ENERJİSA ÜRETİM SANTRALLERİ A.Ş.

AND AFFILITIES

(“ENERJİSA” or “COMPANY”)

PERSONAL DATA RETENTION AND DESTRUCTION POLICY

("POLICY")

İÇİNDEKİLER

1. ENTRANCE

According to the Constitution of the Republic of Turkey, everyone has the right to request the protection of personal data about him. Regarding the protection of personal data, which is a constitutional right, Enerjisa, governed by this Policy; It pays due attention to the protection of

the personal data of its employees, employee candidates, interns, company shareholders, company officials, visitors, employees, shareholders and officials of the institutions it cooperates with, and third parties and makes this a Company policy.

The protection of personal data, which is a constitutional right, is among the most important priorities of our Company. The most important pillar of this issue is governed by this Policy; It constitutes the storage and destruction of personal data of employees, employee candidates, interns, company shareholders, company officials, visitors, employees, shareholders and officials of the institutions we cooperate with and third parties.

Although there are scattered provisions regarding the protection of personal data in our legislation, the absence of an integral, special law in which the basic principles are determined has been seen as an important deficiency in our country for a long time. With the Law on the Protection of Personal Data No. 6698 ("KVKK" or "Law"), which was published in the Official Gazette on April 7, 2016, this deficiency has been eliminated and provisions have been regulated that both public and private sector organizations will be responsible for ensuring the confidentiality, security and use of personal data in line with its purpose.

In this context, Enerjisa takes the necessary administrative and technical measures to protect the personal data processed in accordance with the relevant Law. In this Policy, detailed explanations will be made regarding the basic principles adopted by Enerjisa in the processing of personal data and listed below:

- To keep personal data for the period stipulated in the relevant legislation or required for the purpose for which they are processed,
- Taking the necessary measures in the protection of personal data,
- Ensuring that third parties comply with these principles in the event that personal data is transferred to third parties in line with the requirements of the processing purpose,
- Compliance with the law and honesty rules,
- Ensuring that personal data is accurate and up-to-date when necessary,
- Processing for specific, explicit, and legitimate purposes,
- Being relevant, limited and proportionate to the purpose for which they are processed

1. Purpose of the Policy

The main purpose of this Policy is to determine the main methods for the deletion, destruction or anonymization of personal data processed in accordance with the provisions of the KVKK and other relevant legislation in accordance with the provisions of the Regulation on the Deletion, Destruction or Anonymization of Personal Data ("Regulation") in the event that the reasons

requiring its processing disappear. Thus, the main goal is; to ensure that the relevant transactions are carried out systematically within Enerjisa and to ensure the transparency of the transactions applied to our employees, employee candidates, interns, company shareholders, company officials, visitors, employees of the companies we cooperate with and all persons whose personal data are processed by our company by making explanations about the systems adopted.

In line with the purpose of the policy, it is aimed to ensure full compliance with the legislation in the protection, storage and destruction of personal data carried out by our Company.

1. Scope of the Policy

This Policy; It has been prepared for our employees, employee candidates, interns, company shareholders, company officials, visitors, employees of the companies we cooperate with/receive services from, and all third parties whose personal data are processed by our company and will be applied within the scope of these specified persons.

This Policy will apply to the above-mentioned data subjects, if our Company processes the personal data of these data subjects by fully or partially automatic or non-automatic means, provided that they are part of any data recording system. If the data is not included in the scope of "Personal Data" within the scope specified below or if the personal data processing activity carried out by our Company is not through the above-mentioned means, this Policy will not be applied as it cannot be mentioned that there is a personal data processing described within the scope of KVKK.

1. Definitions of Legal and Technical Terms in the Policy

For definitions not included in this Policy, the definitions in the Law, Regulation and the relevant guide published by the Personal Data Protection Board can be consulted.

Explicit Consent	**:**	Consent on a specific subject, based on information and expressed with free will.
Anonymization	**:**	It is the change of personal data in such a way that it loses its personal data quality and this situation cannot be undone. For example: Making personal data unassociable with a natural person by techniques such as masking, aggregation, data corruption, etc.
Employee Candidate	**:**	Real persons who have applied for a job in our company in any way or who have opened their resume and related information to our company's review.
Group Company	**:**	Enerjisa Üretim Santralleri A.Ş. and its subsidiaries.
Shareholders	**:**	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDINGS S.A.R.L. (hereinafter referred to as "E.ON")
Annihilation	**:**	Deletion, destruction or anonymization of personal data.
Employees,	**:**	Real persons working in institutions (such as business partners,

Shareholders and Officials of the Companies We Cooperate with		suppliers, but not limited to these) with which our company has all kinds of business relations, including the shareholders and officials of these institutions.
Obfuscation	**:**	Operations such as crossing, painting and icing of all personal data in a way that cannot be associated with an identified or identifiable natural person.
Personal data	**:**	Any information relating to an identified or identifiable natural person. Therefore, the processing of information on legal entities is not within the scope of the Law. For example; name-surname, ID, e-mail, address, date of birth, credit card number, etc.
Processing of Personal Data	**:**	Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means, provided that it is a part of any data recording system.
Personal Data Protection Board	**:**	The Board authorized for the execution and administration of KVKK.
Personal Data Owner/Relevant Person	**:**	The natural person whose personal data is processed.
Masking	**:**	Operations such as deletion, strikethrough, painting and starring of certain areas of personal data in a way that cannot be associated with an identified or identifiable natural person.
Sensitive Personal Data	**:**	Data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data are sensitive data.
Company Official	:	Member of the board of directors of our company and other authorized real persons
Third party	:	Third-party real persons (e.g. family members and relatives) who are related to these persons in order to ensure the security of commercial transactions between our company and the above-mentioned parties or to protect the rights of the aforementioned persons and to obtain benefits,
Data Processor	**:**	It is the natural and legal person who processes personal data on behalf of the data controller based on the authorization given by him. For example, a cloud computing company that keeps employee data, a call-center company that searches within the framework of scripts, *etc.*
Data Recording Media	**:**	Any medium containing personal data that is fully or partially automated or processed by non-automatic means, provided that it is part of any data recording system.
Data Recording System	**:**	It refers to the recording system in which personal data is structured and processed according to certain criteria.

Data Controller	**:**	The data controller is the person who determines the purposes and means of processing personal data and manages the place where the data is kept systematically (data recording system).
Visitor	:	Real persons who have entered the physical campuses owned by our company for various purposes or who visit our websites

1.4. Implementation of the Policy and Related Legislation

The relevant legal regulations in force regarding the storage and destruction of personal data will primarily be implemented. In case of inconsistency between the legislation in force and the Policy, our Company accepts that the current legislation will be implemented.

The policy has been created by concretizing and regulating the rules set forth by the relevant legislation within the scope of Enerjisa practices.

2. STORAGE PERIODS OF PERSONAL DATA PROCESSED BY OUR COMPANY

2.1. Retention Periods of Personal Data

If stipulated in the relevant laws and regulations, Enerjisa keeps its personal data for the period specified in these legislations.

If a period of time is not regulated in the legislation regarding how long personal data should be stored, personal data is processed for the period that requires it to be processed in accordance with the practices of our Company, the demands of the relevant Institution/Institutions due to operating in a regulated sector and commercial practices, depending on the services provided by our company while processing that data, and then it is deleted, destroyed or anonymized. Detailed information on this subject can be found in Article 5 of this Policy. It is included in the section.

The purpose of processing personal data has ended; If the relevant legislation and the retention periods determined by the company have come to an end; Personal data can only be stored for the purpose of constituting evidence in possible legal disputes or asserting the relevant right related to personal data or establishing a defense. In the establishment of the periods herein, the statute of limitations for asserting the aforementioned right and the retention periods are determined on the basis of the examples in the requests made to our Company on the same issues

despite the expiry of the statute of limitations. In this case, the stored personal data is not accessed for any other purpose and access to the relevant personal data is provided only when it is required to be used in the relevant legal dispute. Here, too, after the expiry of the aforementioned period, personal data is deleted, destroyed or anonymized.

Personal data processed by our company, 4. If it has been transferred to the third parties specified in the Section, these data must also be deleted, destroyed or anonymized from the third parties transferred upon the termination of the purpose of processing the relevant personal data. Necessary measures are taken by Enerjisa for this purpose, and provisions regarding these measures are included in the contracts. Within the scope of the measures taken; A commitment is taken that the transaction has taken place by notifying the relevant third parties.

2.2. Recording Media

All personal data subject to data processing activities within the scope of the Law are stored in the following environments where personal data processed by fully or partially automatic or non-automatic means, provided that it is a part of any data recording system, are located.

Electronic Media: In the server and network systems of the company, in the applications developed by the company or outsourced as a service, and in cloud systems
Servers (Databases, E-mail, e-folders belonging to Business Units)
Company-owned mobile devices (mobile phone, computer)
Camera recording area
Website created by contracted companies

Non-Electronic Media: Paper, Manual data recording systems (visitor logbook), lockers, archive room

3. CONDITIONS FOR STORING, DELETING, DESTROYING AND ANONYMIZING PERSONAL DATA

3.1. Legal Statement Regarding the Obligation to Store, Delete, Destroy and Anonymize Personal Data

Although it has been processed in accordance with the provisions of the relevant law as regulated in Article 138 of the Turkish Penal Code and Article 7 of the KVKK, personal data is deleted, destroyed or anonymized upon our Company's own decision or upon the request of the personal data owner, in the event that the reasons requiring its processing disappear. In this context, our Company fulfills its relevant obligation with the methods described in this section.

If a request is received by the personal data owner in this regard, an examination is carried out in accordance with the relevant Enerjisa policy, whichever method is the most appropriate for deletion, destruction or anonymization is selected, the transaction is carried out and the personal data owner is informed.

3.2. Techniques for deletion, destruction and anonymization of personal data

The deletion, destruction and anonymization of personal data are carried out in accordance with the Regulation and the techniques in the relevant guide published by the Personal Data Protection Board.

3.2.1. Techniques for Deletion and Destruction of Personal Data

Although it has been processed in accordance with the provisions of the relevant law, our company may delete or destroy personal data at its own discretion or upon the request of the personal data owner if the reasons requiring its processing disappear. The most commonly used deletion or destruction techniques by our company are listed below:

(i) Physical Destruction

Personal data can also be processed non-automatically, provided that it is a part of any data recording system. While deleting/destroying such data, the system of physical destruction of personal data is applied in a way that cannot be used later.

(ii) Soft Erase Securely

While deleting/destroying data processed by fully or partially automated means and stored in digital media; Methods are used to delete the data from the relevant software in a way that cannot be recovered again.

(iii) Secure Deletion by an Expert

In some cases, Enerjisa may agree with an expert to delete personal data on its behalf. In this case, personal data is securely deleted/destroyed by the expert in this field in a way that cannot be recovered again.

3.2.2. Techniques for Anonymizing Personal Data

Anonymization of personal data means that personal data cannot be associated with an identified or identifiable natural person in any way, even by matching it with other data. Our company can anonymize personal data when the reasons requiring the processing of personal data processed in accordance with the law disappear.

In accordance with Article 28 of the KVKK; Anonymized personal data may be processed for purposes such as research, planning and statistics. Such processing is outside the scope of KVKK and the explicit consent of the personal data owner will not be sought.

The most commonly used anonymization techniques by our company are listed below.

(i) Masking

Data masking is a method of anonymizing personal data by removing the basic determining information of personal data from the data set.

(ii) Consolidation

With the data aggregation method, many data are aggregated and personal data is made unassociable with any person.

(iii) Data Derivation

With the data derivation method, a more general content is created from the content of personal data and it is ensured that personal data cannot be associated with any person.

(iv) Data Hashing

With the data hashing method, it is ensured that the values in the personal data set are mixed and the link between the values and the people is broken.

3.3. Technical and Administrative Measures for the Secure Storage of Personal Data, Unlawful Processing and Prevention of Access

	Measures
1	In addition to the penetration tests carried out once a year for all open systems, penetration tests are planned to be carried out after all major changes.
2	Alarms have been defined for data movements on the internet or portable media containing critical data determined on the DLP system.
3	It is ensured that the DLP alarms that occur are examined by the relevant responsible persons and necessary actions are taken.
4	Closure of personal data in reports and authorization studies are carried out.
5	A data classification program has been installed on all employee computers.
6	A data classification system has been established in order not to remove any data from the company and data leakage is tried to be prevented from channels such as mail, usb, printer, etc.
7	Confidentiality commitments are made. Information security commitments are signed by the companies that cooperate/receive services, and audits regarding information security and the processing of personal data in accordance with the law are planned in certain periods based on our audit right.
8	Efforts are being made to develop systems in which consents to the processing of personal data, transfer details, etc. are recorded.
9	Company common area authorizations are being reviewed.
10	Network security and application security are ensured.
11	Closed system network is used for personal data transfers via the network.
12	Key management is implemented.
13	Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
14	The security of personal data stored in the cloud is ensured.
15	Disciplinary regulations with data security provisions are in place for employees.
16	Training and awareness activities are carried out at regular intervals on data security for

	employees.
17	An authorization matrix has been created for employees.
18	Access logs are kept regularly.
19	Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
20	Employees who have a job change or leave their job are removed from their authority in this area.
21	Up-to-date anti-virus systems are used.
22	Firewalls are used.
23	The signed contracts contain data security provisions.
24	Personal data security policies and procedures have been determined.
25	Personal data security issues are reported quickly.
26	Personal data security is monitored.
27	Necessary security measures are taken regarding entry and exit to physical environments containing personal data.
28	The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured.
29	The security of environments containing personal data is ensured.
30	Personal data is reduced as much as possible.
31	Personal data is backed up and the security of the backed-up personal data is also ensured.
32	User account management and authorization control system are implemented and these are also followed.
33	Periodic and/or random audits are carried out and carried out in-house.
34	Log records are kept in such a way that there is no user intervention.
35	Existing risks and threats have been identified.
36	If sensitive personal data is to be sent via e-mail, it must be sent encrypted and using KEP or corporate mail account.
37	Secure encryption / cryptographic keys are used for sensitive personal data and are managed by different units.
38	Intrusion detection and prevention systems are used.
39	Penetration test is applied.
40	Cyber security measures have been taken and their implementation is constantly monitored.
41	Encryption is done.
42	Sensitive persons data transferred in portable memory, CD, DVD media are encrypted and transferred.
43	Service providers that process data are periodically audited on data security.
44	Awareness of data processing service providers on data security is ensured.
45	Data loss prevention software is used.

46	By creating locked archive rooms, it is tried to prevent unauthorized third parties from accessing personal data on physical documents.
47	Classification of physical documents in the archive is made.
48	Due to the principle of proportionality, documents received with contracts, applications, etc., are restricted.

3.4. Technical and Administrative Measures for the Unlawful Destruction of Personal Data

	Measures
1	In all systems, personal data within the scope of the Policy are determined.
2	It is ensured that decisions are made by informing the responsible persons of the relevant data and the data to be deleted.
3	The destruction measures specified in this Policy are applied to the data determined in line with the decisions taken.

4. PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

4.1. Table Showing Personal Data Storage and Destruction Periods

The retention and destruction periods of personal data are shown in the table below on a category basis and indicating the longest periods.

Personal Data Categorization	**Storage and Disposal Period**
ID	15 years from the date of termination of employment
Contact Information	15 years from the date of termination of employment
Location Data	10 years from the date of termination of employment
Personnel	15 years from the date of termination of employment
Legal Action	10 Years
Physical Space Security	10 Years
Transaction Security	10 Years

Financial Data	10 Years
Professional Experience	15 years from the date of termination of employment
Audiovisual Recordings	15 years from the date of termination of employment
Philosophical Beliefs, Religions, Denominations and Other Beliefs	15 years from the date of termination of employment
Association Membership	2 years
Foundation Membership	2 years
Trade Union Membership	2 years
Health Information	15 years from the date of termination of employment
Criminal Conviction and Security Measures	15 years from the date of termination of employment
Other Information-Vehicle information	10 years from the date of termination of employment

In accordance with the relevant process of the Human and Culture unit, the retention period of personal data such as resumes taken and processed during the job application process of employee candidates is 2 years, and after this period expires, they are destroyed within the periodic destruction processes.

In the event that the person concerned applies to our Company and requests the destruction of his/her personal data, our Company:

(a) all of the conditions for processing personal data have disappeared:

(i) finalizes the request of the person concerned within thirty days at the latest and informs the person concerned, and

(ii) If the personal data subject to the request has been transferred to third parties, it notifies the third party of this situation; ensures that the necessary actions are taken before the third party.

(b) If all of the conditions for processing personal data have not been eliminated, the request of the person concerned may be rejected by explaining the reason in accordance with the

third paragraph of Article 13 of the Law, and notifies the person concerned in writing or electronically within thirty days at the latest.

4.2. Periodic Disposal Times Information

Periodic destruction will be carried out every 6 (six) months starting from the date of entry into force of the Regulation and the logs of the transactions will be kept for 3 (three) years.

5. ROLES AND RESPONSIBILITIES

All organs and departments of the Company are responsible for complying with the Personal Data Retention and Destruction Policy and cooperating with the Personal Data Protection Commission. The processes of storage and destruction of personal data; It will be carried out by the Information Technology and Human and Culture unit. Every relevant unit and department that processes personal data, especially the Information Technologies and Human and Culture unit, is personally responsible for the implementation of this Policy. Legal Counsel is a source of advice, consultant and guide in the execution of the processes.

6. REVIEW

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

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

In case of conflict between the legislation in force regarding the protection and processing of personal data and the Personal Data Retention and Destruction Policy, the Company accepts that the legislation in force will be implemented.

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