to be subject to special treatment.
- Employees of the Company may offer and accept gifts, entertainment, compliments, and food at standards deemed acceptable in the business world.
- Awards, plates. similar gifts other than cash, as a token of that day and of symbolic value, can be accepted in seminars and other organizations attended as a representative of the Company.

Other gifts, benefits, holidays, discounts other than abovementioned circumstances and money can be accepted without approval if the value of received gifts is less than the amount stipulated in "Enerjisa Üretim Gift, Donation and Sponsorship Policy", for every calendar year and offering individual / organization, provided that they are in compliance with the Principles for Accepting / Offering Gifts.

The Company may accept suitable products and services, on the condition that they comply with the Principles for Accepting / Offering Gifts, as gifts and offer products and services suitable for the culture and values of the recipient pursuant to the approval of the relevant Deputy General Manager of the Company.

Company personnel cannot request gifts from other individuals and/or organizations in business relationships with the company directly or by way of implication, or accept any undue gift, money, check, property, free holiday, special discounts, etc. that would put the Company under obligation. They cannot accept personal assistance and/or donations from any individual or organization in business relationship with the Company.

In general, gifts in violation of morality, integrity, general customs, and the framework of business relationships of the Company should be returned with the expression "Inappropriate Pursuant to the Principles for Accepting/Offering Gifts"; if gifts are not retrieved by the giving party or if returning the gift has the potential to negatively affect current relationship, relevant gifts should be sent to the Compliance Board to be used for donations and rewards.

No aid or donation shall be accepted from any individual or organization in business relationships with the Company, and information pertaining to donation and aid offers must be disclosed to the affiliated manager. Relevant Manager is liable to notify the situation to the Compliance Board or Compliance-Legal Department.

In exceptional cases where local customs require mutual gift giving above values determined in the company policy, such gifts can be accepted and offered only on behalf of the Company upon approval of the Compliance Board. In any case, gift exchange should be made as deemed proper in the local culture.

<u>Sponsorship, Offering Gifts, and Donations:</u>

CEO and relevant deputy general manager approve gifts and promotional materials that can be offered on behalf of the Company to customers, business partners, or sales agents to maintain business relationships in accordance with the principles

determined by the management of the Company. There is no need for further authorization to distribute approved gifts and promotional materials. Principles for Accepting / Offering Gifts, applicable to accepting gifts, invitations, and donations, are also applicable to offering these.

Donations can be made to public institutions and organizations on behalf of the Company within the limits of the Company signing authority, upon approval of CEO and relevant deputy general manager, to support activities contributing to economic and social development, show awareness of social causes, and support positive improvement of the community, provided that such donations serve social development and public interest. The Company cannot donate to political parties, politicians, or candidates running for political offices.

Sponsorship can be provided on behalf of the Company within the limits of the Company signing authority, upon approval of CEO and relevant deputy general manager, for certain causes such as sports activities, cultural and scientific activities, or educational activities.

All kinds of loan, donation, and similar exchanges between company employees in superior-subordinate relationships and between employees and customers, vendors, and contractors of the Company.

8.5. **Intellectual Property:** The Company ensures that legal procedures are initiated and completed in due time to secure intellectual property rights for newly developed products, processes, and software. It avoids -intentional- unauthorized and undue use of patents, copyrights, trade secrets, brands, computer programs, or other intellectual and industrial property rights owned by other companies.

8.6. **Working Outside the Company:** Employees of the Company cannot work for another individual and/or institution within/outside business hours to obtain additional income or a similar benefit without written approval of relevant Deputy General Manager of the department within the scope of their employment contract, Deputy General Manager Human and Culture, and Chief Legal Counsel. They cannot engage in activities that require them to be considered as "merchant" or "artisan" by direct and indirect means. However, working in another company against remuneration outside working hours can be approved exceptionally by the employee's direct superior. The Employee should make a written notification to the Deputy General Manager for their department, Chief Legal Counsel, and Human and Culture Department in this regard.

Such request of the Employee can be accepted only if;

- There is no conflict of interest with their assignment by the Company and practices of other Sabancı/EON Group companies,
- There is no non-conformity with other business ethics rules and policies that support these rules,
- It does not have a negative impact on fulfillment of their duties in the company.

Employees of the Company cannot act as board members or auditors in companies other than group companies without approval of the Board of Directors of the Company, or take office in competitors or companies in business relationships with SAHOL/EON/the Company. They may work in social responsibility and charitable roles under Non-Profit Organizations and Universities upon written approval of the Human and Culture Deputy General Manager and Chief Legal Counsel, on the condition that their duties within SAHOL/EON/the Company are not hindered.

8.7. **Dress Code:** Employees of the Company are obliged to pay attention to their clothing and appearance to fulfill the requirements of corporate culture. Applicable rules are set forth in Enerjisa Üretim Dress Code Procedure.

8.8. **Hiring Relatives:** Rules in respect of hiring immediate relatives (spouses, parents, siblings, and children) in the same workplace and/or employing them under the same manager or having them work for subcontractors of the Company are implemented in accordance with Enerjisa Üretim Recruitment Procedure.

8.9. **Occupational Health and Safety (OHS) and Protection of Environment:** Employees act and take necessary measures in line with the rules and instructions implemented to this end. Employees cannot keep any item or substance that pose danger for the workplace and/or employees, or that are of illegal nature. The Company is liable to ensure maximum OHS conditions for all employees, provide necessary trainings, and offer necessary equipment. Likewise, employees are liable to attend all relevant trainings and take any measure relevant to the matter. All employees should notify any potential danger, which they notice in their workplaces, verbally/in writing and/or by completing "Near Miss" forms to their managers. Enerjisa Üretim OHS Executive Management is responsible for sharing lessons to be learned from occupational accidents that occur in the field. Every OHS case should be reported objectively to relevant parties within the company.

Enerjisa Üretim OHS Senior Board is responsible for establishment and implementation of OHS policies and rules.

8.10. Substance Abuse: Employees cannot be under the influence of alcohol, drugs, or substances that are considered as stimulants during work hours. Immediate disciplinary action shall be taken against individuals that use such substances at the workplace. As an exception, if legal rules are not violated, alcoholic beverages can be consumed in organizations held by the Company. All employees are liable to act responsibly as required by the workplace environment in such exceptional activities.

8.11. Misconduct: It is unacceptable for the Employees to damage the Company by exercising their authorities for the benefit of themselves and/or their relatives and outside the scope of diligence expected from them. Employees cannot obtain direct or indirect personal gain from procurement and sales activities of the Company, as well as any transaction and contract that the Company enters into. Employees cannot engage in acts and behaviors in violation of ethical rules, the law, and disciplinary code of the Company. Employees are liable to ensure that documents exhibiting expenses that they make due to activities of the company are accurate, current, and true.

8.12. Resource Utilization: Interests of the Company are taken into consideration in resource utilizations to be made on behalf of the Company. Assets, means, and personnel of the Company cannot be used outside the Company, regardless of for which purpose, on whose behalf, and for the benefit of whom they are utilized, unless there is an interest of the Company. All personnel exercise the principle of "economy in every respect". Company resources (such as vehicles, computers, or e-mails) cannot be allocated to political activities. Correct utilization of resources in the interest of the Company also requires correct utilization of time. Employees of the Company should utilize their time well and avoid allocating time for their private affairs during work hours. Managers cannot assign employees for their personal affairs. Private visitors should not be accepted during work hours. Employees should complete their meetings with unavoidable visitors in a reasonable time in connection with the subject of visit and in a manner that would not prevent their work flow.

8.13. Confidentiality of Rights Granted to Employees: Employees are liable to take all kinds of necessary measures to protect any information that Human and Culture department requires to be kept confidential, including material benefits offered by the Company, and prevent disclosure to third parties. Employees know that this

matter is important in terms of protecting the interests of both the Company and them, any behavior to the contrary shall be subject to ethical review and disciplinary investigation within the scope of workplace order and rules pursuant to Workplace Code of Conduct Evaluation Board.

9. ANTI-MONEY LAUNDERING, CORRUPTION, AND BRIBERY

The Company does not tolerate bribery and any form of corruption under any circumstances. No Company employee, executive, or third parties acting on behalf of the Company may directly or indirectly offer, give, or authorize giving bribe or anything of material value to public servants, representatives of State-Owned Enterprises, or employees of other legal entities in order to affect decisions or acquisitions of that person to provide improper benefits to the Company. Similarly, employees of the Company are strictly prohibited from requesting and receiving bribes directly or indirectly from any party.

Any transaction concerning money laundering is strictly prohibited, while the Company takes all kinds of measures to avoid such activities and acts in line with both national and international legislation and embargo regulations, as well as other restrictions in applicable legislation, and also ensures conformity of its employees with these obligations.

10. PROHIBITION OF INSIDER TRADING

Employees of the Company must observe legal regulations in respect of trading Company stocks and avoid getting involved in situations that might lead to conflicts of interest. Employees cannot obtain any commercial income or act as mediators for others, including trading on the stock exchange, by means of insider trading of any information belonging to the Company.

Codes of Practice

- Individuals who have access to information that are not public are strictly prohibited from using such information to gain interest for themselves and/or third parties (including but not limited to operating in electricity and natural gas markets).

- Individuals that are able to trade by obtaining information from the inside are CEO and board members, executives (manager and above), internal/external auditors of a publicly listed company, other individuals that have access to information during fulfillment of their roles and responsibilities, as well as individuals that may directly or indirectly obtain information due to their connections with the mentioned individuals.

- If shares of the Company are offered to the public, such individuals can trade Company shares only by using public information and for investment purposes (holding for more than three months shall be considered as investment).

- If shares of the Company are offered to the public, Company employees other than those mentioned above may freely trade shares of Enerjisa Üretim Companies by using public information, without any time limitation.

- Abovementioned codes of practice are applicable also to spouses and children of such individuals. Transactions to be performed by spouses and children shall be deemed to have been performed by employees.

- Circumstances that are not mentioned in this document should be addressed in accordance with applicable legislation, SAHOL/EON policy/procedures, and Capital Markets Board legislation.

11. OFFERING A SUITABLE WORK ENVIRONMENT AND MOBBING

11.1. The Company acts in compliance with all applicable laws and regulations with regard to employment and work life. Employees of the Company fulfill all legal requirements and act in compliance with legal regulations within the scope of their respective activities.

11.2. Human resources policies and practices of the Company ensures that all practices such as recruitment, promotion-transfer-rotation, remuneration, awarding social benefits, etc. are fair.

11.3. Discrimination based on language, race, color, gender, political view, creed, religion, sect, age, disability status, and similar reasons is unacceptable among employees within the establishment.

11.4. It is ensured that physical work environment and conditions at the workplace are healthy and safe for all employees.

11.5. It is ensured that individuals with different beliefs, views, and opinions work in harmony by creating a positive and accommodating work environment that supports cooperation within the Company and preventing conflicts.

11.6. Private lives and personal boundaries of employees are respected.

11.7. Physical, sexual, and emotional immunities of employees are also observed in addition to any immunity they might have.

11.8. Violation of personal immunities in any manner, by means of physical, sexual and/or emotional abuse at the workplace or any location where they are present due to their jobs, is against the law and ethical rules, and the Company does not tolerate this crime under any circumstances. In this context, all kinds of measures are taken to ensure that employees work in a work environment where their physical, sexual, and emotional immunities are protected.

11.9. Violation of physical integrity of a person and/or sexual harassment of a person without physical contact is defined as sexual assault/abuse. Accordingly, it is unacceptable for any behavior, which could be considered within the scope of this definition, to be displayed.

11.10. Mobbing (Psychological Abuse at the Workplace), which comprises malicious, intentional, negative attitudes and behaviors; which is committed by one person or several people against another person or other people; which continues systematically for a certain period; which aims to intimidate, passivize, or drive apart; which damages personality values, occupational statuses, social relationships, or healths of victim(s); is considered as one of the manners of abuse mentioned above.

11.11. All employees are liable to notify all acts that are considered as mobbing at the workplace, regardless of whether relevant acts are committed against them and/or their colleagues. Religious, language, and racial discrimination is absolutely unacceptable and intolerable within the Company. Furthermore, ethnic discrimination, gender discrimination, and sexual harassment are also considered to be unacceptable acts. Such acts should be notified to the Ethics Supervisor. Malicious and unsubstantial reports shall also be considered as an offense.

12. COMPLIANCE PROCESS AND RESPONSIBILITIES OF COMPLIANCE OFFICER

12.1. Compliance-Legal Department conducts the compliance process. Chief Legal Counsel and Compliance Officer, to be determined by the Chief Legal Counsel, are responsible for conducting the compliance process within the Company.

12.2. Chief Legal Counsel and Compliance Officer are liable to act upon any internal/external report concerning violation of Compliance Rules. They are liable to inform Internal Audit Director with regard to ethical matters, and the Compliance Board with regard to all other compliance matters.

12.3. Chief Legal Counsel and Compliance Officer are also liable for the following;

- Providing guidance and consultancy concerning inquiries and issues submitted by employees with regard to compliance within the Company,
- Notifying deficiencies that might lead to violation of compliance rules of the company, which they notice in processes, and monitoring measures to be taken;
- Escalating reports, submitted to them with regard to violations of compliance rules of the Company, to the Compliance Board and offering full support to investigation activities to be conducted by the Internal Audit Department concerning such reports;
- Conducting training activities for compliance rules of the Company, and monitoring practices within the Company.

13. COMPLIANCE BOARD, REPORTING AND RESOLVING NON-CONFORMITIES REGARDING COMPLIANCE RULES OF THE COMPANY

13.1. The Compliance Board comprises CEO, CFO, HR Deputy General Manager and Chief Legal Counsel, and Compliance Officer (to conduct secretariat duties). If a matter of non-compliance concerns a business unit, Deputy General Manager of respective business unit is also included in the board. Internal Audit Director also acts as a board member in case of matter that concerns ethical rules.

13.2. All employees within the Company and other stakeholders (shareholders, customers, vendors, public authorities) can submit their notices regarding compliance rule violations to Enerjisa Üretim Compliance Line and E-mail address. Only Chief Legal Counsel and Compliance Officer are authorized to access such notice. Chief Legal Counsel and Compliance Officer are responsible for security, confidentiality, and management of the compliance process.

13.3. The non-compliance notice in question is referred by the Chief Legal Counsel and Compliance Officer to the Compliance Board, where it is resolved and settled. If the notice in question pertains to an ethical non-compliance, the matter is referred by the Chief Legal Counsel to the Internal Audit Director. Internal Audit Director decides whether to conduct any investigation.

13.4. If the Internal Audit Director refers the matter for an investigation, policies and procedures determined by the Internal Audit Office shall be implemented.

Annex 1: Enerjisa Üretim Compliance Policy and Enerjisa Üretim Compliance Procedure

Enerjisa Üretim Compliance Policy

As Enerjisa Üretim Santralleri A.Ş. ve İştirakleri ("Enerjisa Üretim"), we commit to the highest standards of compliance with the laws, regulations, rules, and policies applicable to us. We aim to establish a structure involving measures and key processes required to ensure compliance and, accordingly, achieve the following fundamental objectives:

- Clear identification of responsibilities within the scope of compliance,
- Determination and evaluation of compliance liabilities,
- Encouragement of behaviors that ensure establishment and reinforcement of compliance, and showing no tolerance for behaviors that compromise on compliance,
- Performance of compliance audits to check our fundamental compliance liabilities besides standard audits,
- Increasing awareness of employees, determination of their training needs, and organization of trainings for them within the scope of compliance,
- Monitoring our compliance activities and reporting performance,
- Regular review and continuous improvement of our compliance approach and tools.

Enerjisa Üretim Compliance Procedure

1. PURPOSE AND SCOPE

This Compliance Procedure ("Procedure") has been issued to (i) determine compliance procedures, (ii) establish operating principles for such processes, and (iii) determine methods and methodologies to be observed within this scope in Enerjisa Üretim companies.

Compliance programs are conducted by the Compliance-Legal Department under the Compliance function.

Compliance procedures are conducted under 4 main titles in Enerjisa Üretim companies:

2. Legislative Compliance Process

The purpose of this process is to conduct any follow-up with regard to the legislation, to notify amendments to the legislation to relevant departments, to identify potential

non-conformities, to determine corrective actions to be taken, and to increase awareness within the company by reporting any relevant matter.

This process aims to prevent any sanction and risk that might arise from non-conformity with the legislation.

Compliance-Legal Department is responsible for the implementation of Legislative Compliance Process.

Changes in the legislation are currently monitored by the Compliance-Legal Department by means of both the Official Gazette and official websites of Regulatory Bodies. Monitored regulations are circulated as main titles weekly, on every Monday, by e-mail to all Enerjisa Üretim employees. Besides regulatory changes that are circulated on a weekly basis, regulations that significantly and primarily affect the company are separately notified on the date of issuance in the Official Gazette.

A separate regulation meeting is held every week to conduct legislation monitoring process better, and matters concerning changes in the legislation and the effects of changed legislation on our company are evaluated and discussed weekly with relevant business unit managers. During such meetings, the matter is escalated to senior executives and it is ensured that action is taken regarding the process to reflect recently introduced regulation in the legislation or legislative changes to operations of the company.

Regulatory practices are monitored and implemented in respective fields of business of every department.

A list of all regulations that must be observed and that affect business processes was drawn by the Compliance--Legal Department. Compliance-Legal Department demand all business units to file semi-annual reports on Compliance Catalog within the scope of regulatory compliance to determine that applicable regulations are implemented correctly. This catalog contains company details, compliance definition, details of department and manager affiliated with compliance owner, relevant law and legislation details, affected procedure details, monitoring interval, definition of present non-compliance, if any, and actions to be taken, as well as details on deadline of these actions and sanctions to be imposed.

Compliance-Legal Department collects the information, provided in the abovementioned compliance catalog, from relevant departments in every six months. As a result of this analysis, Chief Legal Counsel and Compliance Officer report existing or potential non-conformities, sanctions, and actions to be taken to

the CEO and affiliated deputy general managers in ELT meetings or Compliance Board meetings.

Compliance-Legal Department inquires relevant business units whether departments have taken the actions that should be taken in this process, and checks implementation thereof. In case of non-compliance, the situation is reported again to the relevant deputy general manager.

In addition, Regulatory Authorities may request opinion from our company about draft regulations before they are issued. Compliance-Legal department forms a legal opinion about draft regulations. Furthermore, if applicable legislation requires technical opinion besides legal opinion, Compliance-Legal Department communicates draft regulation to relevant functions and obtains technical opinions of such functions about the regulation. Technical opinions collected by the Compliance-Legal Department are consolidated with legal opinion and shared with the Regulatory Authority.

3. Compliance Process Conducted within the Framework of the Law on Protection of Personal Data (LPPD) ("LPPD Compliance Process")

The purpose of this process is to ensure fulfillment our legal obligations within the scope of the LPPD and applicable legislation, compliance of conducted activities with the legislation on protection of personal data, maintenance and improvement of established systems, identifications of potential non-compliances, determination of corrective actions to be taken, and increasing awareness within the company by reporting all matters in this regard.

This process aims to prevent any sanction and risk that might arise from non-conformity with the LPPD and applicable legislation.

Compliance-Legal Department works with Human and Culture and Information Technologies units as they conduct the LPPD Compliance Process. Personal Data Protection Committee ("Committee") was established to ensure necessary coordination within our Company to ensure, maintain, and sustain compliance with the personal data protection legislation.

Processes concerning the Personal Data Protection Committee are established with the Personal Data Protection Committee Procedure. The Commission comprises at least 4 people, with Chief Legal Counsel, Human and Culture Leader, Information Technologies Director, and a Senior Lawyer among Commission members.

Personal Data Protection Committee is responsible for ensuring uniformity between units of the Company, as well as maintenance and improvement of systems established to ensure compliance of conducted activities with the personal data protection legislation:

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

- To establish a corporate culture that supports the rules on protection and processing of personal data,
- To prepare and implement essential policies regarding protection and processing of personal data upon approval of Human and Culture deputy general manager,
- To resolve on how implementation and inspection of policies on protection and processing of personal data shall be performed and, accordingly, to make internal assignments and ensure coordination,
- To determine steps that should be taken to ensure compliance with the LPPD and applicable legislation, to observe implementation and ensure coordination,
- To increase awareness within the Company and before institutions, with which the Company cooperates, regarding protection and processing of personal data,
- To identify risks that might arise in personal data processing activities of the Company, to ensure that necessary measures are taken, and to offer recommendations for improvement,
- To design and ensure performance of trainings on protection of personal data and implementation of policies,
- To resolve on applications of personal data subjects at the highest level,
- To coordinate performance of information and training activities aimed at ensuring that relevant parties are informed about personal data processing activities of the Company and their legal rights,
- To prepare and implement amendments to essential policies regarding protection and processing of personal data upon approval of Human and Culture deputy general manager,
- Monitoring developments and regulations on protection of personal data, making recommendations to the senior management in respect of necessary actions to be taken in operations of the Company in line with these developments and regulations,
- To manage relationships with the Personal Data Protection Board and Personal Data Protection Authority,

- To fulfill other duties to be assigned by Company management with regard to the protection of personal data.

Compliance-Legal Department prepares company policies on the LPPD under its duty as a member of the Personal Data Protection Committee, and it is ensured that all employees are informed by uploading the policies to relevant intra-company systems. In addition, Compliance-Legal Department organizes classroom and online trainings at regular intervals for all employees of the company to raise awareness about the LPPD and implement the LPPD Compliance Process. Compulsory LPPD training is provided to every new employee that is hired by the Company.

Uniform procedure and Necessity and Reasonableness Test were established to be implemented in retention of documents containing personal data associated with Enerjisa Üretim Santralleri. Compliance-Legal Department draws up a disclosure text for visitors and suppliers in plants, and such texts are updated by the Compliance-Legal Department if necessary.

Compliance-Legal Department made it obligatory to add protective articles, involving relevant regulations within the scope of the LPPD, to relevant agreements.

Information is requested from all relevant units to create a Data Inventory, and the data inventory is prepared in light of received information. The data inventory is regularly updated by the Compliance-Legal Department with information received from relevant business units. In addition, Companies are also registered with VERBIS (Data Controllers Registry Information System) in line with the LPPD compliance process.

LPPD disclosure and consent texts are obtained from all employees as a result of the study conducted by the Human and Culture Department and Compliance-Legal Department.

Compliance-Legal Department responds to questions received from all units of our Company, and offers regular support to units in terms of conducting processes in line with the legislation.

Compliance-Legal Department regularly monitors current legislation within the scope of LPPD with Lexpera and Kazancı memberships. Moreover, it monitors informational e-mails of contracted law offices on daily legislative changes and announcements of relevant public institutions and organizations. In this context, legislative changes regarding LPPD or announcements of the Authority are communicated to "kisiselveri@enerjisauretim.com" address as informational notes.

Compliance-Legal Department and Commission activities shall continue regularly within the scope of the LPPD Compliance Process.

If Personal Data Protection Committee or Compliance-Legal Department identifies a non-compliance during this process, the Committee files such non-compliance with a committee decision and resolves on the action to be taken. Such non-compliance is also notified to the Compliance Board. Compliance Board is not bound by the decision made by the Personal Data Protection Committee, and it is authorized to implement another decision in this regard. If Committee and Board decisions contradict, Board decision shall prevail. Such contradiction shall also be reported by the Chief Legal Counsel to the Compliance Board.

4. Compliance Process Conducted within the Framework of the Law on Protection of Competition ("Competition Compliance Process")

The Purpose of this process is to ensure fulfillment of our legal obligations within the scope of the Law on Protection on Competition ("Competition Law") and applicable legislation, ensure compliance of conducted activities with the Competition Law and applicable legislation, prevent any potential violation, determine preventive actions against potential non-compliance, and increase awareness within the company by reporting all matters in this regard.

This process aims to prevent any sanction and risk that might arise from non-conformity with the Competition Law and applicable legislation.

Compliance-Legal Department is responsible for the implementation of Competition Compliance Program.

Compliance-Legal Department outsources services from a specialist legal counseling office ("Consultant") for this process. Compliance-Legal Department cooperates with the Consultant in the Competition Compliance Process and conducts this process together. The Consultant audits the company in semi-annual periods, particularly by inspecting e-mails, pursuant to the competition law. Furthermore, on-site inspection and mock down audits are conducted to identify potential risks, and necessary actions are determined to avoid any violation. If a potential violation is identified, Chief Legal Counsel reports this situation to the Compliance Board.

Compliance-Legal Department also provides competition awareness trainings to relevant departments, particularly companies and departments that have more interaction with the competition law, as part of the Competition Compliance Process program. These trainings involve raising awareness about behavior in violation of competition, preparation of presentations about how future business processes can

be conducted in compliance with competition, and provision of interactive trainings. Compulsory Competition Compliance training is provided to every new employee that is hired by the Company.

Besides trainings, Compliance-Legal Department regularly makes efforts to establish a work environment sensitive to awareness and competition with visual and written warnings and notices within the scope of Competition Compliance Process.

Compliance-Legal Department shall continue its activities regularly.

5. Compliance Process Conducted within the Framework of Enerjisa Üretim Compliance Manual ("Compliance Process for Enerjisa Üretim Compliance Rules")

The purpose of this process is to define the compliance rules that should be observed by all employees within Enerjisa Üretim, rights of employees in this regard, compliance criteria (values) of the company, and fundamental principles of the company; conduct any follow-up regarding principles and values ("Enerjisa Üretim Compliance Rules") accepted with Enerjisa Üretim Compliance Manual, prepared to reflect the common values of SAHOL (H.Ö. Sabancı Holding) Ethics Code (SA-Ethics) and E.ON Compliance Rules, and raise awareness within the company; establish and review Enerjisa Üretim Compliance Rules; perform analyses and announce modifications of Enerjisa Üretim Compliance Rules; identify potential non-compliances; and increase awareness within the company by reporting all matters in this regard.

This process aims to ensure highest level of compliance with Enerjisa Üretim Compliance Rules, establish a structure involving necessary measures to ensure this, and prevent any sanction, loss of reputation, and risk that might arise from non-compliance.

Compliance-Legal Department conducts the compliance process. In this context;

- Any situation that poses the risk of conflict of interest should be notified by the relevant employee to their direct supervisor and to the Chief Legal Counsel.
- Approval of relevant Deputy General Manager and Chief Legal Counsel must be obtained to use the name of the Company in any activity that is not led by the Company.
- Employees of the Company cannot work for another individual and/or institution within/outside business hours to obtain additional income or a similar benefit without written approval of relevant Deputy General Manager of the department

within the scope of their employment contract, Deputy General Manager Human and Culture, and Chief Legal Counsel.

- Employees of the Company may work in social responsibility and charitable roles under Non-Profit Organizations and Universities upon written approval of the Human and Culture Deputy General Manager and Chief Legal Counsel, on the condition that their duties within SAHOL/EON/the Company are not hindered.

Chief Legal Counsel and Compliance Officer, to be determined by the Chief Legal Counsel, are responsible for conducting the compliance process within Enerjisa Üretim. Chief Legal Counsel is authorized to appoint and dismiss the Compliance Officer. Compliance Officer, appointed by the Chief Legal Counsel, is announced by e-mail to Enerjisa Üretim. Compliance Officer continues to act in this capacity until dismissal from the role or discharge from the Company (whichever comes first).

Chief Legal Counsel and Compliance Officer review the Compliance Manual semi-annually or following changes in SAHOL/EON policies/procedures. In this context; SAHOL/EON policies/procedures are continuously monitored by the Compliance-Legal Department. Revisions made on the Compliance Manual upon approval of the Compliance Board are announced to the whole company by e-mail, and it is ensured that all employees are informed by uploading the revisions to relevant intra-company systems.

Responsibilities of Chief Legal Counsel and Compliance Officer are determined in Enerjisa Üretim Compliance Manual. These are;

Chief Legal Counsel and Compliance Officer responds to questions received from all units in respect of Enerjisa Üretim Compliance Rules, and offers regular support to the units for conducting processes in compliance with Enerjisa Üretim Compliance Manual. During this process, if Chief Legal Counsel or Compliance Officer identifies non-compliance with the Compliance Rules of the Company, the situation is notified to the Compliance Board and recorded. Chief Legal Counsel and Compliance Officer notify job owners about deficiencies, which might lead to violations of compliance rules of the company, noticed in processes conducted by Enerjisa Üretim units, and follow-up measures taken by relevant units. The situation is notified to the Compliance Board if measures are inadequate or no measures are taken. Matters notified to the Compliance Board are finalized and resolved by the Compliance Board and consequent actions to be taken are determined by the Compliance Board. In addition, the Board takes necessary actions by cooperating with the Academy/Training Department to increase awareness about Enerjisa Üretim Compliance Manual and to ensure that every new employee attends compulsory

Compliance Rules training to ensure effective maintenance of the Process for Compliance with Enerjisa Üretim Compliance Rules.

Enerjisa Üretim Compliance Board is responsible for ensuring an environment that will enable implementation of Enerjisa Üretim Compliance Rules. The Compliance Board comprises CEO, CFO, HR Deputy General Manager and Chief Legal Counsel, and Compliance Officer (to conduct secretariat duties). If a matter of non-compliance concerns a business unit, Deputy General Manager of respective business unit is also included in the board. Internal Audit Director also acts as a board member in case of matter that concerns ethical rules. CEO is the Chairman of the Board.

Compliance Board decisions are made by majority vote. If the Board fails to make a decision, the matter is escalated to the Executive Committee and the decision to be made by the Executive Committee is binding.

The role of Board secretary is fulfilled by the Compliance Officer unless decided otherwise by the Compliance Board. Accordingly, Board Secretary sets the agenda and communicates it to Compliance Board members by e-mail before the meeting. If there are witnesses that should be heard with regard to the Compliance Violation Notice subject to the meeting, Board Secretary invites such witnesses to the Compliance Board meeting. Board Secretary is in charge of keeping meeting minutes, recording decisions, and informing relevant units and individuals within the company about Compliance Board decisions for necessary action to be taken. Meeting notes are shared with Compliance Board members by e-mail.

All employees of Enerjisa Üretim and other stakeholders (shareholders, customers, suppliers, public institutions) can submit notices of non-compliance with Enerjisa Üretim Compliance Rules by means of Compliance Violation Notification channels. Only Chief Legal Counsel and Compliance Officer are authorized to access such channels. Notification channels are as follows:

- Compliance Violation Notification E-mail: uyum.ihbar@enerjisauretim.com
- Compliance Violation Notification Line: (0216) 512 40 60
- Internal Extension: 4060

Besides, Compliance Violation Notifications can be made also by means of Chief Legal Counsel and Compliance Officer. Compliance Officer is liable to submit notifications, submitted to them, to Chief Legal Counsel.

Chief Legal Counsel and Compliance Officer primarily conduct preliminary review about whether Violation Notices, which are received by means of Compliance Notification Channels, submitted directly to them, or submitted to Chief Legal Counsel by the Compliance Officer, are related to ethical matters. Notifications that can be subject to ethical violations in terms of contents are submitted to Internal Audit Office. Internal Audit Director decides whether such notice shall be subject to any investigation, and policies and procedures determined by the Internal Audit Office are implemented if the matter is investigated. Chief Legal Counsel and Compliance Officer fully support investigation activities to be conducted by the Internal Audit Department concerning these reports. Chief Legal Counsel and Compliance Officer are obliged to notify all other Compliance Violation Notices to the Compliance Board. Reviews concerning Compliance Violation Notices are conducted, finalized, and resolved by the Compliance Board.

The Compliance Board decides whether to conduct a detailed inspection study within the scope of Compliance Violation Notices. If deemed necessary in this evaluation stage, the Compliance Board may ask for the opinion of deputy general manager of the unit subject to the notice. CEO should be informed before launching any inspection about an executive at the level of manager and/or above. In addition, if deemed necessary, Deputy General Manager of the relevant unit may be informed accordingly.

If, it is determined by the Compliance Board as a result of the inspection that the Compliance Violation Notice has been made falsely or for personal gain, the situation and, if identifiable, the individual that has made the notification are reported to the Internal Audit Office.

The Compliance Board may consult employees or other people, within the scope of the inspection to be conducted, verbally or in writing. All actions aimed at misstatement and/or concealing evidence supporting misconduct are subject to disciplinary action and notified to Internal Audit Office.

Enerjisa Üretim Compliance Board, Human and Culture, Compliance-Legal, and Internal Audit Departments are responsible for guaranteeing confidentiality of reports concerning violations in Enerjisa Üretim Compliance Rules, protection of employees against harassment following relevant reports, ensuring job security of employees that submit notices, and ensuring work safety. If identity of the individual that has made the notification is known or understandable, they cannot be subject to any negative sanction due to the submission of such notice, except for

determination of the fact that the notification has been made falsely or for personal gain.

The Compliance Board must be completely objective as they carry out their duties.

In case the individual that made the notification or third parties, including public authorities (Personal Data Protection Board, Competition Board, etc.), should be informed as a result of performed inspection, the letter to be prepared by the relevant unit should be drafted in coordination with the Compliance Board and it must not be sent without informing the Compliance Board.

If judicial process is initiated with respect to the notification subject to the review of the Compliance Board, the person to be declared as witness to the court shall be determined and notified to the Compliance Board by the Chief Legal Counsel. The process is completed upon obtaining written approval of the Compliance Board.

Members of the Compliance Board and other relevant parties (Compliance-Legal Department, Human and Culture, and relevant process owners) carry out consultations regarding the matter before the court process, and represent Enerjisa Üretim in full agreement.

Compliance Board holds a semi-annual periodic meeting to conduct the compliance process better. Chief Legal Counsel and Compliance Officer may convoke the Compliance Board apart from meetings held due to a Compliance Notice, and set the agenda for these meetings. In these meetings, the Compliance Board may not only review changes in Enerjisa Üretim Compliance Rules or SAHOL/EON policies/procedures directly or upon request of the Chief Legal Counsel and Compliance Officer; but also make recommendations about actions that should be taken to establish and develop an environment that would enable implementation of Enerjisa Üretim Compliance Rules, improve compliance processes, and eliminate contradictions, if any.

If gifts that bear the expression "Inappropriate Pursuant to the Principles for Accepting/Offering Gifts" are not retrieved by the giving party or if returning the gift has the potential to negatively affect current relationship, relevant gifts should be sent to the Compliance Board to be used for donations and rewards. Compliance Board decides where and under which circumstances the gifts delivered to them shall be used and informs the relevant deputy general manager accordingly. The deputy general manager in question cannot use such gift for purposes other than those specified by the Compliance Board.

Enerjisa Üretim Compliance Rules are monitored and implemented in respective fields of business of every department.

A list of all principles and rules, which must be observed within the scope of Enerjisa Üretim Compliance Manual and which affect business processes, is drawn by the Compliance-Legal Department. Compliance-Legal Department demand all relevant business units to file semi-annual reports on Compliance Catalog within the scope of compliance with Enerjisa Üretim Compliance Manual to determine that applicable rules are implemented correctly. This catalog contains company details, compliance definition, details of department and manager affiliated with compliance owner, relevant compliance rule, affected procedure details, monitoring interval, definition of present non-compliance, if any, and actions to be taken, as well as details on deadline of these actions and sanctions to be imposed.

Compliance-Legal Department collects the information, provided in the abovementioned compliance catalog, from relevant departments in every six months. As a result of this analysis, Chief Legal Counsel and Compliance Officer report existing or potential non-conformities, sanctions, and actions to be taken to the Compliance Board in periodic Compliance Board meetings.

Compliance-Legal Department inquires relevant business units whether departments have taken the actions that should be taken in this process, and checks implementation thereof. In case of non-compliance, the situation is reported again to the relevant Deputy General Manager.

Annex 2: Enerjisa Üretim Competition Policy

Enerjisa Üretim Competition Compliance Policy

Under the free market economy, which has been adopted by our Company as well, enterprises can easily get into the market, operate at liberty, and determine prices. In order for enterprises to have these liberties, there must be competition on the market. Institutions that form the electricity market strive to establish a market where market players, i.e. electricity suppliers are free to make decisions, get into and leave the market, and determine prices at liberty. It is indeed impossible for a market that operates fairly and reliably to develop in an industry in which competition is not present or it is restricted.

As known, fundamental policy of our company and our majority shareholders, Sabancı Holding and E.ON SE, is to act in full compliance with the law and all legal regulations in force. In this scope, one of the primary principles of Enerjisa Üretim is to ensure full compliance with competition in view of the Law no. 4054 on Protection of Competition ("Competition Law" or "Law" or "LPC") and all applicable regulations. In this framework, the policy of Enerjisa Üretim to comply with competition is in full harmony with the letter and spirit of the Competition Law.

Companies face hefty fines and damage claims due to violations of the competition law, while individual administrative fines can be imposed on employees as well. Of course, the most significant damage of competition violations is the negative effect on reputation and brand value of our company.

In terms of corporate adoption of competition rules, a significant responsibility falls upon both our company and each of our employees to avoid all these negative outcomes.

Pursuant to the principle of Enerjisa Üretim on 100% compliance with the legislation, it is quite important for every employee to read and learn the fundamental principles and prohibitory rules of the competition law, continuously improve themselves in this area, and increase the awareness of both themselves and people around them about sanctions. Rules imposed by the competition law must be strictly observed, also in consideration of economic foundations and practical implementation, in relationships, communications, and interactions with competitors.

Therefore, our esteemed employees should read this instructional Manual, adhere to determined rules, and take recommendations into consideration. Consequences in violation of competition and sanctions can be prevented only if all employees fulfill

their duties. Thus, all employees are expected to learn and internalize competition rules to the highest extent possible, and act in full compliance with these rules.

Legal Basis of Competition

Constitution of 1982 stipulated that everyone was at liberty to work and make agreements in any area, and it was free to establish private enterprises. The boundaries of such freedom were outlined with the regulation on competition in Article 167 of the Constitution:

«The State is obliged to take measures that ensure reliable and regular operation and improvement of money, credit, capital, property, and service markets, and to prevent monopolization and cartelization arising de facto or by agreement on markets.»

The State fulfills this duty, imposed by the Constitution, by enforcing competition rules and making necessary regulations to ensure sustainability of competition on the market. In this scope, the Law no. 4054 on Protection on Competition was enacted in 1994 in our country.

The purpose of the Competition Law is to ensure protection of competition on property and service markets.

The law covers all property and service markets, as well as all enterprises, across Turkey. The law defines enterprise as natural and legal entities that produce, market, and sell goods and services on the market, as well as units that are able to make independent decisions and comprise a whole in terms of economy. In other words, enterprises are units that engage in economic activities and have economic independence, regardless of whether they are legal entities. For example, holding companies, corporations, sole proprietorships, natural persons that conduct independent business activities, etc. are included in this scope.

Foreign enterprises operating within our country are governed by the Law. Foreign enterprises outside Turkey can be considered within the scope of the Law only due to their actions that affect Turkish market.

Practices Investigated Within the Scope of Competition

Article 4 of the Law

«Non-Competition Agreements, Concerted Practices, and Decisions» are prohibited by this article.

In this context, we encounter vertical and horizontal agreements.

Article 6 of the Law

«Abuse of Dominant Position» is prohibited by this article.

The article prevents abuse of dominant position rather than being in a dominant position.

Article 7 of the Law

«Mergers and Acquisitions» are unlawful and prohibited if they lead to significant reduction of "effective" competition in a part or all of the country.

Practices prohibited in Article 4

Agreements between enterprises, concerted practices, and such decisions and actions of enterprise associations, which aim to directly or indirectly prevent, disrupt, or restrict competition in a certain property or service market, or which cause or may cause this effect, are unlawful and prohibited.

These agreements and actions can be either horizontal, between competitors at the same level, or vertically, between enterprises at different stages of production and distribution chains.

Agreements within the scope of article 4 of the Law no. 4054;

- Are not required to be valid pursuant to the provisions of the Civil Code and the Code of Obligations. Gentlemen's agreements are deemed to be agreements in accordance with the Law no. 4054.
- Are not subject to requirements as to form. Any written, verbal, implied voluntary understanding is sufficient.
- Are not required to be signed.
- Acknowledgment of being bound by the agreement is sufficient.
- Are not required to be enforced. Intent is sufficient.
- Are not required to be in the interest of both parties.
- This can be intentional or due to negligence.

Types of Agreement:

Agreements at different levels of the production chains (e.g. between producers and distributors, distributors and suppliers) are characterized as vertical agreements, while agreements between competitors at the same level of the chain are characterized as horizontal agreements. In this context, green arrows represent horizontal agreements and blue arrows represent vertical agreements in the following chart.

Horizontal Violations

The following actions of enterprises in competition are unlawful and prohibited pursuant to the Law no. 4054;

- Price fixation (increasing or fixing prices, determination of minimum prices, eliminating discounts, determination of discount rates, profit margins, etc.)
- Making collusive bids in tenders (sharing tenders, boycotting tenders, determination of bids to be made in tenders, etc.)
- Market/region/customer sharing
- Determination of production/sale amounts
- Obstructing activities of competitors/kicking competitors out of market/preventing new penetration

Within the scope of cases presented to the Competition Board as a result of horizontal agreements;

- Service fee fixation (agreement between the banks to charge the same EFT fee)
- Product price fixation (agreement between refineries on product output prices)
- Determination of commission rates to be applied (determination of commission to be charged by transporters on transported goods)
- Market sharing (airports shared by aircraft fuel suppliers)
- Supply restrictions (agreement between power generation companies for restriction of supply, causing intentional planned failures)
- Region sharing (regions shared by cement producers)

were encountered.

Presumption of Concerted Practice

In case the presence of an agreement cannot be proven, similarity of price changes on the market, supply and demand equilibrium, or operating areas of enterprises with the markets where competition is prevented, disrupted, or restricted, constitutes presumption of concerted practices by enterprises.

For example:

- Simultaneous and similar price increases by competitors in a certain market,
- Simultaneous termination of a practice in favor of customers (e.g.: discount) by competitors,
- Non-competition of competitors in an area where they should be competing, with no rational explanation (e.g. quotation of same prices by every competitor to a certain buyer, avoidance of competition, etc.)

When presumption of concerted practice is invoked, enterprises should prove that they are not acting in concert. Enterprises can prove that they are not acting in concert only by asserting rational and economic grounds.

Disclosure of Competitively-Sensitive Information

Exchange of strategic information between competitors, which has a direct impact on competition in the market and eliminates uncertainty in the market, is characterized as violation of competition in article 4 of the Law as it leads to cooperative consequences and creates symmetry in the market. Competition Board considers even exchange of competitively-sensitive information between parties as violation. Moreover, even information exchanges that facilitate operation of cartel, ensuring follow-up of whether the rules agreed upon by the parties are observed, are considered as part of cartelization.

The following information is deemed to be competitively-sensitive information;

- Fees, promotions, prices, sales strategies, inventory numbers considered to be applied
- Tenders considered to be attended, bids to be made in tenders
- Costs, profits

- Any matter that constitutes business secret for the company and that gives it competitive advantage

TRY 21,179,390.25 total administrative fine was imposed with the decision no. 17-39/636-276 of 11/28/2017 of the Competition Board on enterprises subject to investigation due to violation of article 4 of the Law no. 4054 by sharing information on loan conditions such as interest and maturity regarding current loan agreements, as well as competitively-sensitive information regarding other financial transactions, by banks that extend loans to corporate clients in Turkey.

Enterprise Associations and Key Considerations

Companies may convene under various professional organizations and non-governmental organizations to achieve certain purposes. Examples to such organizations include Turkish Union of Chambers and Commodity Exchanges (TOBB), Turkish Confederation of Tradesmen and Craftsmen, Turkish Pharmacists' Association, Turkish Industry and Business Association (TÜSİAD), as well as Electricity Distribution Services Association (ELDER), Power Generators' Association (EÜD), Energy Traders' Association (ETD) specific to the electricity industry.

These associations can make decisions with economic effects on markets or establish platforms for its members to make decisions in line with common purposes. Using organizations such as chamber, association, union, etc. that brings competitors in the same industry together as a platform for sharing market information that could impact decisions regarding competition between members can lead to violations of competition.

In enterprise association or industry meetings;

- Always review the agenda before the meeting.
- Always review meeting minutes.
- Keep all agendas, minutes, and documents.

Object and leave the meeting if a competitor mentions subjects that are sensitive in terms of the competition law. Ensure that your objection is written in meeting minutes and obtain a copy of meeting minutes before leaving the meeting.

If there are no minutes in the meeting, objected matters should be notified to other competitor participants in writing immediately after the meeting is left. Always consult with the Compliance-Legal Department before such notice is prepared.

TRY 21,179,390.25 total administrative fine was imposed with the decision no. 17-42/665-294 of 12/21/2017 of the Competition Board on enterprises subject to investigation due to violation of article 4 of the Law no. 4054 by collusion of enterprises, which are members of Turkish Cargo, Courier, and Logistics Operators Association, operating in Cargo Transportation business.

Exemption Regime

Article 5 of the Law no. 4054;

Agreements, concerted practices, and enterprise association decisions between enterprises are exempt from enforcement of the provisions of article 4 of the Law if all of the following conditions are fulfilled:

a) New developments and improvements or economic or technical developments are ensured in production or distribution of goods and provision of services,

b) Consumers benefit as a result,

c) Competition is not eliminated in a significant portion of the relevant market,

d) Competition is not limited more than necessary to achieve the purposes in clauses (a) and (b).

The Board may issue communiqués that grant exemption for types of agreement on certain matters and setting forth the conditions for these if the conditions are fulfilled.

It is investigated whether an agreement/concerted practice/enterprise association decision aims to disrupt, prevent, or restrict competition or have such an effect or have the potential to do so in the future within the scope of the Law no. 4054. Horizontal agreements (for example, R&D, cooperation, specialization, co-production and co-procurement agreements between competitors) and vertical agreements can be permitted under certain conditions in some cases, even if such risks are present.

INDIVIDUAL EXEMPTION:

If, as a result of an agreement between companies,

- Economic or technological development arises,
- Consumers benefit as a result,

- Competition on the market is not significantly eliminated or limited more than necessary,
- Competition is not limited more than required to achieve specified purposes

Relevant enterprises or enterprise associations may apply to the Authority for determination by the Board that the agreement, concerted practice, or enterprise association decision within the scope of article 4 fulfills all of the exemption conditions mentioned above.

GROUP EXEMPTION:

Enterprises do not make applications to have group exemption granted; it is granted by the Competition Board for industries that it deems necessary. There is currently no group exemption for the energy industry.

Abuse of Dominant Position (Article 6)

Article 6 of the Law no. 4054;

It prohibits abuse of dominant position of one or multiple enterprise(s) in a property or service market alone or by means of agreements or concerted practices with other parties throughout or in a part of the country.

The Law no. 4054 defines dominant position as "the power of one or multiple enterprise(s) to determine economic parameters such as price, supply, production, and distribution amount in a certain market independently of their competitors and customers".

While market share is an important element that indicates dominant position, it is not possible to determine a fixed market share ratio for dominant position.

<40%	There is usually no finding of dominant position
40%-50%	Presence of other conditions is required
50%-60%	A strong indicator
60%-70%	Sufficient indicator for presence of dominant position in the absence of indicators to the contrary
>70%	Usually an indicator of dominant position

Dominant position of any enterprise is not prohibited in the context of the competition law. Competition law prohibits abuse of dominant position.

TO-DO LIST

Terms and conditions of services offered to customers **MUST BE DETERMINED** independently of competitors (without communicating with competitors).

THERE SHOULD ALWAYS BE COMPETITION for suitable customers unless there are reasonable commercial reasons not to compete.

ATTENTION MUST BE PAID to prevent non-compete obligations introduced by executed agreements from exceeding 5 years, and review of agreements that contain exclusivity by the Compliance-Legal Department before signing.

Agenda must be requested before meetings to be held with competitors and agenda must be **REVIEWED** in detail before the meeting.

When matters that you consider to be in violation of competition are discussed during the meeting, the meeting must be **LEFT** immediately, this matter must be **WRITTEN** to minutes, and **A COPY OF THE MINUTES MUST BE OBTAINED**

Communication with competitors during meetings **MUST BE LIMITED** to discussion of agenda items, and any other official or unofficial discussion must be **AVOIDED.**

IT MUST BE ENSURED that communications established with competitor enterprises, which operate in the energy industry, in accordance with agreements involving trade relationships remain only within the scope of such relationship.

WHAT TO AVOID

Any agreement that restricts competition **MUST NOT BE MADE** with competitors.

THERE MUST BE NO EXCHANGE OF INFORMATION with competitors concerning any competitively-sensitive matter, particularly prices or price elements such as offered discounts.

A negotiation or meeting, where sensitive information belonging to competitors, **MUST NOT BE ATTENDED**, even if there is no active participation in the discussion.

Mergers and Acquisitions

Some mergers and acquisitions may cause emergence of enterprises that are powerful enough to cause significant harm to the competitive environment in the market, and affect consumer welfare negatively. Therefore, it is important and

necessary to supervise mergers and acquisitions to protect competitive conditions in markets.

Mergers and acquisitions, which create dominant position or strengthen such position of a company dominant in the market and significantly restrict "effective" competition, are prohibited within the scope of the Law no. 4054.

The Board announces with communiqués to be issued that any merger and acquisition must be notified to the Board and permission must be obtained to become legally valid. It is not possible for an operation subject to permission to become legally valid without obtaining permission from the Competition Board, and hefty fines can be imposed and the operation can be declared invalid if an operation subject to permission is carried out without permission of the Competition Board. The Competition Board may permit or decline the relevant operation as a result of its investigation. In some cases, the operation in question can be permitted under certain conditions.

Administrative Fines That Can be Imposed by the Competition Board

Procedural Administrative Fines

Administrative fines are imposed in case procedural obligations stipulated in certain provisions of the Law no. 4054 are not fulfilled.

- Submission of misleading information or documents in applications exemption and negative clearance, as well as applications for permission for mergers and acquisitions

- Performance of mergers and acquisitions subject to permission without permission of the Competition Board

- Submission of incomplete, inaccurate, or misleading information or documents, or failure to submit information or documents within the specified time or at all

An administrative fine, corresponding to one thousandth (0.1%) of yearly gross revenues of the enterprise in question, is imposed under the circumstances mentioned above.

- Preventing or obstructing on-site inspection: In this case, an administrative fine, corresponding to five thousandth (0.5%) of yearly gross revenues of the enterprise in question, is imposed.

If on-site inspection is prevented/obstructed or required information/documents are not submitted within the specified period, an administrative fine, corresponding to five ten thousandth (0.05%) of yearly gross revenues obtained as of the previous fiscal year-end for every additional day of delay.

However, the fine to be determined pursuant to this principle cannot be less than 34,809 (thirty four thousand eight hundred and nine) Turkish Liras for 2021.

Administrative fines, imposed with regard to mergers and acquisitions performed without permission of the Competition Board, shall be imposed on each party in mergers and only the recipient in acquisitions.

Substantial Fines:

Under the circumstances specified in articles 4, 6, and 7 of the Law no. (agreements and practices limiting competition, abuse of dominant position, and performance of a merger/acquisition that creates a dominant position or strengthens dominant position), an administrative fine up to ten per cent (10%) of the yearly gross revenue for the year-end before final decision or, if it is not possible to calculate this, obtained at the nearest fiscal year-end to the date of final decision.

In accordance with the Regulation on Fines to be Imposed in Case of Agreements, Concerted Practices, and Decisions Limiting Competition, as well as Abuse of Dominant Position;

- two per cent (2%) to four per cent (4%) for cartels,
- five thousandth (0.5%) to three per cent (3%) for other violations,

of yearly gross revenues of enterprises, which are determined to have violated the Law no. 4054, obtained at the previous fiscal year-end, is determined as the base fine.

While the rates in question can be increased due to aggravating circumstances such as repetition of violation or continuance of violation after notification of investigation decision, such rates can be reduced due to mitigating circumstances such as assisting in investigation beyond fulfillment of legal obligations, presence of encouragement of public authorities and coercion of other enterprises in the violation, payment of compensation to aggravated parties, and termination of other violations. However, in any case, the upper limit is ten per cent (10%) of the yearly gross revenue of the enterprise in question.

Triple Compensation Risk:

Besides the administrative fines to be imposed by the Competition Board, third parties incurring losses within the scope of actions and practices in violation of competition may file actions for damages. In accordance with the provision of article 58 of the Law no. 4054, if the loss is caused by "agreements" or "decisions" or "gross negligence" of the parties, compensation amounting to three times the material losses that have been incurred or the profit obtained or to be potentially obtained by the parties that caused the loss could be imposed upon request of the party at loss.

Fines to be Imposed on Employees:

If an enterprise violates competition, (in case of behavior prohibited by articles 4, 6, and 7 of the Law no. 4054), a fine up to five per cent (5%) of the fine imposed on the enterprise can be imposed on executives and employees of the enterprise, who are determined to have distinctive effects on the violation.

On-Site Inspection Procedure and Actions to be Taken During On-Site Inspection

The Competition Board acts directly or upon applications filed with them. In accordance with article 15 of the Law no. 4054, the Competition Board may perform inspections on enterprises and enterprise associations as it deems necessary when it fulfills the duties assigned by the law to the board. Inspections are performed by an expert authorized by the Competition Board.

On-site inspections are, by definition, performed without prior notice. When assigned experts arrive for on-site inspections;

- Instruct security and reception personnel to allow the experts inside the building.
- In the meantime, inform other unit managers, executive manager specified in company procedures, and your lawyers.
- Be careful not to inform third parties, particularly your competitors, about the on-site inspection; this is considered as "obstruction of investigation".
- Ask the assigned expert to present their certificate of authorization to you, and receive a copy of the certificate of authorization.
- Conduct the on-site inspection in coordination with the experts and within the framework of courtesy. Make them feel that you are ready to cooperate.

- It should be remembered that obstruction of on-site inspection is also subject to administrative fine.
- Assigned experts have the authority to perform inspections in all buildings, vehicles, and other areas of the company, request all documents, examine documents, e-mails, books, and papers, make copies of these, ask questions to employees about events and documents.
- In accordance with article 15/1(a) of the LPC; they "can examine all kinds of data and books kept on physical and electronic media, as well as information systems, make copies and obtain physical samples of these.
- Messages of employees on Whatsapp and other instant messaging applications can be examined as well.
- The fact that drawers and cabinets are closed and computers are password-protected does not prevent these from being examined.
- Do not attend meetings on your own as far as possible. Carefully note the questions asked by experts in the meeting. Do not hesitate to ask for information about subject and scope of, and reason for investigation.
- Respond to questions asked by the experts to the extent that you are sure about the answer. Avoid responding to questions, which you are not sure how to answer and which are aimed at admission. Try to give short answers relevant to the subject.
- Confidentiality is not a valid reason to avoid providing documents to competition experts. You may try to prevent experts from accessing unrelated documents, but remember that the experts make the final decision.
- Make copies and a list of documents seized by the experts. Meticulously examine the minutes issued by the experts, and state your objections, if any. Do not sign the minutes without reading them carefully and consulting your lawyer.

  Five critical points:

  - Cooperation liability
  - Accompanying specialists
  - Copying each document and record that is received

- Avoidance of trying to prevent on-site inspection (cutting off power, locking rooms, deleting electronic files, removing printed documents or computers from the company)
- Reviewing minutes carefully before signing

Which documents can be examined?

- E-mails
- Planners, Books
- Any data and document kept on information systems
- Faxes
- All documents in your computer: videos, audio recordings
- Professional documents
- Travel records, itineraries
- Expense requests, etc.

Rules to be Observed During On-Site Inspection

Always **MAKE SURE** that the experts are accompanied and **REMEMBER** that you are obliged to cooperate.

REMEMBER that assigned experts have the authority to perform inspections in all buildings, vehicles, and other areas of the company, request all documents, examine documents, e-mails, books, and papers, make copies of these, ask questions to employees about events and documents.

MAKE NOTES about all information that are of importance in terms of on-site inspection, such as the subjects inquired by the experts, what kind of questions they asked, and which keywords they used.

Immediately **REQUEST** assistance from the Compliance-Legal Department at any stage where you are not sure about your rights and obligations.

MAKE A COPY of all electronic documents and papers, which are seized or copied by the experts.

PAY ATTENTION to ensure that answers to questions asked by the experts are short and relevant to the subject.

RESPOND TO questions by remaining within the scope of the question.

Carefully **EXAMINE** the minutes issued by the Competition Board experts as a result of the on-site inspection.

DO NOT ENGAGE IN hostile behavior, **DO NOT PANIC**, or **DO NOT OBSTRUCT/PREVENT** the inspection.

DO NOT ENGAGE IN any misconduct that would compromise your situation, such as destroying any document, deleting files from computers, hiding documents or computers, or warning third parties about inspections.

DO NOT VOLUNTEER to provide any document or information, unless requested directly. **AVOID** commenting about matters, which you are not sure how to respond.

DO NOT DECLINE providing information or documents without a clear legal opinion indicating that declining to provide information of documents is legal.

DO NOT LEAVE experts unattended, without someone to accompany them.

The fact that drawers and cabinets are closed and computers are password-protected shall **NOT PREVENT** these from being examined.

Respond to questions asked by the experts to the extent that you are sure about the answer. **AVOID** responding to questions, which you are not sure how to answer and which are aimed at admission.

DO NOT SIGN minutes without making sure that the conversation was completely and correctly written into minutes**.**

Commitment and Settlement in Preliminary Inquiries and Investigations

Commitments:

If the relevant enterprise makes commitments to eliminate concerns about competition that arise within the scope of articles 4 and 6 of the LPC and such commitments are accepted by the Board, it would be possible not to investigate the enterprise that made a commitment or end an ongoing investigation. No commitment is accepted about explicit and gross violations.

- The Board accepted a commitment made by the enterprise in an ongoing investigation with its decision dated 05.11.2020, and decided in favor of ending the investigation in terms of such enterprise. Such decision is the first example of the commitment mechanism practice.

Settlement Procedure:

The Board may initiate the settlement procedure, in consideration of benefits arising from quick finalization of the investigation process and opinion differences concerning presence or scope of violation, directly or upon request of relevant parties. It is possible for the enterprise, which is under investigation and which accepts the presence of violation, and the Board to reach a settlement until notification of the investigation report. The administrative fine to be determined as a result of the settlement procedure can be discounted up to twenty five per cent.

"De Minimis" Exception

In accordance with the De Minimis Exception introduced by Paragraph 2 of Article 41 of the Law, the Board may avoid investigating agreements, concerted practices, and enterprise association decisions and actions which do not considerably restrict the competition in the market based on criteria such as market share and turnover, with the exception of explicit and gross violations such as price fixation by competitors, region or customer sharing, and restriction of supply amount.

The regulation enabled the Authority to avoid investigating non-competitive behavior that do not considerably restrict the competition in the market. This exception, also applied in the European Union and called "de minimis", aims to achieve procedural economy by avoidance of investigating behavior that do not considerably restrict the competition in the market based on criteria such as market share and turnover, with the exception of explicit and gross violations such as price fixation by competitors, region or customer sharing, and restriction of supply amount.

TERMINATION OF VIOLATION

If the Competition Board determines upon a warning, complaint, request of the Ministry of Commerce, or directly that articles 4, 6, and 7 of the Law (agreements and practices limiting competition, abuse of dominant position, and performance of a merger/acquisition that creates a dominant position or strengthens dominant position) was violated, it states behaviors that should be exhibited or avoided by relevant enterprises or enterprise associations to form competition and structural measures such as transfer of certain activities, partnership shares, or assets by enterprises in its final decision.

Behavioral and structural measures should be proportional to the violation and necessary to terminate the violation effectively. Structural measures are

implemented only in case previously imposed behavioral measures do not yield results. If it is determined with a final decision that behavioral measures do not yield results, at least a 6-month period is granted to relevant enterprises or enterprise associations to observe the structural measures.

An amendment stipulated that structural measures could be imposed in addition to behavioral measures in final decisions of the Board.

This regulation stipulates that the Board may decide in favor of structural measures such as transfer of certain activities, partnership shares, or assets by enterprises.

In order for structural measures to be imposed by the Board, a behavioral measures that prescribe performance or non-performance of a certain action should have been imposed and not yielded any result in the first place, and prescribed structural measure should be proportional to the violation and necessary in effective termination of the violation.

Annex 3: Enerjisa Üretim Personal Data Protection Policies and Procedures

Annex 3-A: Personal Data Protection and Processing Policy

1. PURPOSE AND SCOPE

Enerjisa Üretim, having adopted paying maximum attention to compliance with the legal order since the past, establishes systems for conducting all kinds of activities necessary for compliance with the legislation on processing and protection of personal data.

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

In line with the emphasis placed on protection of personal data by the Company, PDP Policy of the Company establishes the fundamental principles concerning compliance of activities conducted by the Company with the regulations in the Law no. 6698 on Protection of Personal Data ("LPPD"). Sustainability of data security principles adopted by the Company shall be ensured upon implementation of PDP Policy regulations of the Company.

PDP Policy of the Company is about real persons, whose personal data is processed by the Company with automated means or non-automated means as part of any data storage system, matters regarding processing of personal data of company employees are set forth separately in the "Policy for Protection and Processing of Personal Data of Company Employees".

2. OBJECTIVE

PDP Policy of the Company aims to establish necessary systems in line with the objective of creating awareness about 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, Company PDP Policy aims to provide guidance for implementation of regulations set forth by the LPPD and applicable legislation.

3. DEFINITIONS

Important terms used in the PDP Policy of the Company and their definitions are as follows:

Explicit Consent	Freely given, specific and informed consent.

Anonymization	Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.
Communiqué on Principles and Procedures to be Observed in Fulfillment of Disclosure Obligation	Communiqué on Principles and Procedures to be Observed in Fulfillment of Disclosure Obligation, which took effect upon issuance in the Official Gazette no. 30356 of March 10, 2018.
Employee(s)	Employee(s) of the Company.
Employee PDP Policy	"Policy for Protection and Processing of Personal Data of Company Employees", which regulates the principles for protection and processing of personal data of company employees.
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (Briefly, "E.ON")
Regulation on Personal Health Data	Regulation on Personal Health Data, issued in the Official Gazette no. 30808 of June 21, 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.
Personal Data Subject	Natural person, whose personal data is processed.
Personal Data Protection Committee	The committee, which will ensure necessary coordination within the Company to ensure, maintain, and sustain compliance of the Company with the personal data protection legislation.
Processing of Personal Data	All kinds of procedures performed on all or a part of the personal data, such as obtaining, recording, storing, retaining, modifying, readjusting, disclosing, transferring, receiving, making available, classifying, or preventing the use of personal data, by automated or partially automated means or non-automated means as part of a data recording system.

LPPD	Law no. 6698 on Protection of Personal Data dated March 24, 2016, issued in the Official Gazette no. 29677 of April 7, 2016.
PDP Board	Personal Data Protection Board.
PDP Authority	Personal Data Protection Authority.
PDP Compliance Program	The program implemented by the Company with regard to ensuring compliance with the legislation on protection of personal data.
Private Personal Data	Data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life, criminal record and safety measures of individuals, as well as biometric and genetic data.
Company	Enerjisa Üretim Santralleri Anonim Şirketi and its subsidiaries.
Business Partners of the Company	Parties, with which the Company engages in business partnerships for various purposes as it conducts business operations.
Personal Data Storage and Destruction Policy of the Company	"Personal Data Storage and Destruction Policy of the Company", which constitutes basis the procedure for determination of maximum period necessary for the processing purpose of personal data processed by the Company, and for deletion, destruction, and anonymization procedures in accordance with the Regulation on Deletion, Destruction, and Anonymization of Personal Data, issued in the Official Gazette no. 30224 of October 28, 2017.
Company PDP Policy	Personal Data Protection and Processing Policy of the Company.
Suppliers of the Company	Parties that offer contractual services to the Company.
Data Subject Application Form of the Company	Application form to be used by data subjects as they make their applications concerning their rights in article 11 of the LPPD.
Sabancı Group Employee PDP Policy	"Policy for Protection and Processing of Personal Data of Sabancı Group Employees", which regulates the principles for protection and processing of

	personal data of employees of the companies within Sabancı Group.
Sabancı Group PDP Policy	"Policy for Protection and Processing of Personal Data of Sabancı Group", which regulates the principles for protection and processing of personal data by Sabancı Group.
Sabancı Group Companies / Group Companies	All companies within Sabancı Group.
Constitution of the Republic of Turkey	Constitution of the Republic of Turkey no. 2709 dated November 7, 1982; issued in the Official Gazette no. 17863 of November 9, 1982.
Turkish Criminal Code	Turkish Criminal Code no. 5237 dated September 26, 2004; issued in the Official Gazette no. 25611 of October 12, 2004.
Data Processor	Natural and legal persons, who process personal data on behalf of the data controller based on the authority granted by the data controller.
Data Controller	The person person who determines the purpose and means of processing personal data and is responsible for the establishment and management of the data filing system.
Communiqué on Principles and Procedures for Application to the Data Controller	Communiqué on Principles and Procedures for Application to the Data Controller, which took effect upon issuance in the Official Gazette no. 30356 of March 10, 2018.

4. ROLES AND RESPONSIBILITIES AND PERSONAL DATA PROTECTION COMMITTEE

Personal Data Protection Committee was established by the Company to ensure necessary coordination within the Company to ensure, maintain, and sustain compliance with the personal data protection legislation. The Commission comprises at least 4 people, Human and Culture Group Manager, Information Technologies Group Manager, Legal Advisor, and a Senior Lawyer among Commission members. Personal Data Protection Committee is responsible for ensuring uniformity between units and departments of the Company, as well as maintenance and improvement

of systems established to ensure compliance of conducted activities with the personal data protection legislation. Committee processes were established with a procedure.

In this context, fundamental duties of the Personal Data Protection Committee are given below:

- To establish a corporate culture that supports the rules on protection and processing of personal data,
- To prepare and implement essential policies regarding protection and processing of personal data upon approval of Human and Culture deputy general manager,
- To resolve on how implementation and inspection of policies on protection and processing of personal data shall be performed and, accordingly, to make internal assignments and ensure coordination,
- To determine steps that should be taken to ensure compliance with the LPPD and applicable legislation, to observe implementation and ensure coordination,
- To increase awareness within the Company and before institutions, with which the Company cooperates, regarding protection and processing of personal data,
- To identify risks that might arise in personal data processing activities of the Company, to ensure that necessary measures are taken, and to offer recommendations for improvement,
- To design and ensure performance of trainings on protection of personal data and implementation of policies,
- To resolve on applications of personal data subjects at the highest level,
- To coordinate performance of information and training activities aimed at ensuring that relevant parties are informed about personal data processing activities of the Company and their legal rights,
- To prepare and implement amendments to essential policies regarding protection and processing of personal data upon approval of Human and Culture deputy general manager,
- Monitoring developments and regulations on protection of personal data, making recommendations to the senior management in respect of necessary actions to be taken in operations of the Company in line with these developments and regulations,

- To manage relationships with the Personal Data Protection Board and Personal Data Protection Authority,
- To fulfill other duties to be assigned by Company management with regard to the protection of personal data.

All business units that process personal data, particularly Human and Culture Department and Information Technologies Department, are responsible for practices such as protection, processing, deletion, and transfer of personal data, and for fulfillment of obligations such as data security, disclosure, and explicit consent, as regulated in the legislation, in respect of the data retained by them. Although Personal Data Protection Committee is responsible for implementation of the Company PDP Policy in all Company operations, activities, and processes; Legal Office shall act as the consultant, source of recommendation, and guide in implementation of regulations, procedures, guidelines, standards, and training activities prepared in line with the Company PDP Policy. All employees, stakeholders, visitors, and relevant third parties throughout the Company are obliged to cooperate with the Legal Office both in compliance with the Company PDP Policy, and prevention of legal risks and immediate threats. All bodies and departments of the Company are responsible for observing compliance with Company PDP Policy.

Human and Culture Deputy General Manager is authorized to modify and implement Policies as necessary, with the exception of revocation of personal data policies.

5. FUNDAMENTALS OF COMPANY PDP POLICY

5.1. SCOPE OF COMPANY PDP POLICY

Data subjects included in the scope of Company PDP Policy, whose personal data is processed by the Company, are grouped as follows:

- Prospective Employees of the Company

  Individuals who have not made a contract of employment with the Company but are being evaluated by the Company to make an agreement.
- Relatives of Employees
- Consultants
- Business Partners of the Company, their Executives and Employees

  Natural person executives, shareholders, employees of organizations in business relationships with the Company.

- Visitors of the Company

  Natural persons who visit Company buildings or websites operated by the Company.

- Other Natural Persons

  All natural persons outside the scope of the Policy for Protection and Processing of Personal Data of Company Employees.

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

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

The Company principally checks whether processing conditions are present as it processes personal data. If such processing conditions are not present, the Company obtains explicit consent from personal data subjects to engage in personal data processing activities.

Under the conditions mentioned above, our Company can process personal data for purposes including but not limited to the following:

	PURPOSES
1	Enforcement of Access Authorizations
2	Conducting Training Activities
3	Conducting Prospective Employee / Intern / Student Selection and Placement Processes,
4	Conducting Application Processes of Prospective Employees
5	Conducting Finance and Accounting Activities
6	Conducting Good / Service Procurement Processes
7	Conducting Contractual Processes
8	Providing Information to Competent Individuals, Institutions, and Organizations
9	Conducting Internal Audit / Investigation / Intelligence Activities
10	Conducting Audit / Ethics Activities
11	Ensuring Physical Location Security
12	Ensuring Security of Data Controller Operations

13	Conducting Occupational Health and Safety Activities
14	Conducting / Auditing Business Activities
15	Conducting Activities in Compliance with the Legislation
16	Conducting Information Security Processes
17	Generation and Follow-up of Visitor Records
18	Organization and Event Management
19	Conducting Business Continuity Activities
20	Conducting Communication Activities
21	Follow-up and Conduct of Legal Affairs
22	Conducting Emergency Management Processes
23	Receiving and Evaluating Recommendations Aimed at Improvement of Business Processes
24	Follow-up of Requests / Complaints
25	Conducting Social Responsibility and Civil Society Activities

6. PRINCIPLES ADOPTED BY THE COMPANY WITH REGARD TO PROCESSING AND PROTECTION OF PERSONAL DATA

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

The Company acts in compliance with (i) fundamental principles, (ii) personal data processing conditions, and (iii) private personal data processing conditions as it conducts data processing activities.

6.1.1. Compliance with Fundamental Principles

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

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

The Company conducts personal data processing activities in compliance with the law and the rules of integrity, pursuant to the legislation on protection of personal data, particularly the Constitution of the Republic of Turkey.

(2) Ensuring accuracy and currency of processed personal data

While personal data processing activity is conducted by the Company, all kinds of necessary administrative and technical measures are taken to ensure accuracy and currency of personal data within technical means. In this scope, our Company established mechanisms to correct and verify accuracy of personal data, in case personal data belonging to personal data subjects are incorrect.

(3) Processing personal data for certain, clear, and legitimate purposes

The Company conducts personal data processing activities pursuant to clear and lawful purposes determined before starting personal data processing activities.

(4) Processing personal data so that they are relevant, limited, and proportionate to the purposes of processing

The Company processes personal data in connection with the conditions of data processing and to the extent necessary for provision of services. In this context, personal data processing purpose is determined before starting personal data processing activity, and data processing activities are not conducted with the assumption that the data could be used in the future. The need for data processing activity and, if necessary, actions to be taken according to the nature of data, are determined and implemented by following the method specified in the Personal Data Processing Necessity and Reasonableness Testing Procedure before personal data processing activities.

(5) Retaining personal data as long as stipulated in the applicable legislation or required for the purpose of their processing

The Company retains personal data for the period stipulated in the applicable legislation or, unless the duration for retaining personal data is stipulated in the legislation, for the period that requires processing in accordance with Company practices, requirements of relevant Institution(s) on the grounds of operating in a regulated industry, and business practices based on the services offered while processing such data. Accordingly, in case the period stipulated in the legislation expires or the reasons that require processing are not available anymore, the Company deletes, disposes, or anonymizes personal data. Rules applicable to this matter are announced in the Personal Data Storage and Destruction Policy.

6.1.2. Compliance with the Conditions for Personal Data Processing

The Company conducts personal data processing activities in compliance with the conditions for data processing set forth in article 5 of the LPPD. In this context,

personal data processing activities are conducted in the presence of the following personal data processing conditions:

(1) Presence of Explicit Consent of Personal Data Subject

The Company conducts personal data processing activities if the data subject provides their consent freely, with adequate knowledge about the matter, clearly and beyond doubt, and limited to that process.

(2) Express Stipulation of Personal Data Processing Activity in the Law

If there is a clear regulation in the law concerning personal data processing activities, the Company may conduct personal data processing activities limited to the applicable legal regulation.

(3) Failure to Obtain Explicit Consent of the Data Subject Due to Actual Impossibility and the Need to Process Personal Data

Under circumstances where personal data subjects cannot declare their consent or their consent is deemed invalid, if it is necessary to process personal data to protect lives and bodily integrity of individuals, the Company conducts data processing activities in this scope.

(4) Direct Relation of Personal Data Processing Activity with Drawing up or Executing an Agreement

Under circumstances directly related to drawing up or execution of an agreement, the Company conducts data processing activities if it is necessary to process personal data of parties to the agreement.

(5) Requirement to Conduct Personal Data Processing Activity for the Company to Fulfill Its Legal Obligation

In case the Company, having adopted acting sensitively as necessary in terms of legal compliance as a Company Policy, has a legal obligation, personal data activities are conducted to fulfill such legal obligation.

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

Personal data, made public (disclosed to the public by any means) by the relevant person, are processed by the Company in compliance with the purpose for which they are made public.

(7) Requirement to Process Data for Establishment, Exercise, or Protection of a Right

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

(8) The Need to Conduct Personal Data Processing Activities for Legitimate Interests of the Company, on the Condition that Fundamental Rights and Liberties of the Data Subject are not Harmed

If it is necessary to process personal data for legitimate interests of the Company, data processing activities can be conducted unless fundamental rights and liberties of the data subject shall not be harmed. In this context, "balance testing" practice recognized in the referenced regulation is conducted by the Company to determine the presence of such condition.

6.1.3. Compliance with the Conditions for Private Personal Data Processing

The Company pays special attention to processing of private personal data that pose the risk of leading to discrimination when processed unlawfully. In this context, the Company sensitively determines whether data processing conditions are present to begin with, then conducts data processing activities after making sure that lawfulness condition is fulfilled. Rules applicable to this matter are announced in the Private Personal Data Protection Policy.

Private personal data can be processed by the Company under the following circumstances provided that adequate measures determined by the PDP Board are taken:

(1) Processing Personal Health Data

The Company can process personal health data in the presence of any condition listed below:

– By entities under confidentiality obligation or authorized institutions and organizations only for the purposes of protection of public health, preventive medicine, performance of medical diagnosis, treatment and care services, planning and management of health services and financing, or

– Presence of explicit consent of personal data subject.

(2) Processing Private Personal Data Other Than Health and Sexual Life

The Company can process private personal data other than health and sexual life (data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life, criminal record and safety measures, as well as biometric and genetic data), provided that the data subject provides explicit consent or under circumstances stipulated in the law.

6.1.4. Compliance with the Conditions for Personal Data Transfer

Personal data transfer conditions, regulated in articles 8 and 9 of the LPPD, are observed in personal data transfers to be performed by the Company.

(1) Domestic Transfer of Personal Data

The Company acts in line with the data processing conditions in domestic data transfer activities pursuant to article 8 of the LPPD.

(2) Transfer of Personal Data Abroad

In accordance with article 9 of the LPPD, personal data can be transferred abroad by the Company in compliance with the requirements for (i) explicit consent or (ii) personal data processing, provided that the recipient country is among countries with adequate protection, announced by the PDP Board, or written commitment of adequate protection by the data controllers in Turkey and the relevant foreign country and permission of the PDP Board in case there is no adequate protection in the relevant foreign country.

Personal data can be transferred by the Company to data centers belonging to Microsoft by taking necessary security measures as a result of utilization of Microsoft Office 365 applications. Such data centers are located in countries listed in the relevant link [1], particularly EU countries and USA. Data hosted in Microsoft data centers are technically inaccessible by third parties, including Microsoft, due to the encryption methods that are used. If Microsoft engineers need to access data for any technical reason, access is technically impossible in case Enerjisa Üretim does not permit such access[2].

[1] Country information for central data center location of Microsoft and information on which data centers are used in access from Turkey are available at the address https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations.

[2] Customer Lockbox feature, which subjects the need to access data to the initiative and permission of Enerjisa Üretim, is enabled on our platform. Details of the technology are accessible via https://social.technet.microsoft.com/wiki/contents/articles/35748.office-365-what-is-customer-lockbox-and-how-to-enable-it.aspx.

6.2. PROVISION OF INFORMATION TO PERSONAL DATA SUBJECTS BY THE COMPANY

The Company conducts necessary processes to ensure that data subjects are informed during collection of personal data pursuant to article 10 of the LPPD and the Communiqué on Principles and Procedures to be Observed in Fulfillment of Disclosure Obligation. In this context, disclosure texts provided by the Company to data subjects contain the following information:

(1) Business name of our company,

(2) Purposes of our Company for processing personal data of data subjects,

(3) Recipients and purpose of transfer of processed personal data,

(4) Method of and legal grounds for personal data collection,

(5) Rights of data subject.

6.3. FINALIZATION OF PERSONAL DATA SUBJECT APPLICATIONS BY THE COMPANY

In the capacity of the data controller and pursuant to article 13 of the LPPD, the Company conducts necessary processes to ensure finalization of applications as soon as possible and at the latest within thirty (30) days according to the nature of request if the data subjects submit their requests concerning their personal data in writing, using the Data Subject Application Form available on www.enerjisauretim.com.tr, or by means of other methods determined by the PDP Board. Data subjects should make their requests concerning their personal data in line 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.

Within the scope of ensuring data security, the Company may request information to determine whether the applicant is the owner of personal data subject to the application. Our Company may also address questions to the personal data subject about their application to ensure that the application of the data subject is finalized in line with the request.

The Company may decline requests by stating their justification in cases such as the potential of the application of the data subject to obstruct rights and liberties of other persons, require disproportionate effort, or involve public information.

6.3.1. Rights of Personal Data Subjects

In accordance with article 11 of the LPPD, data subjects can apply to our Company and file requests about the following matters with the Data Subject Application Form:

(1) Find out whether your personal data was processed,

(2) Request pertinent information if your personal data was processed,

(3) Find out the purpose of processing and whether your personal data was purposefully used,

(4) Find out local and foreign third parties to whom your personal data is transferred,

(5) Request correction of your personal data if it was incompletely or incorrectly processed, and request notification of this procedure to third parties to whom your personal data was transferred,

(6) Request deletion, destruction, or anonymization of your personal data in case the reasons for processing no longer exist, and request notification of this procedure to third parties to whom your personal data was transferred, even though your personal data was processed pursuant to the LPPD and other provisions of applicable law,

(7) Object to an outcome against you due to the analysis of your processed personal data exclusively by means of automated systems,

(8) Request compensation for your losses if you incur losses due to unlawful processing of your personal data.

6.3.2. Circumstances Outside the Rights of Personal Data Subjects Pursuant to the Legislation

Personal data subjects cannot assert their rights in respect of the following matters as the following circumstances are not included in the scope of the LPPD in accordance with article 28 of the LPPD:

(1) Processing personal data for artistic, historic, literary, or scientific purposes or within the scope of freedom of expression, provided that national defense, national security, public security, right to privacy, or personal rights are not violated or no crime is constituted.

(2) Processing personal data for official statistics and purposes such as research, planning, and statistics by way of anonymization.

(3) Processing personal data within the scope of preventive, protective, and informative activities conducted by public institutions and organizations that are lawfully assigned and authorized to ensure national defense, national security, public security, public order, or economic safety.

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

Personal data subjects cannot assert their rights, with the exception of demanding indemnification of losses, under the following circumstances in accordance with article 28/2 of the LPPD:

(1) The need for personal data processing for the prevention of committing a crime or for crime investigation.

(2) Processing personal data which are made public by the personal data subject.

(3) The need for processing personal data for performance of supervision or regulatory duties and disciplinary investigation and prosecution to be carried out by the assigned and authorized public institutions and organizations and by public professional organizations, in accordance with the power conferred on them by the law.

(4) The need for processing personal data for protection economic and financial interests of state related to budget, tax 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 description of such categories, are as follows:

PERSONAL DATA CATEGORIES	EXPLANATION

Identity Information	Personal data that contains information on identity of the person; for example, documents such as driving license, identity card, and passport containing information such as name and surname, TR 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, Social Security Institution ID, signature, vehicle license plate, etc.
Contact Details	Contact details; personal data such as telephone number, address, e-mail address, and fax number.
Physical Location Security Information	Personal data concerning records and documents obtained upon entrance to a physical location and during the stay inside the physical location; camera footage, records made at the security checkpoint, etc.
Process Security Information	Personal data such as IP address information, Website login and logout details, Password and code information, which are processed to ensure technical, administrative, legal, and business security of both the data subject and the Company as business activities of the Company are conducted.
Finance	Personal data such as bank account number, IBAN, credit card details, financial profile, asset data, income details.
Personnel Information	All kinds of personal data, processed to obtain information to serve as a basis for establishment of personnel rights of Company employees or natural people in employment relationships with our Company.
Legal Action	Personal data, processed within the scope of determination and follow-up of legal claims and rights, discharge of obligations, and compliance with legal obligations and Company policies.
Association Membership	If included in the CV of a prospective employee
Foundation Membership	If included in the CV of a prospective employee
Union Membership	If included in the CV of a prospective employee
Professional Experience	Personal data such as diploma information, Attended courses, Vocational training details, Certificates, and Transcript details.

Audio-Visual Records	Audio-Visual Data, Photographs and camera footage (except for footage within the scope of Physical Location Security Information), audio records, and data on documents constituting copies of documents that contain personal data
Philosophical Belief, Religion, Sect, and Other Beliefs	If the data subject presented their old identity card to the Company for Company records, religious details specified in the religion field of the identity card.
Penal Conviction and Security Measures	Criminal record, obtained for generation of personnel file and internal audit processes
Vehicle Information	Vehicle information, received by the Company for the purpose of keeping visitor logs and ensuring physical location security
Health Data	Information on disability status, blood type, personal health, used devices and prostheses, etc.

6.4.2. Recipient Groups

Pursuant to the principles set forth in the LPPD and particularly articles 8 and 9 of the LPPD, personal data of data subjects, included in the scope of Company PDP Policy, can be transferred for specified purposes to the entity groups listed in the following table:

RECIPIENT GROUPS	DEFINITION	DATA TRANSMISSION PURPOSE
Business Partner	Third parties, with which the Company engages in business partnerships for purposes such as conducting business operations	Limited to the purpose of fulfilling the objectives of business partnership
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (Briefly, "E.ON"), which are shareholders of the Company	For purposes such as planning strategic measures regarding business activities and maintaining operations of the Company, including Board resolutions and internal audit reports.

Supplier	Parties that offer contractual services to the Company pursuant to orders and instructions of the Company within the scope of conducting business activities of the Company	Limited to the purpose of offering necessary services, outsourced by the Company from the supplier, to the Company for performance of business operations of the Company
Subsidiaries	Companies, shares of which are held by the Company	Limited to ensuring performance of business activities, which require participation of subsidiaries of the Company as well
Sabancı Group Companies	All companies that comprise Sabancı Group	Limited to the purposes such as planning strategies regarding business activities and maintaining operations of the Company, as well as auditing
Legally Competent Public Institutions and Organizations	Public institutions and organizations that are authorized to obtain information and documents from the Company pursuant to the provisions of applicable legislation	Limited to the purpose of request of relevant public institutions and organizations within their legal authority

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

In order to prevent unlawful disclosure, access, transfer, or other security deficits regarding personal data, the Company takes all kinds of necessary measures that are deemed possible according to the nature of the data to be protected. Applicable rules are given in the Personal Data Storage and Destruction Policy.

In this context, the Company takes all kinds of (i) administrative and (ii) technical measures, (ii) an inspection system is established within the Company, and (iv) actions stipulated in the LPPD are taken in the case of unlawful disclosure of personal data.

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

– The Company trains and raises awareness of employees with regard to the legislation on protection of personal data.

– In case personal data are subject to transfer, the Company ensures that articles, indicating that recipient of personal data shall fulfill obligations aimed at ensuring data security, are added to agreements with parties to whom personal data are transferred by the Company.

– Personal data processing activities conducted by the Company are examined in detail and, in this context, steps to be taken to ensure compliance with the personal data processing conditions stipulated in the LPPD are determined.

– The Company determines the practices to be implemented for ensuring compliance with the LPPD, and regulates these practices with internal policies.

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

– The Company takes technical measures, to the extent enabled by technology, with regard to protection of personal data, and such measures are updated and improved in parallel with developments.

– Specialist personnel is employed for technical issues.

– Implementation of measures are audited at regular intervals.

– Software and systems are installed to ensure security.

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

(3) Audit Activities Conducted by the Company with Regard to Protection of Personal Data

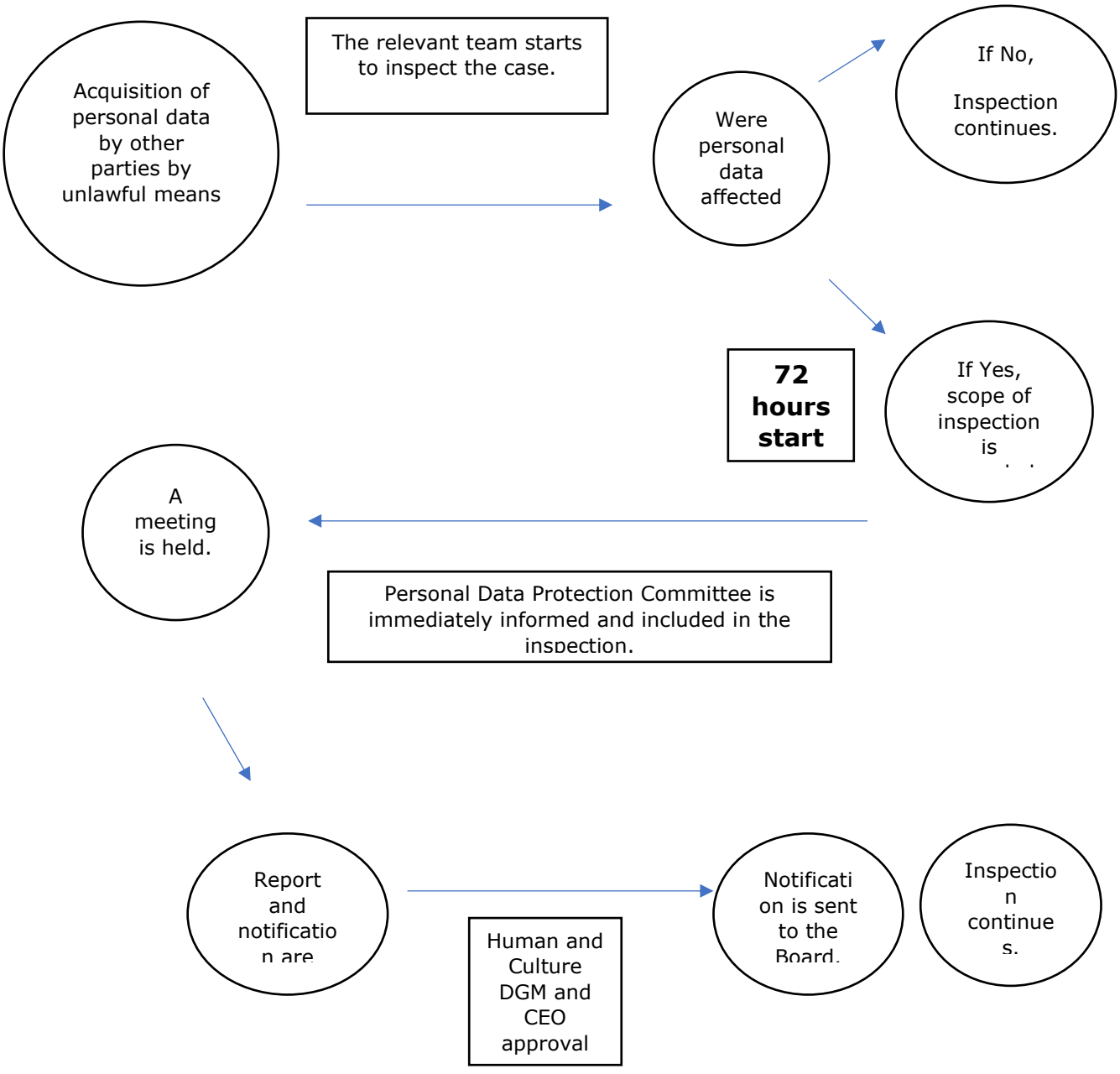
Internal Audit Office of the Company audits compliance of technical measures, administrative measures, and practices, implemented by the Company within the scope of ensuring protection and security of personal data, with applicable legislation, policies, procedures, and instructions, as well as functioning and effectiveness of such measures and practices. Internal Audit Office of the Company can either perform such audit through its organization, or have it conducted by external audit firms as deemed necessary. Results of audit activities conducted in this scope are reported to Internal Audit Committee, CEO, and relevant function managers of the Company. Process owners are responsible for regular follow-up of actions planned with regard to audit results. Process owners periodically submit follow-up and progress reports to the Internal Audit Office of the Company, and Internal Audit Office performs follow-up, validation testing, and audits for actions

within the scope of such reports. Activities, aimed at development and improvement of measures taken with regard to protection of data, are conducted by relevant enforcement units, without being limited to audit results.

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

c) The Company should notify relevant parties and Personal Data Protection Board (hereinafter, "Board") in the shortest time possible if transmitted personal data are obtained by other parties by unlawful means. Such "shortest time" was determined by a Board decision as 72 hours for notifications to be made to the Board.

Relevant units must act swiftly and in coordination to manage this process optimally and to minimize the risks that may arise as a result of Board inspections. Therefore, the flow chart, to be followed in case of occurrence and identification of a data violation, should be as follows:



Unlawful acquisition of personal data, for which the Company as act the data controller, by other parties can be determined primarily by Information Technologies unit. Such a violation can be identified as a finding as a result of inspections conducted by the Internal Audit unit. In such cases or if violation is identified by other units, abovementioned data violation process should be started immediately. If it is determined that personal data were affected by the data violation, Personal Data Protection Committee is promptly included in the process and the situation is promptly notified to kisiselveri@enerjisauretim.com by e-mail.

Relevant matters, particularly conducted detection activities, number of people affected by the violation, number of data affected by the violation, adverse effects of the violation, and measures that should be taken, are evaluated in the meeting to be held by the Personal Data Protection Committee. The Committee may include executives and employees from relevant departments in the meeting if it deems necessary. Information on data violations, effects, and taken measures are recorded. Meeting and determination outcomes are issued as a report and submitted to the approval of Human and Culture Deputy General Manager and CEO with the draft notification. The notification is sent to the Board upon approval.

In case of failure to notify the Board within 72 hours on valid grounds, the reasons for the delay are also submitted to the Board along with the notification to be made. "Personal Data Violation Notification Form", available on the website of the Board, is used for the notification to be made to the Board. In case it is not possible to provide the information on the form at the same time, such information is provided in stages without delay.

Investigations regarding the violation continue within the company. Data subjects, who are determined to have been affected by the violation, are contacted and informed as soon as reasonably possible. If contact address of the relevant person cannot be reached, notification is made through suitable methods such as announcement on the website of the Company. If deemed necessary, public disclosure and information activities are conducted upon receiving the opinion of Corporate Communication unit as well.

6.6. PROCESS FOR COMPLIANCE WITH THE LAW ON PROTECTION OF PERSONAL DATA

The Company conducts a compliance process to ensure fulfillment legal obligations within the scope of the LPPD and applicable legislation, compliance of conducted activities with the legislation on protection of personal data, maintenance and

improvement of established systems, identifications of potential non-compliances, determination of corrective actions to be taken, and to increase awareness within the company by reporting all matters in this regard. Rules concerning the compliance process are set forth in Enerjisa Üretim Compliance Manual and Compliance Policy and Procedure, announced with regard to this process.

7. REVIEW

This Policy document takes effect upon approval of Human and Culture Deputy General Manager of the Company. Human and Culture Deputy General Manager of the Company is responsible for amendments to be made in this Policy and implementation thereof, except for the abolition of this Policy. This Policy can be amended and put into effect upon approval of Human and Culture deputy general manager.

Codes of practice to be issued in affiliation with this Policy, which shall establish the manner of enforcement of matters specified in this Policy regarding certain specific issues, shall be issued as a procedure. Procedures shall be issued and put into effect upon approval of Human and Culture deputy general manager.

This Policy is reviewed at least once a year in any case and, if it is necessary to make amendments, the policy is updated upon submission to the approval of Human and Culture deputy general manager.

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

Company PDP Policy is published on the website (www.enerjisauretim.com) of the Company, and it is accessible by personal data subjects. Modifications to be made on the Company PDP Policy, in parallel with modifications on and newly introduced provisions in the applicable legislation, shall be made available to data subjects so that data subjects can easily access the policy.

Annex 3-B: Policy for Protection and Processing of Personal Data of Employees

1. PURPOSE AND SCOPE

Enerjisa Üretim, having adopted paying maximum attention to compliance with the legal order since the past, establishes systems for conducting all kinds of activities necessary for compliance with the legislation on processing and protection of personal data.

Employee Personal Data Protection (PDP) Policy regulates the principles adopted by the Company for protection and processing of personal data of Company employees.

In line with the emphasis placed on protection of personal data by the Company, Employee PDP Policy establishes the fundamental principles concerning compliance of activities conducted by the Company with the regulations in the Law no. 6698 on Protection of Personal Data ("LPPD"), and sets forth the requirements to be fulfilled by the Company in this context. Sustainability of data security principles adopted by the Company shall be ensured upon implementation of Employee PDP Policy regulations.

2. OBJECTIVE

Employee PDP Policy aims to establish necessary systems in line with the objective of lawful processing and protection of personal data of Employees within the Company, creating awareness in this regard, and to ensure compliance with the legislation.

In this context, Employee PDP Policy aims to provide guidance for Company employees in implementation of regulations set forth by the LPPD and applicable legislation.

3. DEFINITIONS

Important terms used in the Employee PDP Policy and their definitions are as follows:

Explicit Consent	Freely given, specific and informed consent.
Anonymization	Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data.

Communiqué on Principles and Procedures to be Observed in Fulfillment of Disclosure Obligation	Communiqué on Principles and Procedures to be Observed in Fulfillment of Disclosure Obligation, which took effect upon issuance in the Official Gazette no. 30356 of March 10, 2018.
Employee(s)	Employee(s) of the Company.
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (Briefly, "E.ON")
Regulation on Personal Health Data	Regulation on Personal Health Data, issued in the Official Gazette no. 30808 of June 21, 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.
Personal Data Subject	Natural person, whose personal data is processed.
Personal Data Protection Committee	The committee, which will ensure necessary coordination within the Company to ensure, maintain, and sustain compliance of the Company with the personal data protection legislation.
Processing of Personal Data	All kinds of procedures performed on all or a part of the personal data, such as obtaining, recording, storing, retaining, modifying, readjusting, disclosing, transferring, receiving, making available, classifying, or preventing the use of personal data, by automated or partially automated means or non-automated means as part of a data recording system.
LPPD	Law no. 6698 on Protection of Personal Data dated March 24, 2016, issued in the Official Gazette no. 29677 of April 7, 2016.
PDP Board	Personal Data Protection Board.
PDP Authority	Personal Data Protection Authority.
LPPD Compliance Process	The program implemented by the Company with regard to ensuring compliance with the legislation on protection of personal data
Private Personal Data	Data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life,

	criminal record and safety measures of individuals, as well as biometric and genetic data.
Company	Enerjisa Üretim Santralleri A.Ş. and its subsidiaries.
Business Partners of the Company	Parties, with which the Company engages in business partnerships for various purposes as it conducts business operations.
Company PDP Policy	"Policy for Protection and Processing of Personal Data the Company", which regulates the principles for protection and processing of personal data.
Personal Data Storage and Destruction Policy of the Company	"Personal Data Storage and Destruction Policy of the Company", which constitutes basis the procedure for determination of maximum period necessary for the processing purpose of personal data processed by the Company, and for deletion, destruction, and anonymization procedures in accordance with the Regulation on Deletion, Destruction, and Anonymization of Personal Data, issued in the Official Gazette no. 30224 of October 28, 2017.
Company PDP Policy	Personal Data Protection and Processing Policy of the Company.
Suppliers of the Company	Parties that offer contractual services to the Company.
Data Subject Application Form of the Company	Application form to be used by data subjects as they make their applications concerning their rights in article 11 of the LPPD.
Sabancı Group Employee PDP Policy	"Policy for Protection and Processing of Personal Data of Sabancı Group Employees", which regulates the principles for protection and processing of personal data of employees of the companies within Sabancı Group.
Sabancı Group PDP Policy	"Policy for Protection and Processing of Personal Data of Sabancı Group", which regulates the principles for protection and processing of personal data by Sabancı Group.
Sabancı Group Companies / Group Companies	All companies within Sabancı Group.
Constitution of the Republic of Turkey	Constitution of the Republic of Turkey no. 2709 dated November 7, 1982; issued in the Official Gazette no. 17863 of November 9, 1982.
Turkish Criminal Code	Turkish Criminal Code no. 5237 dated September 26, 2004; issued in the Official Gazette no. 25611 of October 12, 2004.

Data Processor	Natural and legal persons, who process personal data on behalf of the data controller based on the authority granted by the data controller.
Data Controller	The person who determines the purpose and means of processing personal data and is responsible for the establishment and management of the data filing system.
Communiqué on Principles and Procedures for Application to the Data Controller	Communiqué on Principles and Procedures for Application to the Data Controller, which took effect upon issuance in the Official Gazette no. 30356 of March 10, 2018.

4. ROLES AND RESPONSIBILITIES

Personal Data Protection Committee was established by the Company to ensure necessary coordination within the Company to ensure, maintain, and sustain compliance with the personal data protection legislation. The Commission comprises at least 4 people, Human and Culture Group Manager, Information Technologies Group Manager, Legal Advisor, and a Senior Lawyer among Commission members. Personal Data Protection Committee is responsible for ensuring uniformity between units and departments of the Company, as well as maintenance and improvement of systems established to ensure compliance of conducted activities with the personal data protection legislation. Committee processes were established with a procedure.

In this context, fundamental duties of the Personal Data Protection Committee are given below:

- To establish a corporate culture that supports the rules on protection and processing of personal data,
- To prepare and implement essential policies regarding protection and processing of personal data upon approval of Human and Culture deputy general manager,
- To resolve on how implementation and inspection of policies on protection and processing of personal data shall be performed and, accordingly, to make internal assignments and ensure coordination,
- To determine steps that should be taken to ensure compliance with the LPPD and applicable legislation, to observe implementation and ensure coordination,

- To increase awareness within the Company and before institutions, with which the Company cooperates, regarding protection and processing of personal data,
- To identify risks that might arise in personal data processing activities of the Company, to ensure that necessary measures are taken, and to offer recommendations for improvement,
- To design and ensure performance of trainings on protection of personal data and implementation of policies,
- To resolve on applications of personal data subjects at the highest level,
- To coordinate performance of information and training activities aimed at ensuring that relevant parties are informed about personal data processing activities of the Company and their legal rights,
- To prepare and implement amendments to essential policies regarding protection and processing of personal data upon approval of Human and Culture deputy general manager,
- Monitoring developments and regulations on protection of personal data, making recommendations to the senior management in respect of necessary actions to be taken in operations of the Company in line with these developments and regulations,
- To manage relationships with the Personal Data Protection Board and Personal Data Protection Authority,
- To fulfill other duties to be assigned by Company management with regard to the protection of personal data

All business units that process personal data, particularly Human and Culture Department and Information Technologies Department, are responsible for practices such as protection, processing, deletion, and transfer of personal data, and for fulfillment of obligations such as data security, disclosure, and explicit consent, as regulated in the legislation, in respect of the data retained by them. Although Personal Data Protection Committee is responsible for implementation of the Employee PDP Policy in all Company operations, activities, and processes; Legal Office shall act as the consultant, source of recommendation, and guide in implementation of regulations, procedures, guidelines, standards, and training activities prepared in line with the Employee PDP Policy.

All employees throughout the Company are obliged to cooperate with the Legal Office both in compliance with the Employee PDP Policy, and prevention of legal risks and immediate threats.

All bodies and departments of the Company are responsible for observing compliance with Employee PDP Policy.

Human and Culture Deputy General Manager is authorized to modify and implement Policies as necessary, with the exception of revocation of personal data policies.

5. FUNDAMENTALS OF EMPLOYEE PDP POLICY

5.1. SCOPE OF EMPLOYEE PDP POLICY

Employees, interns, and company executives (hereinafter, "Employee" or "Data Subject") are governed by the principles regulated with the Employee PDP Policy until their employment agreement with the Company expires. Prospective and former employees of the Company are included in the scope of the Company PDP Policy.

6. PRINCIPLES ADOPTED BY THE COMPANY

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

The Company acts in compliance with (i) fundamental principles, (ii) personal data processing conditions, and (iii) private personal data processing conditions as it conducts Employee data processing activities.

6.1.1. Compliance with Fundamental Principles

The Company adopts the following fundamental principles within the scope of ensuring and maintaining compliance with the legislation in protection of personal data of the Employees:

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

The Company conducts personal data processing activities in compliance with the law and the rules of integrity, pursuant to the legislation on protection of personal data, particularly the Constitution of the Republic of Turkey.

(2) Ensuring accuracy and currency of processed personal data

While personal data processing activity is conducted by the Company, all kinds of necessary administrative and technical measures are taken to ensure accuracy and currency of personal data of the Employees within technical means. In this scope, the Company established mechanisms to correct and verify accuracy of personal data, in case personal data belonging to personal data subject Employees are incorrect.

(3) Processing personal data for certain, clear, and legitimate purposes

The Company conducts personal data processing activities pursuant to clear and lawful purposes determined before starting personal data processing activities.

(4) Processing personal data so that they are relevant, limited, and proportionate to the purposes of processing

The Company processes personal data of Employees in connection with the conditions of data processing and to the extent necessary for achievement of data processing purposes. In this context, personal data processing purpose is determined before starting personal data processing activity, and data processing activities are not conducted with the assumption that the data could be used in the future. The need for data processing activity and, if necessary, actions to be taken according to the nature of data, are determined and implemented by following the method specified in the Personal Data Processing Necessity and Reasonableness Testing Procedure before personal data processing activities.

(5) Retaining personal data as long as stipulated in the applicable legislation or required for the purpose of their processing

The Company retains personal data of Employees for the period stipulated in the applicable legislation or, unless the duration for retaining personal data is stipulated in the legislation, for the period that requires processing in accordance with Company practices, requirements of relevant Institution(s) on the grounds of operating in a regulated industry, and business practices based on the services offered while processing such data. Accordingly, in case the period stipulated in the legislation expires or the reasons that require processing are not available anymore, the Company deletes, disposes or anonymizes personal data. Rules applicable to this matter are announced in the Personal Data Storage and Destruction Policy.

6.1.2. Compliance with the Conditions for Personal Data Processing

The Company processes personal data of the Employees in compliance with the conditions for data processing set forth in article 5 of the LPPD. In this context,

personal data processing activities are conducted in the presence of the following personal data processing conditions:

(1) Presence of Explicit Consent of Personal Data Subject

The Company conducts personal data processing activities if the Employees provides their consent freely, with adequate knowledge about the matter, clearly and beyond doubt, and limited to that process.

(2) Express Stipulation of Personal Data Processing Activity in the Law

If there is a clear regulation in the law concerning personal data processing activities, the Company may conduct personal data processing activities for Employees limited to the applicable legal regulation.

(3) Failure to Obtain Explicit Consent of the Data Subject Employees Due to Actual Impossibility and the Need to Process Personal Data

Under circumstances where Employees cannot declare their consent or their consent is deemed invalid, if it is necessary to process personal data to protect lives and bodily integrity of individuals, the Company conducts data processing activities in this scope.

(4) Direct Relation of Personal Data Processing Activity with Drawing up or Executing an Agreement

Under circumstances directly related to drawing up or execution of an agreement, the Company conducts data processing activities if it is necessary to process personal data of parties to the agreement.

(5) Requirement to Conduct Personal Data Processing Activity for the Company to Fulfill Its Legal Obligation

In case the Company, having adopted acting sensitively as necessary in terms of legal compliance as a Company Policy, has a legal obligation, personal data activities are conducted to fulfill such legal obligation.

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

Personal data, made public (disclosed to the public by any means) by the Employees, are processed by the Company in compliance with the purpose for which they are made public.

(7) Requirement to Process Data for Establishment, Exercise, or Protection of a Right

If it is required to process personal data for establishment, exercise, or protection of a right, the Company processes personal data of the Employees in parallel with this requirement.

(8) The Need to Conduct Personal Data Processing Activities for Legitimate Interests of the Company, on the Condition that Fundamental Rights and Liberties of the Data Subject are not Harmed

If it is necessary to process personal data for legitimate interests of the Company, data processing activities can be conducted unless fundamental rights and liberties of the data subject Employees shall not be harmed. In this context, "balance testing" practice recognized in the referenced regulation is conducted by the Company to determine the presence of such condition.

6.1.3. Compliance with the Conditions for Private Personal Data Processing

The Company pays special attention to processing of private personal data that pose the risk of leading to discrimination when processed unlawfully. In this context, the Company determines whether data processing conditions are present in processing of private personal data of Employees to begin with, then conducts data processing activities after making sure that lawfulness condition is fulfilled. Rules applicable to this matter are announced in the Private Personal Data Protection Policy.

Private personal data can be processed by the Company under the following circumstances provided that adequate measures determined by the PDP Board are taken:

(i) Processing Personal Health Data

The Company can process personal health data of Employees in the presence of any condition listed below:

– by entities under confidentiality obligation or authorized institutions and organizations only for the purposes of protection of public health, preventive medicine, performance of medical diagnosis, treatment and care services, planning and management of health services and financing, or

– Presence of explicit consent of data subject.

(ii) Processing Private Personal Data Other Than Health and Sexual Life

The Company can process private personal data of Employees other than health and sexual life (data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life, criminal record and safety measures, as well as biometric and genetic data), provided that the data subject provides explicit consent or under circumstances stipulated in the law.

6.1.4. Compliance with the Conditions for Personal Data Transfer

Personal data transfer conditions, regulated in articles 8 and 9 of the LPPD, are observed in Employee personal data transfers to be performed by the Company.

(1) Domestic Transfer of Personal Data of Employees

The Company acts in line with the data processing conditions in domestic data transfer activities pursuant to article 8 of the LPPD.

(2) Transfer of Personal Data of Employees Abroad

In accordance with article 9 of the LPPD, personal data can be transferred abroad by the Company in compliance with the requirements for (i) explicit consent or (ii) personal data processing, provided that the recipient country is among countries with adequate protection, announced by the PDP Board, or written commitment of adequate protection by the data controllers in Turkey and the relevant foreign country and permission of the PDP Board in case there is no adequate protection in the relevant foreign country.

Personal data of employees can be transferred by the Company to data centers belonging to Microsoft by taking necessary security measures as a result of utilization of Microsoft Office 365 applications. Such data centers are located in countries listed in the relevant link [3], particularly EU countries and USA. Data hosted in Microsoft data centers are technically inaccessible by third parties, including Microsoft, due to the encryption methods that are used. If Microsoft engineers need to access data for any technical reason, access is technically impossible in case Enerjisa Üretim does not permit such access[4].

[3] Country information for central data center location of Microsoft and information on which data centers are used in access from Turkey are available at the address https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations.

[4] Customer Lockbox feature, which subjects the need to access data to the initiative and permission of Enerjisa Üretim, is enabled on our platform. Details of the technology are accessible via https://social.technet.microsoft.com/wiki/contents/articles/35748.office-365-what-is-customer-lockbox-and-how-to-enable-it.aspx.

6.2. PROVISION OF INFORMATION TO PERSONAL DATA SUBJECTS

The Company conducts necessary processes to ensure that Employees are informed during collection of their personal data pursuant to article 10 of the LPPD and the Communiqué on Principles and Procedures to be Observed in Fulfillment of Disclosure Obligation. In this context, disclosure texts provided by the Company to the Employees contain the following information:

(1) Business name of our company,

(2) Purpose for processing personal data of the Employees,

(3) Recipients and purpose of transfer of processed personal data,

(4) Method of and legal grounds for personal data collection,

(5) Rights granted to the Employees due to being data subjects.

6.3. FINALIZATION OF EMPLOYEE APPLICATIONS REGARDING THEIR PERSONAL DATA

In the capacity of the data controller and pursuant to article 13 of the LPPD, the Company conducts necessary processes to ensure finalization of applications as soon as possible and at the latest within thirty (30) days according to the nature of request if the Employees submit their requests concerning their personal data, arising from being data subjects, in writing, using the **Data Subject Application Form** available on www.enerjisauretim.com.tr or by means of other methods determined by the PDP Board. Data subjects should make their requests concerning their personal data in line 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.

Within the scope of ensuring data security, the Company may request information to determine whether the applicant is the owner of personal data subject to the application. Our Company may also address questions to the personal data subject about their application to ensure that the application of the data subject is finalized in line with the request.

The Company may decline requests by stating their justification in cases such as the potential of data subject applications made by the Employees to obstruct rights and liberties of other persons, require disproportionate effort, or involve public information.

6.3.1. Rights of Employees Concerning Their Personal Data

In accordance with article 11 of the LPPD, Employees can apply to our Company and file requests about the following matters with the **Data Subject Application Form** :

(1) Find out whether your personal data was processed,

(2) Request pertinent information if your personal data was processed,

(3) Find out the purpose of processing and whether your personal data was purposefully used,

(4) Find out local and foreign third parties to whom your personal data is transferred,

(5) Request correction of your personal data if it was incompletely or incorrectly processed, and request notification of this procedure to third parties to whom your personal data was transferred,

(6) Request deletion, destruction, or anonymization of your personal data in case the reasons for processing no longer exist, and request notification of this procedure to third parties to whom your personal data was transferred, even though your personal data was processed pursuant to the LPPD and other provisions of applicable law,

(7) Object to an outcome against you due to the analysis of your processed personal data exclusively by means of automated systems,

(8) Request compensation for your losses if you incur losses due to unlawful processing of your personal data.

6.3.2. Circumstances Outside the Rights of Personal Data Subjects Pursuant to the Legislation

Personal data subjects cannot assert their rights in respect of the following matters as the following circumstances are not included in the scope of the LPPD in accordance with article 28 of the LPPD:

(1) Processing personal data for artistic, historic, literary, or scientific purposes or within the scope of freedom of expression, provided that national defense, national security, public security, right to privacy, or personal rights are not violated or no crime is constituted.

(2) Processing personal data for offical statistics and purposes such as research, planning, and statistics by way of anonymization.

(3) Processing personal data within the scope of preventive, protective, and informative activities conducted by public institutions and organizations that are lawfully assigned and authorized to ensure national defense, national security, public security, public order, or economic safety.

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

Personal data subjects cannot assert their rights, with the exception of demanding indemnification of losses, under the following circumstances in accordance with paragraph two of article 28 of the LPPD:

(1) The need for personal data processing for the prevention of committing a crime or for crime investigation.

(2) Processing personal data which are made public by the personal data subject.

(3) The need for processing personal data for performance of supervision or regulatory duties and disciplinary investigation and prosecution to be carried out by the assigned and authorized public institutions and organizations and by public professional organizations, in accordance with the power conferred on them by the law.

(4) The need for processing personal data for protection economic and financial interests of state related to budget, tax and financial matters.

6.4. PROVISION OF SECURITY AND CONFIDENTIALITY OF PERSONAL DATA OF EMPLOYEES BY THE COMPANY

In order to prevent unlawful disclosure, access, transfer, or other security deficits regarding personal data, the Company takes all kinds of necessary measures that are deemed possible according to the nature of the data to be protected. Applicable rules are given in the Personal Data Storage and Destruction Policy.

In this context, in order to ensure security of personal data of Employees, the Company takes all kinds of (i) administrative and (ii) technical measures, (ii) an inspection system is established within the Company, and (iv) actions stipulated in the LPPD are taken in the case of unlawful disclosure of personal data.

(1) Administrative Measures Taken for Lawful Processing of Personal Data and to Prevent Unlawful Access to Personal Data

– The Company trains and raises awareness of Employees with regard to the legislation on protection of personal data.

– In case personal data are subject to transfer, the Company ensures that articles, indicating that recipient of personal data shall fulfill obligations aimed at ensuring data security, are added to agreements with parties to whom personal data are transferred by the Company.

– Conducted personal data processing activities are examined in detail and, in this context, steps to be taken to ensure compliance with the personal data processing conditions stipulated in the LPPD are determined.

– The Company determines the practices to be implemented for ensuring compliance with the LPPD, and regulates these practices with internal policies.

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

– The Company takes technical measures, to the extent enabled by technology, with regard to protection of personal data, and such measures are updated and improved in parallel with developments.

– Specialist personnel is employed for technical issues.

– Implementation of measures are audited at regular intervals.

– Software and systems are installed to ensure security.

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

(3) Audit Activities Conducted by the Company with Regard to Protection of Personal Data

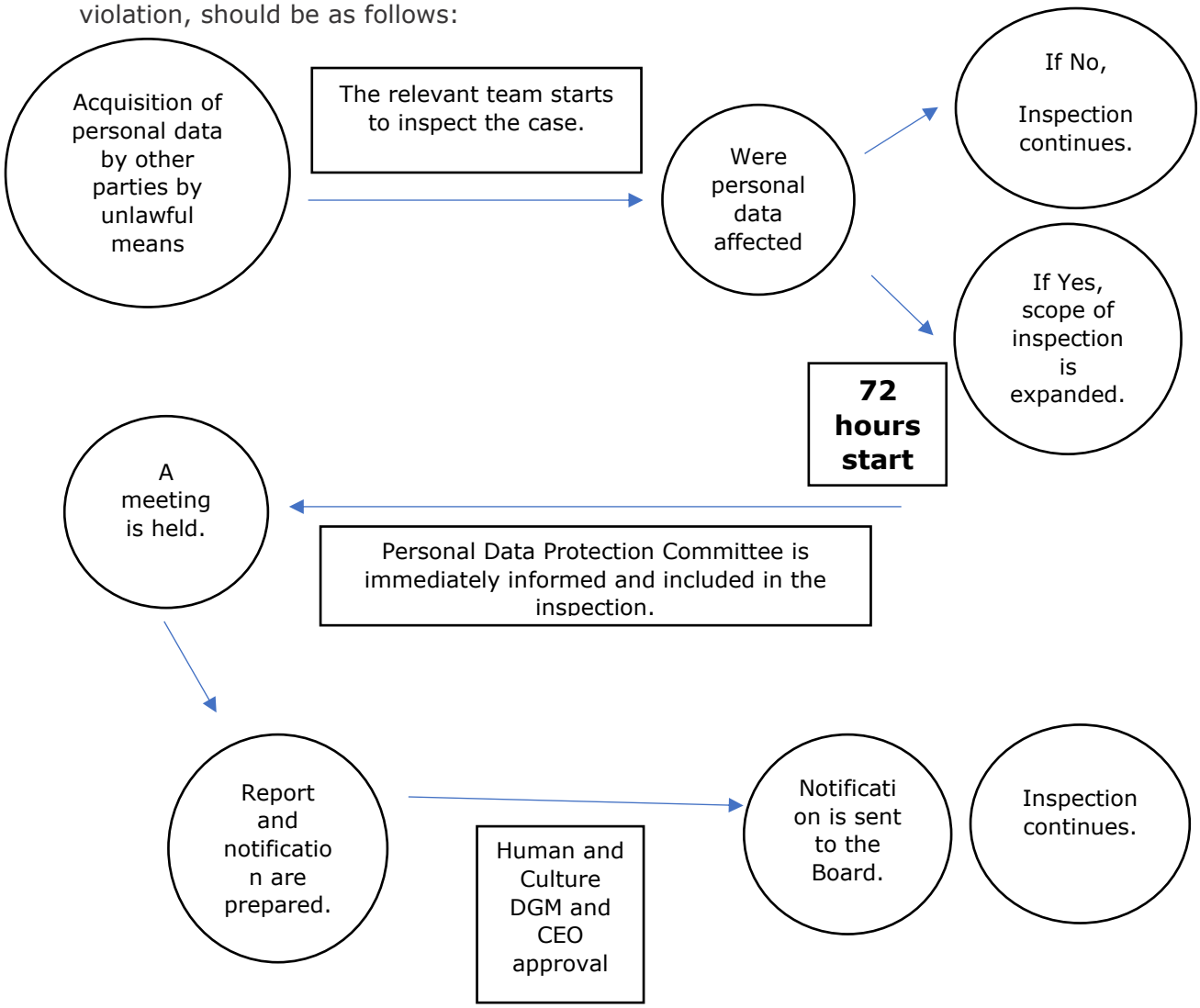
Internal Audit Office of the Company audits compliance of technical measures, administrative measures, and practices, implemented by the Company within the scope of ensuring protection and security of personal data, with applicable legislation, policies, procedures, and instructions, as well as functioning and effectiveness of such measures and practices. Internal Audit Office of the Company can either perform such audit through its organization, or have it conducted by external audit firms as deemed necessary. Results of audit activities conducted in

this scope are reported to CEO and relevant function managers of the Company. Process owners are responsible for regular follow-up of actions planned with regard to audit results. Process owners periodically submit follow-up and progress reports to the Internal Audit Office of the Company, and Internal Audit Office performs follow-up, validation testing, and audits for actions within the scope of such reports. Activities, aimed at development and improvement of measures taken with regard to protection of data, are conducted by relevant enforcement units, without being limited to audit results.

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

c) The Company should notify relevant parties and Personal Data Protection Board (hereinafter, "Board") in the shortest time possible if transmitted personal data are obtained by other parties by unlawful means. Such "shortest time" was determined by a Board decision as 72 hours for notifications to be made to the Board.

Relevant units must act swiftly and in coordination to manage this process optimally and to minimize the risks that may arise as a result of Board inspections. Therefore, the flow chart, to be followed in case of occurrence and identification of a data violation, should be as follows:



Unlawful acquisition of personal data, for which the Company as act the data controller, by other parties can be determined primarily by Information Technologies unit. Such a violation can be identified as a finding as a result of inspections conducted by the Internal Audit unit. In such cases or if violation is identified by other units, abovementioned data violation process should be started immediately. If it is determined that personal data were affected by the data violation, Personal Data Protection Committee is promptly included in the process and the situation is promptly notified to kisiselveri@enerjisauretim.com by e-mail.

Relevant matters, particularly conducted detection activities, number of people affected by the violation, number of data affected by the violation, adverse effects of the violation, and measures that should be taken, are evaluated in the meeting to be held by the Personal Data Protection Committee. The Committee may include executives and employees from relevant departments in the meeting if it deems necessary. Information on data violations, effects, and taken measures are recorded. Meeting and determination outcomes are issued as a report and submitted to the approval of Human and Culture Deputy General Manager and CEO with the draft notification. The notification is sent to the Board upon approval.

In case of failure to notify the Board within 72 hours on valid grounds, the reasons for the delay are also submitted to the Board along with the notification to be made. "Personal Data Violation Notification Form", available on the website of the Board, is used for the notification to be made to the Board. In case it is not possible to provide the information on the form at the same time, such information is provided in stages without delay.

Investigations regarding the violation continue within the company. Data subjects, who are determined to have been affected by the violation, are contacted and informed as soon as reasonably possible. If contact address of the relevant person cannot be reached, notification is made through suitable methods such as announcement on the website of the Company. If deemed necessary, public disclosure and information activities are conducted upon receiving the opinion of Corporate Communication unit as well.

6.5. PROCESS FOR COMPLIANCE WITH THE LAW ON PROTECTION OF PERSONAL DATA

The Company conducts a compliance process to ensure fulfillment legal obligations within the scope of the LPPD and applicable legislation, compliance of conducted activities with the legislation on protection of personal data, maintenance and

improvement of established systems, identifications of potential non-compliances, determination of corrective actions to be taken, and to increase awareness within the company by reporting all matters in this regard. Rules concerning the compliance process are set forth in Enerjisa Üretim Compliance Manual and Compliance Policy and Procedure, announced with regard to this process.

7. PROCESSING CONDITIONS AND PURPOSES FOR PROCESSING PERSONAL DATA OF EMPLOYEES, AND CATEGORIES OF PERSONAL DATA SUBJECT TO DATA PROCESSING ACTIVITIES

7.1. PROCESSING CONDITIONS AND PURPOSES FOR PROCESSING PERSONAL DATA OF EMPLOYEES

Our Company processes personal data for the purposes stated in the following table, limited to the personal data processing conditions specified in paragraph 2 of article 5 and paragraph 3 of article 6 of the LPPD.

The Company principally checks whether processing purposes are present as it processes personal data. If such processing purposes are not present, the Company obtains explicit consent from personal data subjects to engage in personal data processing activities.

Under the conditions mentioned above, our Company can process personal data for purposes including but not limited to the following:

	PURPOSES
1	Enforcement of Wage Policy
2	Conducting Talent / Career Development Activities
3	Conducting Performance Evaluation Processes
4	Conducting Training Activities
5	Conducting Processes for Benefits and Interests of Employees
6	Conducting Employee Satisfaction and Loyalty Processes
7	Conducting Finance and Accounting Activities
8	Providing Information to Competent Individuals, Institutions, and Organizations
9	Conducting Internal Audit / Investigation / Intelligence Activities
10	Conducting Audit / Ethics Activities
11	Ensuring Physical Location Security
12	Ensuring Security of Data Controller Operations
13	Conducting Occupational Health and Safety Activities

14	Conducting / Auditing Business Activities
15	Conducting Activities in Compliance with the Legislation
16	Conducting Information Security Processes
17	Conducting Retention and Archiving Activities
18	Generation and Follow-up of Visitor Records
19	Organization and Event Management
20	Conducting Business Continuity Activities
21	Planning Human Resources Processes
22	Conducting Communication Activities
23	Follow-up and Conduct of Legal Affairs
24	Conducting Emergency Management Processes
25	Fulfillment of Obligations Arising from the Employment Contract and the Legislation for Employees
26	Receiving and Evaluating Recommendations Aimed at Improvement of Business Processes
27	Follow-up of Requests / Complaints
28	Enforcement of Access Authorizations

7.2 CATEGORIES AND RECIPIENT GROUPS OF PERSONAL DATA SUBJECT TO PERSONAL DATA PROCESSING ACTIVITIES REGARDING EMPLOYEES

7.2.1. PERSONAL DATA CATEGORIES

The Company processes personal data of Employees, categorized under the following groups, partially or completely by automated means or non-automated means as part of the data recording system.

PERSONAL DATA CATEGORIES	**EXPLANATION**
Identity Information	Personal data that contains information on identity of the person; for example, documents such as driving license, identity card, and passport containing information such as name and surname, TR 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, Social Security Institution ID, signature, vehicle license plate, etc.
Contact Details	Contact details; personal data such as telephone number, address, e-mail address, and fax number.
Location Data	Personal data that identifies the location of the person as they use company vehicles and devices; GPS location, travel data, etc.

Physical Location Security Information	Personal data concerning records and documents obtained upon entrance to a physical location and during the stay inside the physical location; camera footage, records made at the security checkpoint, etc.
Process Security Information	Personal data such as IP address information, Website login and logout details, Password and code information, which are processed to ensure technical, administrative, legal, and business security of both the data subject and the Company as business activities of the Company are conducted.
Finance	Personal data such as bank account number, IBAN, credit card details, financial profile, asset data, income details.
Personnel Information	All kinds of personal data, processed to obtain information to serve as a basis for establishment of personnel rights of Company employees or natural people in employment relationships with our Company.
Legal Action	Personal data, processed within the scope of determination and follow-up of legal claims and rights, discharge of obligations, and compliance with legal obligations and Company policies.
Professional Experience	Personal data such as diploma information, Attended courses, Vocational training details, Certificates, and Transcript details.
Audio-Visual Records	Audio-Visual Data, Photographs and camera footage (except for footage within the scope of Physical Location Security Information), audio records, and data on documents constituting copies of documents that contain personal data
Philosophical Belief, Religion, Sect, and Other Beliefs	If the data subject presented their old identity card to the Company for Company records, religious details specified in the religion field of the identity card.
Penal Conviction and Security Measures	Criminal record, obtained for generation of personnel file and internal audit processes
Vehicle Information	Vehicle information, received for the purpose of providing benefits/interests offered by the Company to employees, or ensuring physical location security.
Health Data	Information on disability status, blood type, personal health, used devices and prostheses, etc.

7.2.2. RECIPIENT GROUPS

Pursuant to the principles set forth in the LPPD and particularly articles 8 and 9 of the LPPD, the Company may transfer personal data of data subjects, included in the scope of Employee PDP Policy, for specified purposes to the entity groups listed in the following table:

RECIPIENT GROUPS	DEFINITION	DATA TRANSMISSION PURPOSE
Business Partner	Third parties, with which the Company engages in business partnerships for purposes such as conducting business operations	Limited to the purpose of fulfilling the objectives of business partnership
Shareholders	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (Briefly, "E.ON"), which are shareholders of the Company	For purposes such as planning strategic measures regarding business activities and maintaining operations of the Company, including Board resolutions and internal audit reports.
Supplier	Parties that offer contractual services to the Company pursuant to orders and instructions of the Company within the scope of conducting business activities of the Company	Limited to the purpose of offering necessary services, outsourced by the Company from the supplier, to the Company for performance of business operations of the Company
Subsidiaries	Companies, shares of which are held by the Company	Limited to ensuring performance of business activities, which require participation of subsidiaries of the Company as well
Sabancı Group Companies	All companies that comprise Sabancı Group	Limited to the purposes such as planning strategies regarding business activities and maintaining operations of the Company, as well as auditing
Legally Competent Public Institutions and Organizations	Public institutions and organizations that are authorized to obtain information and documents from the Company pursuant to the provisions of applicable legislation	Limited to the purpose of request of relevant public institutions and organizations within their legal authority

8. REVIEW

This Policy document takes effect upon approval of Human and Culture deputy general manager. Human and Culture deputy general manager is responsible for amendments to be made in this Policy and implementation thereof, except for the abolition of this Policy. This Policy can be amended and put into effect upon approval of Human and Culture deputy general manager.

Codes of practice to be issued in affiliation with this Policy, which shall establish the manner of enforcement of matters specified in this Policy regarding certain specific issues, shall be issued as a procedure. Procedures shall be issued and put into effect upon approval of Human and Culture deputy general manager.

This Policy is reviewed at least once a year in any case and, if it is necessary to make amendments , the policy is updated upon submission to the approval of Human and Culture deputy general manager.

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

Employee PDP Policy is available on the internal system named QDMS, and it is accessible by Employees. Modifications to be made on the Employee PDP Policy, in parallel with modifications on and newly introduced provisions in the applicable legislation, shall be made available to data subjects so that data subject Employees can easily access the policy.

Annex 3-C: Personal Data Storage and Destruction Policy

1. INTRODUCTION

Every person is entitled to request protection of personal data about them in accordance with the Constitution of the Republic of Turkey. In terms of protection of personal data, which is a constitutional right, Enerjisa Üretim takes necessary care to protect the personal data of its employees, prospective employees, interns, company shareholders, company executives, as well as employees, shareholders, and executives of establishments with which cooperate, and third parties governed by this Policy, and transforms this into a Company policy.

Protection of personal data, which is a constitutional right, is among the top priorities of our Company. The most important element of this matter comprises storage and destruction processes for the personal data of employees, prospective employees, interns, company shareholders, company executives, visitors, as well as employees, shareholders, and executives of establishments with which we cooperate, and third parties, governed by this Policy.

Despite the presence of disorganized provisions on protection of personal data in our legislation, absence of a special complementary law, which establishes fundamental principles, was considered as a material deficit in our country for a long time. Such deficit was eliminated with the Law no. 6698 on Protection of Personal Data ("LPPD" or "Law"), put into effect upon issuance in the Official Gazette on April 7, 2016, and provisions were regulated with regard to obligations of both public and private sector organizations to ensure confidentiality, security, and purposeful use of personal data.

In this context, Enerjisa Üretim takes necessary administrative and technical measures to protect the personal data processed pursuant to the applicable Law. This Policy contains detailed explanations on the following fundamental principles adopted by Enerjisa Üretim in respect of processing personal data:

- Retaining personal data as long as stipulated in the applicable legislation or required for the purpose of their processing,
- Taking necessary measures regarding storage of personal data,
- Ensuring that third parties observe these principles in case personal data are transferred to third parties in line with the requirements of processing purposes.

1.1. OBJECTIVE OF THE POLICY

The main objective of this Policy is to determine the principal methods for deletion, destruction, or anonymization of personal data, processed pursuant to the provisions of the LPPD and other applicable legislation, in accordance with the provisions of the Regulation on Deletion, Disposal or Anonymization of Personal Data ("Regulation") in case reasons that require processing are not available anymore. Thus, the main aim is to ensure that relevant procedures are conducted systematically within Enerjisa Üretim and to ensure transparency of procedures, carried out for our employees, prospective employees, interns, company shareholders, company executives, visitors, employees of companies with which we cooperate, and all entities, whose personal data are processed by our company, by making explanations about adopted systems.

In line with the objective of the Policy, it is aimed to ensure full compliance with the legislation in personal data protection, storage, and destruction activities conducted by our Company.

1.2. SCOPE OF THE POLICY

This Policy was prepared for our employees, prospective employees, interns, company shareholders, company executives, visitors, employees of companies with which we cooperate/from which we receive services, and all third party entities, whose personal data are processed by our company, and implementation scope of the policy shall cover such people.

This Policy shall be implemented for abovementioned people if our Company processes personal data of such people completely or partially by automated means or non-automated means as part of a data recording system. If the Data is not included in the scope of "Personal Data" within the following scope, or if personal data processing activity conducted by our Company is not subject to abovementioned means, this Policy shall not be applicable as personal data processing, as described within the scope of the LPPD, cannot be referred.

1.3. DEFINITIONS OF LEGAL AND TECHNICAL TERMS USED IN THE POLICY

Definitions in the Law, Regulation, and relevant guidelines published by the Personal Data Protection Board can be referenced for definitions that are not given in this Policy.

Explicit Consent	**:**	Freely given, specific and informed consent.
Anonymization	**:**	Irreversible modification of personal data so that it loses its nature of personal data. E.g.: Rendering data inassociable with a natural person with techniques such as masking, aggregation, data corruption etc.
Prospective Employee	**:**	Natural persons that made a job application to our Company, or made their resumés or relevant details available to examination by our Company by any means.
Group Company	**:**	Enerjisa Üretim Santralleri A.Ş. and its subsidiaries.
Shareholders	**:**	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (Briefly, "E.ON")
Disposal	**:**	Deletion, destruction or anonymization of personal data.
Employees, Shareholders, and Executives of Companies with Which We Cooperate	**:**	Natural persons that are employed in establishments (including but not limited to business partners or suppliers), with which our company engages in any business relationship, including shareholders and executives of such establishments.
Obfuscation	**:**	Actions such as blacking out, painting over, and blurring all personal data, so that they cannot be associated with an identified or identifiable natural person.
Personal Data	**:**	Any information relating to an identified or identifiable natural person. Therefore, the Law does not cover processing of information concerning legal entities. For example; name and surname, TR ID, e-mail, address, date of birth, credit card number, etc.
Processing of Personal Data	**:**	All kinds of procedures performed on all or a part of the personal data, such as obtaining, recording, storing, retaining, modifying, readjusting, disclosing, transferring, receiving, making available, classifying, or preventing the use of personal data, by automated or partially automated means or non-automated means as part of a data recording system.

Personal Data Protection Board	**:**	The Board authorized for enforcement and administration of the LPPD.
Personal Data Subject/Relevant Person	**:**	Natural person, whose personal data is processed.
Masking	**:**	Actions such as erasing, blacking out, painting over, and using asterisks to hide certain personal data, so that they cannot be associated with an identified or identifiable natural person.
Private Personal Data	**:**	Data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life, criminal record and safety measures of individuals, as well as biometric and genetic data, constitute private personal data.
Company Executive	:	Natural person board members and other executives of our Company
Third Party	:	Third party natural persons (e.g. family members and relatives) associated with such persons, for the purpose of ensuring security of business transactions with the parties mentioned above, or protecting the rights of such entities, and afford interests
Data Processor	**:**	Natural and legal persons, who process personal data on behalf of the data controller based on the authority granted by the data controller. For example, cloud computing company that stores employee data, call-center company that makes calls according to scripts, etc.
Data Recording Medium	**:**	Any type of environment that keeps the personal data processed wholly or partially by automated means or non-automated means, provided that they form part of a data recording system.
Data Recording System	**:**	The recording system where personal data are processed by being structured according to specific criteria.
Data Controller	**:**	Data controller is the entity that determines processing purposes and means for personal data, and administers the location where data are retained systematically (data recording system).

Visitor	:	Natural entities that access physical locations owned by our Company for various purposes or that visit our websites

1.4. IMPLEMENTATION OF THE POLICY AND APPLICABLE LEGISLATION

Applicable legal regulations, in force with regard to storage and destruction of personal data, shall be primarily implemented. Our Company acknowledges that the legislation in force shall prevail in case of discrepancy between the legislation in force and the Policy.

The Policy was established by embodiment and regulation of rules, set forth by the applicable legislation, within the scope of Enerjisa Üretim practices.

2. CATEGORIZATION, PROCESSING PURPOSES, AND RETENTION PERIODS OF PERSONAL DATA PROCESSED BY OUR COMPANY

2.1. CATEGORIZATION OF PERSONAL DATA

Personal data in specified categories are processed by Enerjisa Üretim in compliance with the principles set forth and all obligations regulated in the LPPD, based on and limited to one or several personal data processing condition(s) specified in article 5 of the LPPD, in line with the legitimate and lawful personal data processing purposes of our Company. Data subjects regulated within the scope of this Policy, associated with the personal data processed under these categories, are specified in section 3 of this Policy.

Personal Data Categorization	**Personal Data Categorization Description**
Identity Information	Information such as name and surname, mother's - father's name, mother's maiden name, date of birth, place of birth, marital status, series and order no. of identity card, TR identity number, etc. specified on documents such as driving license, identity card, certificate of residence, passport, lawyer identity card, and marriage certificate, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Contact Details	Information such as address, address no., e-mail address, contact address, registered e-mail address (KEP), telephone number, etc. which clearly belong to an identified or identifiable natural person, processed

	partially or completely by automated means or non-automated means as part of the data recording system
Location Data	Information that identifies the location of vehicle owner, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Audio-Visual Records	Audio-Visual Data, Photographs and camera footage (except for footage within the scope of Physical Location Security Information), audio records, and data on documents constituting copies of documents that contain personal data
Physical Location Security Information	Personal data such as records and documents obtained upon entrance to a physical location and during the stay inside the physical location, camera footage and records made at the security checkpoint, visitor entrance and exit logs, etc., which clearly belong to an identified or identifiable natural person, and which are included in the data recording system
Process Security Information	Data such as IP address information, Website login and logout details, Password and code information, etc. which are processed to ensure our technical, administrative, legal, and business security as our business activities are conducted, which clearly belong to an identified or identifiable natural person, and which are included in the data recording system
Financial Information	Processed personal data concerning information, documents, and records indicating any financial outcome created according to the type of legal relationship, established by our company with the personal data subject, as well as bank account number, IBAN, financial profile, etc., which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Personnel Information	Payroll information, disciplinary proceedings, employment certificate records, property declaration information, resumé information, performance evaluation reports, etc., processed to obtain information to serve as a basis for establishment of personnel rights of our employees or natural people in employment relationships with our Company, which clearly belong to an identified or identifiable natural person, processed partially or

	completely by automated means or non-automated means as part of the data recording system
Legal Action	Data such as information in correspondence with judicial authorities and information in court files, processed within the scope of determination and follow-up of our legal claims and rights, discharge of liabilities, and legal obligations, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Professional Experience	Data such as diploma information, attended courses, vocational training details, certificates, transcript details, etc. concerning professional experience, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Philosophical Belief, Religion, Sect, and Other Beliefs	Data such as religion, philosophical belief, sect, other beliefs, etc., which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Association Membership	Data such as association membership information, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Foundation Membership	Data such as foundation membership information, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Union Membership	Data such as union membership information, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Medical Information	Medical data such as disability status, blood type, personal health, used devices and prostheses, etc., which clearly belong to an identified or identifiable natural person, processed partially or completely by automated

	means or non-automated means as part of the data recording system
Penal Conviction and Security Measures	Data such as criminal record, security measures, etc., which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system
Other Information- Vehicle Information	Vehicle information data such as license plate, which clearly belong to an identified or identifiable natural person, processed partially or completely by automated means or non-automated means as part of the data recording system

2.2. PROCESSING CONDITIONS AND PURPOSES FOR PROCESSING PERSONAL DATA

Our Company processes personal data, limited to the personal data processing conditions specified in paragraph 2 of article 5 and paragraph 3 of article 6 of the LPPD. These conditions are;

i) Express stipulation in the legislation that our Company conducts activities with respect to processing of personal data,

ii) The need for our Company to process personal data in direct relation with and as required for drawing up or executing an agreement,

iii) The need to process personal data for compliance with a legal obligation of our Company,

iv) Provided that personal data are made public by the personal data subject, processing of personal data by our Company, limited to the purpose for which they were made public,

v) The need for our Company to process personal data for the establishment, exercise, or protection of the rights of our Company or the personal data subject or third parties,

vi) The need to engage in personal data processing activities for legitimate interests of our Company, on the condition that fundamental rights and liberties of the personal data subject are not harmed,

vii) The need for our Company to engage in personal data processing activities for the protection of life or physical integrity of the personal data subject or another person under circumstances where the personal data subject is unable to explain their consent due to physical disability or legal invalidity,

viii) Stipulation in the law that private personal data of the personal data subject, other than health and sexual life, can be processed,

ix) Processing of private personal data concerning health and sexual life of the personal data subject by entities under confidentiality obligation or authorized institutions and organizations only for the purposes of protection of public health, preventive medicine, performance of medical diagnosis, treatment and care services, planning and management of health services and financing.

The Company principally checks whether abovementioned conditions are present as it processes personal data. If such processing conditions are not present, the Company obtains explicit consent from personal data subjects to engage in personal data processing activities.

Under the conditions mentioned above, our Company can process personal data for purposes including but not limited to the following:

	Purposes
1	Conducting Contractual Processes
2	Conducting Talent / Career Development Activities
3	Conducting Performance Evaluation Processes
4	Conducting Training Activities
5	Conducting Processes for Benefits and Interests of Employees
6	Conducting Employee Satisfaction and Loyalty Processes
7	Conducting Finance and Accounting Activities
8	Providing Information to Competent Individuals, Institutions, and Organizations
9	Conducting Internal Audit / Investigation / Intelligence Activities
10	Conducting Audit / Ethics Activities
11	Ensuring Physical Location Security

12	Ensuring Security of Data Controller Operations
13	Conducting Occupational Health and Safety Activities
14	Conducting / Auditing Business Activities
15	Conducting Activities in Compliance with the Legislation
16	Conducting Information Security Processes
17	Conducting Retention and Archiving Activities
18	Generation and Follow-up of Visitor Records
19	Organization and Event Management
20	Conducting Good / Service Procurement Processes
21	Conducting Business Continuity Activities
22	Planning Human Resources Processes
23	Conducting Communication Activities
24	Follow-up and Conduct of Legal Affairs
25	Conducting Emergency Management Processes
26	Conducting Prospective Employee / Intern / Student Selection and Placement Processes
27	Conducting Application Processes of Prospective Employees
28	Fulfillment of Obligations Arising from the Employment Contract and the Legislation for Employees
29	Receiving and Evaluating Recommendations Aimed at Improvement of Business Processes
30	Conducting Social Responsibility and Civil Society Activities
31	Follow-up of Requests / Complaints
32	Enforcement of Wage Policy
33	Enforcement of Access Authorizations
34	Information given in religion field on old identity cards
35	If included in resumés during the job application process

If personal data subject avoids providing explicit consent, the interpretation should be that personal data processing activities of our relevant business units operating

toward a purpose, other than personal data processing activities within the scope of the same purpose that do not require explicit consent of the personal data subject for data processing as mentioned in the first paragraph, cannot be performed; instead of the performance of all personal data processing activities by our relevant business units within the scope mentioned above.

2.3. PERSONAL DATA RETENTION PERIODS

If a certain period is stipulated in applicable laws and legislation, Enerjisa Üretim retains personal data as long as the period specified in such legislation.

If a certain period, for which personal data should be retained, is not specified in the legislation, personal data are retained for the period that requires processing in accordance with Company practices, requirements of relevant Institution(s) on the grounds of operating in a regulated industry, and business practices based on the services offered by our company while processing such data, upon which personal data is deleted, destroyed, or anonymized. Detailed information on this matter is available in Section 5 of this Policy.

If processing purpose of the personal data is no longer available, and if retention periods stipulated by the applicable legislation and the company have expired, personal data can be retained only for the purpose of constituting evidence in potential legal disputes or assertion of rights or establishment of defense associated with the personal data. In establishment of the periods herein, retention periods are determined on the basis of limitation periods aimed at assertion of the mentioned right, as well as examples in requests that were previously submitted to our Company concerning the same matter despite expiration of limitation periods. In this case, retained personal data are not accessed for any other purpose and such personal data are accessed only when they should be used in the relevant legal dispute. Upon expiration of the period mentioned herein, personal data are deleted, destroyed, or anonymized.

If personal data processed by our Company have been transferred to third parties specified in Section 4, such data must be deleted, destroyed, or anonymized by the recipient third parties upon expiration of the processing purpose of such personal data. Enerjisa Üretim takes necessary measures for this purpose, and provisions concerning these measures are added to agreements. Third parties are notified and their acknowledgment is obtained regarding performance of the procedure.

3. CATEGORIZATION CONCERNING PERSONAL DATA SUBJECTS, WHOSE PERSONAL DATA ARE PROCESSED BY OUR COMPANY

While our Company processes personal data of the following personal data subject categories, implementation scope of this Policy is limited to our employees, prospective employees, interns, company shareholders, company executives, visitors, employees of companies with which we cooperate/from which we receive services, and all third parties, whose personal data are processed by our Company.

Although categories of persons, whose personal data are processed by our Company, are in the scope mentioned above; persons outside these categories may direct their requests to our Company pursuant to the LPPD, and requests of such persons shall also be taken into consideration within the scope of this Policy.

The concepts of our employees, prospective employees, interns, company shareholders, company executives, employees of companies with which we cooperate/from which we receive services, and third parties associated with such persons, included in the scope of this Policy, are clarified below.

Personal Data Subject Category	**Description**
Visitor	Natural entities that access physical locations owned by our Company for various purposes or that visit our websites
Third Party	Third party natural persons (e.g. family members and relatives) associated with such persons, for the purpose of ensuring security of business transactions with the parties mentioned above, or protecting the rights of such entities, and afford interests
Employee	Natural persons, who are affiliated with our Companies under employment contracts, and who serve in this scope
Intern	Natural persons, who serve as interns in our Companies
Prospective Employee	Natural persons that made a job application to our Company, or made their resumés or relevant details available to examination by our Company by any means
Company Executive	Natural person board members and other executives of our Company
Employees of companies with which we cooperate/from which we receive services	Natural persons that are employed in establishments (including but not limited to business partners, dealers, agents, suppliers, consultants, attorneys), with which our company engages in any business relationship, including shareholders and executives of such establishments

Abovementioned personal data subject categories and the types of personal data, processed for the persons in these categories, are detailed below.

Personal Data Categorization	**Personal Data Category Associated with Relevant Personal Data**
Identity Information	Employee, Prospective Employee, Intern, Company Executive, Visitor, Employees of Companies With Which We Cooperate/From Which We Receive Services, Third Party
Contact Details	Employee, Prospective Employee, Intern, Company Executive, Visitor, Employees of Companies With Which We Cooperate/From Which We Receive Services, Third Party
Location Data	Employee
Physical Location Security Information	Employee, Intern, Visitor, Employees of Companies With Which We Cooperate/From Which We Receive Services
Process Security Information	Visitor, Employee, Intern, Employees of Companies With Which We Cooperate/From Which We Receive Services
Audio-Visual Records	Employee, Intern, Employees of Companies With Which We Cooperate/From Which We Receive Services, Third Party
Finance	Employee, Company Shareholder, Company Executive, Employees of Companies With Which We Cooperate/From Which We Receive Services, Third Party
Personnel Information	Employee, Prospective Employee, Intern, Employees of Companies With Which We Cooperate/From Which We Receive Services
Professional Experience	Employee, Intern, Prospective Employee, Employees of Companies With Which We Cooperate/From Which We Receive Services
Legal Action	Employee, Company Executive, Employees of Companies With Which We Cooperate/From Which We Receive Services
Philosophical Belief, Religion, Sect, and Other Beliefs	Employee, Intern
Association Membership	Prospective Employee

Foundation Membership	Prospective Employee
Union Membership	Prospective Employee
Medical Information	Employee, Intern, Employees of Companies With Which We Cooperate/From Which We Receive Services
Penal Conviction and Security Measures	Employee, Intern, Employees of Companies With Which We Cooperate/From Which We Receive Services
Other Information-Vehicle Information	Visitor, Employees of Companies With Which We Cooperate/From Which We Receive Services, Third Party

4. THIRD PARTIES, TO WHOM PERSONAL DATA ARE TRANSFERRED BY OUR COMPANY, AND TRANSFER PURPOSES

Pursuant to articles 8 and 9 of the LPPD, our Company may transfer personal data of data subjects, included in the scope of Company PDP Policy, for specified purposes to the entity groups listed in the following table:

Recipient Groups	Definition	Data Transmission Purpose
Business Partner	Third parties, with which our Company engages in business partnerships for purposes such as conducting business operations.	Transmission of data in a manner limited to and reasonable for the purpose of fulfilling the objectives of business partnership
Supplier	Defines the parties that offer contractual services to our Company pursuant to orders and instructions of our Company within the scope of conducting business activities of our Company.	Transmission of data in a manner limited to and reasonable for the purpose of offering necessary services, outsourced by our Company from the supplier, to our Company for performance of business operations of our Company
Subsidiaries	Companies, shares of which are held by the Company	Transmission of data in a manner limited to and reasonable for ensuring performance of business activities, which require participation of subsidiaries as well, because Enerjisa Üretim Santralleri A.Ş. is an umbrella company.
Sabancı Group Companies	All companies that comprise Sabancı Group.	Transmission of data in a manner limited to and reasonable for purposes such as conducting operational activities, planning strategies for

		business activities, and audit of our Company.
Legally Competent Public Institutions and Organizations	Means the public institutions and organizations that are authorized to obtain information and documents from our Company pursuant to the provisions of applicable legislation.	Transmission of data in a manner limited to and reasonable for the purpose of request of relevant public institutions and organizations within their legal authority Data
Shareholder	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (Briefly, "E.ON"), which are Shareholders of our Company	Transmission of data in a manner limited to and reasonable for purposes such as planning strategic measures regarding business activities and maintaining operations of the Company, including Board resolutions and internal audit reports.

5. CONDITIONS FOR STORAGE, DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

5.1. LEGAL DISCLOSURE CONCERNING THE OBLIGATION FOR STORAGE, DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

Although personal data has been processed pursuant to applicable legal provisions as regulated in article 138 of Turkish Criminal Code and article 7 of the LPPD, such personal data are deleted, destroyed, or anonymized based on the decision of our Company or request of personal data subject if the reasons that require processing are no longer available. In this context, our Company fulfills its relevant obligation using methods explained in this section.

If a request is received in this regard from the personal data subject, an investigation is conducted pursuant to the relevant policy of Enerjisa Üretim, upon which the most suitable method is selected among deletion, destruction, and anonymization procedures, the procedure is performed, and the personal data subject is informed.

5.2. TECHNIQUES FOR DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

Personal data deletion, destruction, and anonymization procedures are performed in compliance with the Regulation and the techniques in the relevant guidelines issued by the Personal Data Protection Board.

5.2.1. Personal Data Deletion and Destruction Techniques

Although personal data has been processed pursuant to applicable legal provisions, our Company may delete or destroy personal data based on its decision or request of personal data subject if the reasons that require processing are no longer available. Deletion or destruction techniques, which are most commonly used by our Company, are listed below:

(i) Physical Destruction

Personal data can also be processed by non-automated means as part of any data recording system. Physical destruction system is implemented, in a manner that would render personal data from being used later, when such data are deleted/destroyed.

(ii) Secure Deletion via Software

Methods for deleting data irrecoverably from the relevant software are used when data processed by completely or partially automated means and stored on digital media are deleted/destroyed.

(iii) Secure Deletion by a Specialist

Enerjisa Üretim may, in certain cases, employ a specialist to delete personal data on its behalf. In this case, personal data are securely and irrecoverably deleted/destroyed by a specialist in this field.

5.3. TECHNIQUES FOR ANONYMIZATION OF PERSONAL DATA

Anonymization of personal data means rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data. Our Company may anonymize personal data when reasons that require processing of personal data, which are processed lawfully, are no longer available.

Pursuant to article 28 of the LPPD, anonymized personal data can be processed for purposes such as research, planning, and statistics. Such processing procedures are outside the scope of the LPPD, and explicit consent of personal data subjects shall not be required.

Anonymization techniques, which are most commonly used by our Company, are listed below.

(i) Masking

Method for anonymization of personal data by removing fundamental identifier information of personal data from the data set by means of data masking.

(ii) Aggregation

Multiple data are aggregated with data aggregation method and personal data are transformed so that they cannot be associated with any person.

(iii) Data Derivation

A more general content is generated from the content of personal data by means of data derivation method, and personal data are transformed so that they cannot be associated with any person.

(iv) Data Shuffling

Data shuffling method ensures that values in the personal data set are shuffled and the connection between values and persons is detached.

5.4. TECHNICAL AND ADMINISTRATIVE MEASURES TO ENSURE SECURE STORAGE OF PERSONAL DATA AND TO PREVENT UNLAWFUL PROCESSING AND ACCESS

	Measures
1	It is planned to perform penetration tests following all major changes in addition to the penetration tests, which are performed once a year for all exterior-facing systems.
2	Alarms were defined for data movements involving critical data, identified on DLP system, to the internet or portable media.
3	It is ensured that received DLP alarms are analyzed by relevant personnel and necessary actions are taken.
4	Personal data are hidden on reports and authorization studies are conducted.
5	Data classification software was installed on the computers of all employees.
6	A data classification system was established to prevent removal of any data from the Company, and it is attempted to prevent data leaks through channels such as e-mail, usb, printer, etc.
7	Confidentiality commitments are received. It is ensured that information security commitments are signed by companies with which the company cooperates/from which services are received, and

	audits on information security and lawful processing of personal data are scheduled at certain intervals based on our right to audit.
8	Operations are conducted to develop systems where approvals obtained for processing of personal data, transfer details, etc. are recorded.
9	Common area authorizations of the company are reviewed.
10	Network security and application security is provided.
11	Closed system network is used in transfer of personal data via network.
12	Key management is implemented.
13	Security measures are taken within the scope of supply, development, and maintenance of information technologies systems.
14	Security of personal data stored on the cloud is ensured.
15	Disciplinary regulations, involving data security provisions for employees, are available.
16	Data security training and awareness activities are conducted for employees at certain intervals.
17	An authorization matrix was established for employees.
18	Access logs are regularly kept.
19	Corporate policies were prepared and started to be implemented about access, information security, use, retention, and destruction.
20	Relevant authorizations for employees, who are reassigned or who leave their jobs, are revoked.
21	Current anti-virus systems are used.
22	Firewalls are used.
23	Signed agreements contain data security provisions.
24	Personal data security policies and procedures were established.
25	Personal data security issues are swiftly reported.
26	Personal data security is monitored.
27	Necessary security measures are taken in respect of entrance to and exit from physical locations containing personal data.
28	Physical locations containing personal data are secured against external risks (fire, flood, etc.).

29	Security of media containing personal data is ensured.
30	Personal data are minimized as much as possible.
31	Personal data are backed up and personal data backups are also secured.
32	User account management and authorization control system are implemented and monitored.
33	Internal periodic and/or random audits are conducted and outsourced.
34	Log records are kept in a manner that prevents user intervention.
35	Existing risks and threats were determined.
36	If private personal data are to be sent by e-mail, they are always sent with encryption and via KEP or corporate e-mail account.
37	Secure encryption / cryptographic keys are used for private personal data and these are administered by different units.
38	Attack detection and prevention systems are used.
39	Penetration testing is conducted.
40	Cyber security measures were taken and their implementation is constantly monitored.
41	Encryption is performed.
42	Private personal data, transferred on portable drives, CDs, and DVDs are transferred with encryption.
43	Service providers that process data are audited in certain intervals with regard to data security.
44	It is ensured that awareness of service providers that process data is raised with regard to data security.
45	Data loss prevention software is used.
46	Locked archive rooms are established and it is attempted to prevent unauthorized third parties from accessing personal data on physical documents.
47	Physical documents in the archive are classified.
48	Documents obtained with agreements, applications, etc. were limited pursuant to the principle of proportionality.

5.5. TECHNICAL AND ADMINISTRATIVE MEASURES TO DESTROY PERSONAL DATA IN COMPLIANCE WITH THE LAW

	Measures
1	Personal data included in the scope of the Policy are identified on all systems.
2	Data to be deleted are informed and it is ensured that deletion decisions are made with the controllers of relevant data.
3	Destruction measures, set forth in this Policy, are performed on the data identified in line with decisions that have been made.

6. RETENTION AND DESTRUCTION PERIODS FOR PERSONAL DATA

6.1. TABLE SHOWING RETENTION AND DESTRUCTION PERIODS FOR PERSONAL DATA

Retention and destruction periods for personal data are shown in the following table on a category basis and indicating the longest periods.

Personal Data Categorization	**Retention and Destruction Period**
Identity Information	15 year after ending of employment
Contact Details	15 year after ending of employment
Location Data	10 year after ending of employment
Personnel	15 year after ending of employment
Legal Action	10 Year
Physical Location Security	10 Year
Process Security	10 Year
Finance	10 Year
Professional Experience	15 year after ending of employment

Audio-Visual Records	15 year after ending of employment
Philosophical Belief, Religion, Sect, and Other Beliefs	15 year after ending of employment
Association Membership	6 Months
Foundation Membership	6 Months
Union Membership	6 Months
Medical Information	15 year after ending of employment
Penal Conviction and Security Measures	15 year after ending of employment
Other Information-Vehicle Information	10 year after ending of employment

In accordance with the relevant process of Human and Culture unit, personal data of prospective employees such as resumés, received and processed during job application, are retained for 6 months, upon expiration of which such data are destroyed pursuant to periodic destruction processes.

6.2. INFORMATION ON PERIODIC DESTRUCTION DURATIONS

Periodic destruction shall be performed in every 6 (six) months beginning from the effective date of the Regulation, and logs for performed procedures shall be retained for 3 (three) years.

7. ROLES AND RESPONSIBILITIES

All organs and departments of the Company are responsible for observing compliance with Personal Data Storage and Destruction Policy and cooperating with the Personal Data Protection Committee. Processes for retention and destruction of personal data shall be conducted by Information Technologies unit and Human and Culture unit. Every relevant unit and department that processes information, particularly Information Technologies unit and Human and Culture unit, is directly responsible for the implementation of this Policy. Legal Office offer consultancy and guidance in conducting processes.

8. REVIEW

This Policy document takes effect upon approval of Human and Culture Deputy General Manager of the Company. Amendments to be made in this Policy and implementation thereof are subject to the approval of the Human and Culture Deputy General Manager of the Company.

Codes of practice to be issued in affiliation with this Policy, which shall establish the manner of enforcement of matters specified in this Policy regarding certain specific issues, shall be issued as Procedures. Procedures shall be issued and put into effect upon approval of Human and Culture Deputy General Manager.

This Policy is reviewed at least once a year in any case and, if it is necessary to make amendments , the policy is updated upon submission to the approval of Human and Culture Deputy General Manager.

The Company acknowledges that applicable legislation shall prevail in case of conflict between the applicable legislation on protection and processing of personal data and this Personal Data Storage and Destruction PDP Policy.

Personal Data Storage and Destruction Policy is published on the website (www.enerjisauretim.com) of the Company, and it is accessible by personal data subjects. Modifications to be made on the Personal Data Storage and Destruction Policy, in parallel with modifications on and newly introduced provisions in the applicable legislation, shall be made available to data subjects so that data subjects can easily access the policy.

Annex 3-D: Private Personal Data Protection Policy

1. PURPOSE AND SCOPE

Enerjisa Üretim, having adopted paying maximum attention to compliance with the legal order since the past, establishes systems for conducting all kinds of activities necessary for compliance with the legislation on processing and protection of personal data.

The principles adopted by the Company for protection of private personal data are regulated pursuant to the Private PDP Policy. This policy shall not be applicable non-private personal data.

In line with the emphasis placed on protection of personal data by the Company, Private PDP Policy establishes the fundamental principles concerning protection and processing of private personal data, in addition to other Company Policies that ensure compliance of activities conducted by the Company with the regulations in the Law no. 6698 on Protection of Personal Data ("LPPD"). Sustainability of data security principles adopted by the Company shall be ensured upon implementation of Private PDP Policy regulations.

Private PDP Policy addresses both company employees and other natural persons, whose private personal data are processed by the Company with automated means or non-automated means as part of any data storage system.

2. OBJECTIVE

Private PDP Policy aims to establish necessary systems in line with the objective of lawful processing and protection of private personal data within the Company, creating awareness in this regard, and to establish the necessary mechanism to ensure compliance with the legislation.

In this context, Private PDP Policy aims to provide guidance for implementation of regulations set forth by the LPPD and applicable legislation.

3. DEFINITIONS

Important terms used in the Private PDP Policy and their definitions are as follows:

Explicit Consent	Freely given, specific and informed consent.
Employee(s)	Employee(s) of the Company.

Employee PDP Policy	"Policy for Protection and Processing of Personal Data of Company Employees", which regulates the principles for protection and processing of personal data of company employees.
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.
Personal Data Subject	Natural person, whose personal data is processed.
Personal Data Protection Committee	The committee, which will ensure necessary coordination within the Company to ensure, maintain, and sustain compliance of the Company with the personal data protection legislation.
Processing of Personal Data	All kinds of procedures performed on all or a part of the personal data, such as obtaining, recording, storing, retaining, modifying, readjusting, disclosing, transferring, receiving, making available, classifying, or preventing the use of personal data, by automated or partially automated means or non-automated means as part of a data recording system.
LPPD	Law no. 6698 on Protection of Personal Data dated March 24, 2016, issued in the Official Gazette no. 29677 of April 7, 2016.
PDP Board	Personal Data Protection Board.
PDP Authority	Personal Data Protection Authority.
Private Personal Data	Data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life, criminal record and safety measures of individuals, as well as biometric and genetic data.
Company	Enerjisa Üretim Santralleri Anonim Şirketi and its subsidiaries.
Business Partners of the Company	Parties, with which the Company engages in business partnerships for various purposes as it conducts business operations.

Personal Data Storage and Destruction Policy of the Company	"Personal Data Storage and Destruction Policy of the Company", which constitutes basis the procedure for determination of maximum period necessary for the processing purpose of personal data processed by the Company, and for deletion, destruction, and anonymization procedures in accordance with the Regulation on Deletion, Destruction, and Anonymization of Personal Data.
Company PD Policy	Personal Data Protection and Processing Policy of the Company.
Suppliers of the Company	Parties that offer contractual services to the Company.
Data Subject Application Form of the Company	Application form to be used by data subjects as they make their applications concerning their rights in article 11 of the LPPD.
Sabancı Group Companies / Group Companies	All companies within Sabancı Group.
Data Processor	Natural and legal persons, who process personal data on behalf of the data controller based on the authority granted by the data controller.
Data Controller	The entity that determines processing purposes and means for personal data, and administers the location where data are retained systematically.
Data Controllers Registry	Public Data Controllers Registry, kept under supervision of the Personal Data Protection Authority, under supervision of the PDP Board

4. ROLES AND RESPONSIBILITIES

All organs and departments of the Company are responsible for observing compliance with Private Personal Data Protection Policy and cooperating with the Personal Data Protection Committee. Processes for protection and processing private personal data shall be conducted by Information Technologies unit and Human and Culture unit. All organs and departments of the Company that process personal data, particularly Human and Culture unit and Information Technologies unit, are directly responsible for observing compliance with Private PDP Policy, fulfillment of obligations set forth in the Policy, and taking measures. Legal Office offer consultancy and guidance in conducting processes.

5. FUNDAMENTALS OF PRIVATE PDP POLICY

5.1. GROUPS OF PERSONS GOVERNED BY PRIVATE PDP POLICY

Data subjects included in the scope of Private PD Policy, whose private personal data are processed by the Company, are grouped as follows:

- Company Employees

  Persons under employment contracts with the Company.

- Interns

  Persons employed as interns in the Company.

- Prospective Employees of the Company

  Individuals who have not made a contract of employment with the Company but are being evaluated by the Company to make an agreement.

- Business Partners of the Company their Executives and Employees

  Natural person executives, shareholders, employees of organizations, business partners, suppliers in business relationships with the Company.

- Other Natural Persons

  All natural persons outside the scope of the Policy for Protection and Processing of Personal Data of Company Employees.

5.2. PURPOSES FOR PROCESSING PRIVATE PERSONAL DATA WITHIN THE SCOPE OF BUSINESS OPERATIONS CONDUCTED BY THE COMPANY

Private personal data of data subjects can be processed for the purposes including, without limitation, the following, within the scope of activities conducted by the Company:

i) Planning Human Resources Processes,

ii) Fulfillment of Obligations Arising from the Employment Contract and the Legislation for Employees,

iii) Conducting Employee Satisfaction and Loyalty Processes,

iv) Conducting Processes for Benefits and Interests of Employees,

v) Conducting Talent / Career Development Activities,

vi) Conducting Performance Evaluation Processes

vii) Conducting Emergency Management Processes

viii) Ensuring Physical Location Security

ix) Conducting Activities in Compliance with the Legislation

x) Conducting / Auditing Business Activities,

xi) Conducting Occupational Health and Safety Activities,

xii) Conducting Audit / Ethics Activities,

xiii) Conducting Internal Audit / Investigation / Intelligence Activities,

xiv) Conducting Business Continuity Activities

xv) If included in resumés during the job application process

6. PRINCIPLES ADOPTED BY THE COMPANY WITH REGARD TO PROCESSING AND PROTECTION OF PRIVATE PERSONAL DATA

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

The Company principally acts in compliance with (i) fundamental principles, (ii) personal data processing conditions, and (iii) private personal data processing conditions, details of which are specified in PD Policy of the Company, as it conducts data processing activities.

6.1.1. Compliance with the Conditions for Private Personal Data Processing

The Company pays special attention to processing of private personal data that pose the risk of leading to discrimination when processed unlawfully. In this context, the Company determines whether data processing conditions are present in processing of private personal data to begin with, then conducts data processing activities after making sure that lawfulness condition is fulfilled.

Private personal data can be processed by the Company under the following circumstances provided that adequate measures determined by the PDP Board are taken:

(1) Processing Personal Health Data

The Company can process personal health data in the presence of any condition listed below:

– by entities under confidentiality obligation or authorized institutions and organizations only for the purposes of protection of public health, preventive medicine, performance of medical diagnosis, treatment and care services, planning and management of health services and financing, or

– Presence of explicit consent of personal data subject.

(2) Processing Private Personal Data Other Than Health and Sexual Life

The Company can process private personal data other than health and sexual life (data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or union membership, health, sex life, criminal record and safety measures, as well as biometric and genetic data), provided that the data subject provides explicit consent or under circumstances stipulated in the law.

6.2. TAKING ADEQUATE MEASURES IN PROCESSING OF PRIVATE PERSONAL DATA

The Company takes the following measures pursuant to the Decision no. 2018/10 of 31/01/2018 of the Personal Data Protection Board as it processes private personal data:

6.2.1. With regard to employees included in the scope of private personal data processing procedures;

(1) Provision of regular trainings about the law and subordinate regulations, as well as private personal data security,

(2) Entering into confidentiality agreements,

(3) Clear definition of authorization scopes and durations for users authorized to access data,

(4) Performance of periodic authorization controls,

(5) Immediate revocation of authorizations for employees, who are reassigned or who leave their jobs, and retrieving inventory allocated to them, if any, within this scope,

6.2.2. If private personal data are processed, stored, and/or accessed on electronic media;

(1) Storage of data using cryptographic methods,

(2) Keeping cryptographic keys on a secure and different media,

(3) Secure logging of activity records for all actions performed on data,

(4) Constant follow-up of security updates for media containing data, regular performance of necessary security testing, recording test results,

(5) If data are accessed by means of a software, making user authorizations for such software, regular performance of security testing for such software, and recording test results,

(6) Provision of at least two-factor authentication system if it is necessary to access data remotely,

6.2.3. If private personal data are processed, stored, and/or accessed on physical media;

(1) Ensuring that adequate security measures (against situations such as electrical failure, fire, flood, theft, etc.) are taken according to the nature of the environment where private personal data is stored,

(2) Ensuring physical security of these environments and preventing unauthorized entry and exit,

6.2.4. If private personal data are to be transferred;

Personal data are transferred by taking necessary security measures for the purposes mentioned above, to the extent required by business processes, and pursuant to the processing conditions required by the legislation and the rules on transfer of personal data, specified in article 8 and 9 of the LPPD; and personal data can be stored on servers and electronic media used within this scope. The nature of such transfers and recipient parties vary based on the type and nature of the relationship between data subjects and the Company, the purpose of transfer, and applicable legal grounds; while measures taken by the Company pursuant to the policies and implementation principles and procedures are valid in this scope.

(1) If it is necessary to transfer the data by e-mail, transferring data with encryption via corporate e-mail address or Registered Electronic Mail (KEP) account,

(2) If it is necessary to transfer data with media such as flash drive, CD or DVD, encryption of data with cryptographic methods and keeping cryptographic key on a different media,

(3) In case of transfer between servers in different physical locations, performance of data transfer by establishing a VPN between servers or by means of sFTP,

(4) If it is necessary to transfer data on paper, necessary measures should be taken against risks such as theft, loss, or unauthorized people viewing the documents, and the documents should be sent in "classified document" format.

7. REVIEW

This Policy document takes effect upon approval of Human and Culture Deputy General Manager of the Company. Amendments to be made in this Policy and implementation thereof are subject to the approval of the Human and Culture Deputy General Manager of the Company.

Codes of practice to be issued in affiliation with this Policy, which shall establish the manner of enforcement of matters specified in this Policy regarding certain specific issues, shall be issued as Procedures. Procedures shall be issued and put into effect upon approval of Human and Culture Deputy General Manager.

This Policy is reviewed at least once a year in any case and, if it is necessary to make amendments , the policy is updated upon submission to the approval of Human and Culture Deputy General Manager.

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

Private PDP Policy is published on the website (www.enerjisauretim.com) of the Company, and it is accessible by personal data subjects. Modifications to be made on the Private PDP Policy, in parallel with modifications on and newly introduced provisions in the applicable legislation, shall be made available to data subjects so that data subjects can easily access the policy.

Annex 3-E: Personal Data Protection Committee Procedure

1. PURPOSE AND SCOPE

The purpose of this document is to establish the objective of and operating procedures for the Personal Data Protection Committee, established within the scope of the process for compliance with the Law no. 6698 on Protection of Personal Data, and the procedure covers Enerjisa Üretim Santralleri A.Ş. and all of its subsidiaries.

2. OBJECTIVE OF THE COMMITTEE

"Personal Data Protection Committee" (Committee) was established by the Company to ensure necessary coordination within the Company to ensure, maintain, and sustain compliance with the personal data protection legislation.

3. DUTIES OF THE COMMITTEE

The Committee is responsible for ensuring uniformity between units of the Company, as well as maintenance and improvement of systems established to ensure compliance of conducted activities with the personal data protection legislation. In this context, fundamental duties of the Committee are as follows:

- To establish a corporate culture that supports the rules on protection and processing of personal data,
- To prepare and implement essential policies regarding protection and processing of personal data of employees upon approval of Human and Culture Deputy General Manager,
- To resolve on how implementation and inspection of policies on protection and processing of personal data of employees shall be performed and, accordingly, to make internal assignments and ensure coordination,
- To determine steps that should be taken to ensure compliance with the LPPD and applicable legislation, to observe implementation and ensure coordination,
- To increase awareness within the Company and before institutions, with which the Company cooperates, regarding protection and processing of personal data,

- To identify risks that might arise in personal data processing activities of the Company, to ensure that necessary measures are taken, and to offer recommendations for improvement,
- To design and ensure performance of trainings on protection of personal data and implementation of policies,
- To resolve on applications of personal data subjects at the highest level,
- To coordinate performance of information and training activities aimed at ensuring that relevant parties are informed about personal data processing activities of the Company and their legal rights,
- To prepare and implement amendments to essential policies regarding protection and processing of personal data upon approval of Human and Culture Deputy General Manager,
- Monitoring developments and regulations on protection of personal data, making recommendations to the senior management in respect of necessary actions to be taken in operations of the Company in line with these developments and regulations,
- To manage relationships with the Personal Data Protection Board and Personal Data Protection Authority,
- To fulfill other duties to be assigned by Company management with regard to the protection of personal data.

4. FINALIZATION OF DATA SUBJECT APPLICATIONS

The Committee is responsible for evaluation and finalization of applications to be made by personal data subjects to the Company. Applications are evaluated and finalized as described in the Procedure for Receiving, Evaluating, and Responding to Data Subject Applications.

5. STRUCTURE OF THE COMMITTEE

The Commission comprises at least 4 people, Human and Culture Group Manager, Information Technologies Group Manager, Legal Advisor, and a Senior Lawyer among Commission members.

6. MANNER OF PERFORMANCE OF DUTIES

a) The Committee convenes twice a year to fulfill its duties set forth in article two, whenever deemed necessary by Committee members. Meeting notes are circulated to all Committee members via kisiselveri@enerjisauretim.com.

b) Data Inventory is reviewed semi-annually by the Committee. The Committee requests semi-annual updates concerning the Data Inventory from departments . The inventory is revised according to updates communicated by departments and updates, if available, are recorded in the Data Registry.

c) The Committee notifies managers of Company units that, in case of any change in personal data processing procedures, they need to notify the Committee before implementing such changes and they should perform relevant actions according to the instructions of the Committee.

Annex 3-F: Personal Data Processing Necessity and Reasonableness Testing Procedure

1. PURPOSE AND SCOPE

The purpose of this procedure is to establish the process for ensuring legal compliance of data processing before personal data are processed pursuant to the Law no. 6698 on Protection of Personal Data.

This procedure covers Enerjisa Üretim Santralleri A.Ş. and all of its subsidiaries.

2. IMPLEMENTATION

Personal data processing comprises all kinds of procedures conducted on your information, including but not limited to obtaining, recording, storage, classification, update, retention, modification, disclosure, transfer, and making data available.

We need to make sure that data processing is lawful before we conduct any processing activity concerning personal data. To this end, we need to follow the steps mentioned below:

A. THE NEED FOR DATA PROCESSING

In order to process personal data, data processing must be necessary in the first place. Thus, our answer to the following questions must be "yes":

1. Is the purpose for Personal Data Processing legitimate, certain, and clear?	Yes	No
2. Are the data necessary to fulfill the purpose?	Yes	No
3. Are unnecessary data excluded from data processing?	Yes	No
4. Are data processed for a limited duration?	Yes	No

If our answer to all questions is "yes", we can pass on to the second stage. Otherwise, we need to continue processing personal data.

B. Determination of Data Type

At this stage, it is necessary to determine whether the data to be processed constitute General Data or Private Data.

Private Personal Data comprises data on race, ethnicity, political view, philosophical belief, religion, sect or other beliefs, manners of clothing, association, foundation or

union membership, health, sex life, criminal record and safety measures of individuals, as well as biometric and genetic data. Such data can be processed only upon obtaining Explicit Consent of the data subject.

If the data to be processed are classified as Private Personal Data, the test should be terminated at this point and it should be investigated whether Explicit Consent is available; if not, Explicit Consent should be obtained.

If the data to be processed do not qualify as Private Personal Data, we need to pass on to the following step and check whether at least one of the data processing conditions is present:

C. Presence of at Least One of the Data Processing Conditions

It should be checked whether at least one of the following conditions is present. These conditions, i.e. conditions of legal compliance, are stipulated in the Law and they cannot be expanded.

1. Express stipulation in the legislation. For example, retention of personal data of employees pursuant to the law.
2. The need for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid. For example, disclosing personal health data of a person who is unconscious.
3. The need to process personal data of contractual parties, provided that it is directly related to drawing up or executing an agreement. For example, processing personal data of employees to issue payrolls or recording address information of the company to make a delivery.
4. The need to process personal data for compliance with a legal obligation of our Company. For example, sharing information during audits specific to areas such as energy or capital markets, fulfilling information requests received from judicial authorities.
5. Being made public by the data subject themselves.

For example, inclusion of contact details of a person, who wants to sell their house, in the sale ad.
6. The need to process data for the establishment, exercise, or protection of any right. For example, retention of necessary information concerning a former employee as long as the limitation of action.
7. Requirement of data processing for lawful and legitimate interests of our company, so that fundamental rights and freedoms of the relevant person are not impaired. For example, processing data for the purpose of offering rewards and premiums that increase employee loyalty.

If at least one of the mentioned data processing conditions is present, we can process data by informing the data subject. Information is provided by means of the Disclosure Text, and original signature is received as proof. With regard to the personal data in question, disclosure text should contain the purpose for data processing, recipients and purpose for transfer of processed personal data, method of and legal grounds for data collection, as well as the rights of the relevant person under the Law on Protection of Personal Data.

Unless at least one of the mentioned conditions is present, data processing can be performed only upon obtaining Explicit consent of the data subject.

If you believe that Disclosure Text and Explicit Consent should be obtained, please receive support from the Personal Data Protection Committee (kisiselveri@enerjisauretim.com).

Caution: Explicit Consent must be obtained if data processing activities involve transfer of data abroad. In such a case, you should primarily contact the Personal Data Protection Committee to request an opinion (kisiselveri@enerjisauretim.com).

Annex 3-G: Procedure for Storing Printed Documents Containing Personal Data for Plants

1. PURPOSE AND SCOPE

The purpose of this procedure is to establish the process for retention of printed documents containing personal data in Plants pursuant to the Law no. 6698 on Protection of Personal Data.

This procedure covers Enerjisa Üretim Santralleri A.Ş. and all of its subsidiaries.

2. IMPLEMENTATION

A. Processing, Retention, and Destruction of Personal Data

Personal data processing means all kinds of procedures conducted on your information, including but not limited to obtaining, recording, storage, classification, update, retention, modification, disclosure, transfer, and making data available. These procedures are conducted in compliance with the Personal Data Protection and Processing Policy of our Company. Personal data storage and destruction processes should be conducted in compliance with the Personal Data Storage and Destruction Policy. Such procedures are published on QDMS.

Our Company acts in the capacity of Data Controller in terms of the personal data that it retains.

B. Retention of Documents Containing Personal Data

Personal data of employees, interns, contractor employee, visitor, family members of employees, and third parties such as consultants can be processed in our plants. These persons are called the Data Subjects.

Our Compant is responsible for ensuring security and confidentiality of Personal Data collected from Data Subjects in the capacity of the Data Controller. Therefore, we must observe the following rules in retention processes for physical documents containing personal data.

1. Physical documents containing personal data;

- should be kept in a locked environment,
- archived in an easily accessible manner, i.e. when searched in the order of name and surname,

- the number of employees with access to the data should be limited to only the necessary individuals,
- data should be protected against access by unauthorized and unrelated persons,
- access by individuals without in unrelated positions should be prevented.

2. Data, legally determined retention periods of which expire, should be destroyed pursuant to the Personal Data Storage and Destruction Policy published on QDMS.

3. Resumés of candidates and interns should not be retained physically. Even if resumés are physically printed, they should be immediately destroyed when they are no longer needed.

4. It must be important for us to act in cooperation with our Human and Culture department in terms of retaining employee, prospective employee, and intern data.

5. Health data of employees comprise private personal data, and they should be kept only by the company doctor.

6. Policy for Protecting and Processing Private Personal Data, published on QDMS, should be observed with regard to private personal data.

In case personal data are unlawfully acquired by unauthorized individuals, Personal Data Protection Committee should be informed promptly by e-mail via kisiselveri@enerjisauretim.com. In addition, Personal Data Protection Committee should be contacted via kisiselveri@enerjisauretim.com for all inquiries.

Annex 3-H: Procedure for Receiving, Evaluating, and Responding to Data Subject Applications

1. PURPOSE AND SCOPE

The purpose of this procedure is to establish the process for receiving, evaluating, and responding to applications by personal data subjects pursuant to the Law no. 6698 on Protection of Personal Data.

This procedure covers Enerjisa Üretim Santralleri A.Ş. and all of its subsidiaries.

2. DEFINITIONS

Abbreviation	Description
Law	Law no. 6698 on Protection of Personal Data
Procedure	Procedure for Receiving, Evaluating, and Responding to Data Subject Applications
Application Form	The form published on the website of the Company and attached to this procedure for use in applications to be made by Data Subjects in accordance with article 13 of the Law
Authority	Personal Data Protection Authority
Board	Personal Data Protection Board
Employees	Company Employees
Company	Enerjisa Üretim Santralleri A.Ş. and its subsidiaries
Data Processor	Real or legal entity that processes personal data on behalf of the data controller as defined in the law
Data Subject	Natural person, whose personal data is processed
Personal Data	Any information relating to an identified or identifiable natural person as long as it is included in the scope of the law
Data Categorization	Category details concerning data subject, personal data, and recipient party, as specified in the Data Inventory
Data Inventory	The document where the inventory of all data processing processes and purposes of the Company is kept
Process	Each data processing activity specified in the Data Inventory

3. IMPLEMENTATION

3.1 Receiving Application

A. Manner of Application

Data subjects may submit their requests to the data controller within the scope of their rights specified in article 11 of the Law in writing or by means of registered e-mail (KEP) address, secure electronic signature, mobile signature, or an e-mail address that was previously notified by the relevant person to the data subject and registered in the system of the data controller, or by means of a software or application developed for the purpose of application.

At this point, the person who receives the application in person, by means of notification procedure, or e-mail, notifies such application by e-mail to the Personal Data Protection Committee via kisiselveri@enerjisauretim.com to have applications recorded and submitted to the relevant person without delay The person that receives the application, particularly the Administrative Affairs unit, is responsible for notification of such applications to the Personal Data Protection Committee.

B. Application Contents

In the application;

a) Name, surname, and signature if the application is in writing,

b) TR Identity Number for citizens of the Republic of Turkey, nationality, passport number, or identity number for foreigners, if available,

c) Residence or workplace address for notification,

ç) E-mail address, telephone, and fax number for notification, if available,

d) Subject matter of request,

must be included.

Relevant information and documents are attached to the application.

Notification date of document to the data controller or their representative is deemed as the application date in respect of written applications.

In respect of applications made by other means, the date when the application is received by the data controller is deemed as the application date.

B.1 Application Made by Agent or Legal Representative

Even if it is indicated in the that the Data Subject may file a request with the Data Controller, there is no rule preventing agent or legal representative of the Data Subject from making the application. Therefore, certain applications cannot be made directly by the Data Subject.

In such case, it should be checked whether the applicant is authorized to make the application. For example, the application can be sent by the lawyer of the Data Subject. In this case, a copy of the power of attorney should be requested from the lawyer to verify their authorization.

Applications for requests concerning Personal Data of children can be made by their legal representatives. In such a case, copies of documents that prove the authority of legal representatives must be requested.

B.2 Collective Application

Multiple Data Subjects can submit their collective applications regarding processed Personal Data according to the structure or commercial nature of the Company. For example, applications can be made about Personal Data of several people with a power of attorney.

In case of a collective application, the Company is advised to separate applications for each person and perform separate evaluations. In such a case, the following actions should be taken:

- Verification of the authorization of third party, who submits the application on behalf of Data Subjects,
- Verification of the identity of the Data Subject.

C. Responding to Applications

The data controller is liable to take all kinds of administrative and technical measures to finalize applications effectively, pursuant to the law and the rules of integrity.

The data controller accepts the application or rejects by stating their justification.

The data controller notifies their response to the relevant person in writing or on electronic media.

Response letter should contain the following elements:

a) Details of the data controller or its representative,

b) Name and surname of the applicant, TR ID number for the citizens of the Republic of Turkey, nationality, passport number or, if available, identity number details for foreigners, residence or work address for notification, e-mail address, telephone and fax number for notification, if available,

c) Subject matter of request,

ç) Explanations of the data controller concerning the application,

The data controller finalizes the requests specified in the application at no charge, as soon as possible and at the latest within thirty days according to the nature of request. However, if the response letter exceeds ten pages, TRY 1 processing fee can be charged for every page exceeding ten pages. If the response to the application is given on a storage media such as CD or flash drive, the fee that can be charged cannot exceed the cost of the storage media. If the application is caused by the mistake of the data controller, charged fee is refunded to the relevant party.

If the request of the relevant person is accepted, necessary action is taken and the relevant person is informed as soon as possible.

D. Application Evaluation Process

Requests of Data Subjects should be evaluated and finalized by the Company as soon as possible and at the latest within 30 days from the date of application. If a response is not given within this period, if the application is declined, or if given response is deemed insufficient, the applicant can file a complaint with the Board within thirty days from the date of finding out about the response and, in any case, within sixty days from the date of application.

Data subject applications are submitted by the Administrative Affairs Office to the Legal Office through the document management system on the date when the applications are received by our Company. Legal Office circulates the request to members of the Personal Data Protection Committee (Committee) via kisiselveri@enerjisauretim.com e-mail address. Requests are responded by Committee members at the latest within one week.

E. Keeping Incident Records

The response sent to the data subject is shared with all Committee members via kisiselveri@enerjisauretim.com e-mail address. Incident records, documents, and outcomes regarding the application in question are stored in the electronic directory created for this matter.

Annex 3-I: Right to Information Application Form within the Scope of the Law on Protection of Personal Data

EXPLANATION

Applications are made upon completion of the following form in writing or by electronic means, by clearly indicating the company that is subject to the applications.

Written applications with original signatures are delivered to the address "**Barbaros Mah. Çiğdem Sk. My Office No:1/16 Ataşehir İstanbul**" of our company in person, or by delivery of application by proxy with a notarized power of attorney indicating that the agent is authorized to file an application with regard to the rights specified within the scope of article 11 of the LPPD, or through notary public.

Electronic applications are made by delivery to the following Registered E-Mail (KEP) address of the relevant company by means of registered e-mail (KEP) address of the Applicant, if available, an electronic signature with "secure electronic signature" certificate, mobile signature, or e-mail address that was previously notified by the Aplicant to our Company and registered in the system of our Company.

enerjisauretimsantralleri@hs01.kep.tr
enerjisadogalgaz@hs01.kep.tr
enerjisasucati@hs01.kep.tr
enerjisatoptansatis@hs01.kep.tr
enerjisauretim@hs01.kep.tr
ibaelektrik@hs01.kep.tr
pervarielektrik@hs01.kep.tr

Company Subject to the Application:

- Enerjisa Üretim Santralleri A.Ş.
- Enerjisa Enerji Üretim A.Ş.
- Enerjisa Elektrik Enerjisi Toptan Satış A.Ş.
- Enerjisa Doğalgaz Toptan Satış A.Ş.
- İBA Elektrik Üretim Madencilik Sanayi ve Ticaret A.Ş.
- Enerjisa Suçatı Elektrik Üretim A.Ş.
- Pervari Elektrik Üretim Madencilik Sanayi ve Ticaret A.Ş.

A. Contact details for the applicant:

Name	:
Surname	:
TR Identity Number	:
Passport Number (For Foreigners)	:
Telephone Number	:
Fax Number	:
E-mail	:
Registered e-mail (KEP - if available)	:

Address :

B. Please describe your relationship with our Company.

☐ Supplier

☐ Former Employee

Years of Employment : ……

☐ Current Employee

☐ Job Application / Resumé Sharing

Date: ……

☐ Third Party Company Employee

Please indicate company, date, and position details pertaining to your employment.

……

☐ Other: …….

The unit with which you communicated within our company, if available:…….……

C. Please indicate the right, under which you are making the request, as specified in article 11 of the LPPD, and your request in detail:

……

……

……

……

……

……

D. Please select the method for notification of our response to your application:

☐ I want it to be sent to my address.

☐ I want it to be sent to my e-mail address.

☐ I want it to be sent to my registered e-mail address.

Applicant (Personal Data Subject)

Name and Surname :

Application Date :

Signature :

This application form was prepared to enable the exercise of your rights specified in the Law on Protection of Personal Data and the applicable legislation and performance of the liabilities of our company in this regard, and it has been devised to enable thorough submission of your application to our Company and prevent you from encountering any delay due to an incomplete application.

You might be required to show or provide proof (e.g. identity card, passport, etc.) regarding the data that you provided during the application to prevent unfair and unlawful processing of your personal data and to avoid potential risks. We would like to inform you that your request shall be declined if it is understood that the data that you requested are not related to personal data or they are related to the personal data of other individuals.