PERSONAL DATA STORAGE AND DESTRUCTION POLICY

TABLE OF CONTENTS

1. INTRODUCTION

Pursuant to the Constitution of the Republic of Türkiye, every person has the right to request for protection of personal data about them. In terms of protection of personal data which forms a Constitutional Right, Enerjisa pays due care and attention to protect the personal data of its employees, employee candidates, interns, company shareholders, company officials, visitors, as well as employees, shareholders, and officials of the organizations that it cooperates with and third parties as governed with 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 is comprised of the processes regarding the storage and destruction of personal data pertaining to our employees, employee candidates, interns, company shareholders, company officials, our visitors, as well as employees, shareholders and officials of the companies we cooperate with and third parties as governed by this Policy.

The absence of a special complementary law setting forth the fundamental principles despite the presence of disorganized provisions on protection of personal data in our legislation has been considered as a material deficiency in our country for a long time. This deficiency was eliminated with the Personal Data Protection Law no. 6698 which entered into effect upon its publication in the Official Gazette on 7 April 2016 (the "PDP Law" or the "Law"); setting forth the provisions governing the obligations of both public and private sector institutions to ensure the confidentiality and security of personal data and the use of such date in line with their intended purposes.

In this context, Enerjisa takes necessary organizational and technical measures to protect personal data processed pursuant to the said Law. This Policy will include detailed explanations about the following fundamental principles adopted by Enerjisa in terms of processing of personal data:

- Storage of personal data for the period as stipulated in the relevant legislation or required for their processing purposes;
- Taking necessary measures regarding storage and preservation of personal data;
- Ensuring the compliance of third parties with these principles as well in case of transfer of personal data to third parties in line with the requirements of their processing purposes;
- Compliance with the law and the rules of integrity;
- Ensuring that personal data are accurate and up-to-date, where necessary;
- Processing for specified, explicit and legitimate purposes;
- Relevance, limitation to and proportionality with the data processing purposes.

1.1. PURPOSE OF THE POLICY

The main purpose of this Policy is to set forth the principal methods for erasure, destruction or anonymization of personal data, processed pursuant to the provisions of the PDP Law and other applicable legislation, in accordance with the provisions of the By-Law on Erasure, Destruction or

Anonymization of Personal Data (the "By-Law") if the reasons requiring their processing cease to exist. Thus, the main objective is to make sure that relevant procedures are conducted systematically within Enerjisa and to ensure transparency of the implemented procedures for our employees, employee candidates, interns, company shareholders, company officials, visitors, the employees of the companies we cooperate with and all persons and entities whose personal data are processed by our company, by providing explanations about the adopted systems.

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

1.2. SCOPE OF THE POLICY

This Policy has been prepared for our employees, employee candidates, interns, company shareholders, company officials, visitors, the employees of the companies we cooperate with, and all third parties whose personal data are processed by our company; and shall apply to all these persons as listed herein.

This Policy shall apply to the aforementioned persons, in cases where our Company processes the personal data of these data subjects, in part or in whole, whether by automated means or non-automated means that are a part of any data recording system. This Policy shall not apply if the relevant data does not fall within the scope of "Personal Data" as specified below or if the personal data processing activity conducted by our Company is not conducted through the aforementioned means, in which case it will be impossible to mention about any personal data processing described under the PDP Law.

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

For definitions not provided herein, please refer to the definitions provided in the Law, the By-Law and the relevant guidelines published by the Personal Data Protection Board.

Explicit Consent	**:**	Freely given, specific and informed consent related to a specific matter.
Anonymization	**:**	Irreversible modification of persona data so that it loses its nature of personal data. For example, rendering personal data impossible to link with a natural person through the techniques such as masking, aggregation, data perturbation, etc.
Employee Candidate	**:**	Natural persons that have applied for a job to our Company through any means and made their CVs and related data available for review by our Company.
Group Company	**:**	means Enerjisa Üretim Santralleri A.Ş. and its subsidiaries.
Shareholders	**:**	H.Ö. Sabancı Holding A.Ş. and DD TURKEY HOLDİNGS S.A.R.L. (hereinafter referred to as "E.ON")
Disposal	**:**	Erasure, destruction or anonymization of personal data.

Employees, Shareholders and Officials of the Companies we cooperate with	**:**	Natural persons employed in and working for the companies having any kind of business relationship with our Company (including, without limitation, business partner, supplier, etc., including also the shareholders and officials of these companies.
Blackening	**:**	The processes such as scratching out, painting and blurring all of the personal data in a way so that it becomes impossible to link them with an identified or identifiable natural person.
Personal Data	**:**	Any information relating to an identified or identifiable natural person. Therefore, the processing of data concerning legal-person entities is not covered by the Law. For example; name and surname, Turkish ID No., e-mail, address, date of birth, credit card number, etc.
Processing of Personal Data	**:**	Any operation or set of operations performed on personal data, in part or in whole, whether by automated means, or non-automated means that are a part of any data recording system, such as collection, recording, storage, preservation, alteration, revision, disclosure, transfer, acquisition, retrieval, categorization or prevention of the use of such data.
Personal Data Protection Board	**:**	The board authorized to manage and execute the PDP Law.
Personal Data Subject/Related Person	**:**	The natural person whose personal data is processed.
Masking	**:**	means the processes such as erasing, scratching out, painting or marking with asterisks certain fields of personal data in a way that it becomes impossible to link them with any identified or identifiable natural person.
Special Categories of Personal Data	**:**	Data relating to race, ethnic origin, political view, philosophical belief, religion, sect or other beliefs, clothing/dressing, association, foundation or trade-union membership, health, sexual life, criminal convictions and offences and related security measures as well as biometric and genetic data constitute special categories of personal data.
Company Official	:	Natural-person board members and other authorized executives of our Company
Third Party	:	Third-party natural persons (e.g. family members and relatives) associated with the aforementioned parties, for the purpose of ensuring security of business transactions between our Company and the said parties or protecting the rights of or affording interests for such persons.
Data Processor	**:**	The natural or legal person processing personal data on behalf of the data controller based on the authorization granted by the data controller. For example, cloud computing company storing employee data, call-center company making calls according to scripts, *etc*.
Data Recording Medium	**:**	Any media containing personal data processed whether by automated means, in part or in whole, or non-automated means that are a part of any data recording system.
Data Recording System	**:**	The recording system through which personal data are structured and processed according to specific criteria.

Data Controller	**:** Data controller is the person determining the purposes and means of processing of personal data and managing the system where data are
	filed systematically (data recording system).
Visitor	: Natural persons entering the physical premises of our Company or visiting our websites for various purposes.

1.4. IMPLEMENTATION OF THE POLICY AND THE RELEVANT LEGISLATION

Relevant legal regulations that are in force with respect to the storage and destruction of personal data shall primarily apply. Our Company acknowledges that applicable legislation shall prevail in case of any discrepancy between applicable legislation in force and the Policy.

The Policy has been established by embodying and arranging 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. PERSONAL DATA STORAGE PERIODS

If stipulated in the relevant laws and regulations, Enerjisa stores personal data for the periods specified in such legislation.

If there is no period stipulated for storage of personal data in the relevant legislation, personal data are processed for the necessary period required for processing of relevant data pursuant to our Company's practices in connection with the services offered by our Company while processing such data, the requests of the relevant Authorities/Agencies due to operation in a regulated industry and relevant business practices; and then, they are erased and destroyed or anonymized. Further information on this matter is provided in Section 5 of this Policy.

If the processing purpose of personal data has ceased to exist and the storage periods stipulated by applicable legislation and specified by the company have expired; personal data may be stored only for the purpose of constituting evidence in case of potential legal disputes or claiming relevant rights or establishing the defence related to the personal data. In determination of the periods mentioned herein, the storage periods are determined on the basis of limitation periods for claiming the relevant rights and the examples in the requests previously raised against our Company on the same matters despite the expiration of limitation periods. In this case, stored personal data cannot be accessed for any other purposes and the relevant personal data are accessed only when they are to be used in any relevant legal dispute. Upon expiration of the period mentioned herein, personal data are erased, destroyed or anonymized.

If personal data processed by our Company have been transferred to third parties specified in Section 4, such data must also be erased, destroyed or anonymized by the recipient third parties to whom they have been transferred upon expiration of the processing purposes for the relevant

personal data. Enerjisa takes necessary measures to this effect, and provisions about these measures are incorporated into agreements. Notices are sent to the relevant third parties and their commitment regarding the completion of the procedure is obtained within the scope of the measures taken as such.

2.2. RECORDING MEDIA

Our Company stores all personal data subject to data processing activities within the scope of the Law in/on the following media containing personal data processed, whether by automated means in part or in whole, or non-automated means that are a part of any data recording system.

Electronic Media: In the Company-owned server and network systems, in the applications and cloud systems developed by the company itself or outsourced as a service
Servers (Databases, E-mail, e-folders of Business Units)
Company-owned mobile devices (mobile phones, computers)
Camera recording areas
Websites with their infrastructures created by contracted companies

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

3. CONDITIONS FOR STORAGE, ERASURE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

3.1. LEGAL DISCLOSURE ABOUT THE OBLIGATION FOR STORAGE, ERASURE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Personal data are erased, destroyed or anonymized based on the Company's own decision or data subject's request if the reasons requiring their processing cease to exist even though they have been processed pursuant to applicable legal provisions as set forth in article 138 of the Turkish Criminal Code and article 7 of the PDP Law. In this context, our Company fulfils its relevant obligation with the methods described in this section.

If a request is received to this effect from the personal data subject, a review is made according to the relevant Enerjisa policy; and the most suitable method is selected from and among erasure, destruction or anonymization procedures, then, the relevant procedure is performed and the personal data subject is informed in relation thereto.

3.2. TECHNIQUES FOR ERASURE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Personal data erasure, destruction or anonymization procedures are executed in compliance with the By-Law and the techniques in the relevant guidelines issued by the Personal Data Protection Board.

3.2.1. TECHNIQUES FOR ERASURE AND DESTRUCTION OF PERSONAL DATA

Our Company may erase or destroy personal data based on its own decision or upon the data subject's request if the reasons requiring their processing cease to exist even though the relevant data have been processed in accordance with applicable legal provisions. The erasure or destruction methods that are most commonly used by our Company are listed below:

(i) Physical Destruction

Personal data can also be processed by non-automated means that are a part of any data recording system. When such data are erased/destroyed, the system of physical destruction is applied in a way that renders them impossible to be used later.

(ii) Secure Deletion from the Software

When erasing/destroying the data processed by automated means in part or in whole and stored in digital media, methods to erase the data from the relevant software in an irretrievable way are used.

(iii) Secure Deletion by a Specialist

Enerjisa may, in some specific cases, employ a specialist to delete/erase personal data on its behalf. In such cases, personal data are securely erased/destroyed by a person specialized in this field in an irrecoverable way.

3.2.2. 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 by matching them with other data. Our Company may anonymize personal data when the reasons requiring the processing of personal data that are lawfully processed cease to exist.

Pursuant to article 28 of the PDP Law; anonymized personal data can be processed for purposes such as research, planning and statistics. Such processing procedures are excluded from the scope of the PDP Law; and the explicit consent of the data subject shall not be sought.

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

(i) Masking

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

(ii) Aggregation

Multiple data are aggregated and personal data are rendered impossible to be linked with any person by using data aggregation method.

(iii) Data Derivation

With data derivation method, a more general content is created from the content of the personal data, and thus, personal data are rendered impossible to be linked with any person.

(iv) Data Shuffling

With data shuffling method, values in the personal data set are shuffled and the link between the values and persons is broken.

3.3. TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE SECURE STORAGE OF, AND TO PREVENT UNLAWFUL PROCESSING OF AND ACCESS TO PERSONAL DATA

	Measures
1	It is planned to perform penetration testing following all major changes, in addition to the penetration tests performed once a year for all exterior-facing systems.
2	Alarms have been defined for data movements to Internet or portable media, involving critical data identified on the DLP system.
3	It is ensured that received DLP alarms are analysed by relevant responsible persons and necessary actions are taken.
4	Personal data are hidden on reports and authorization efforts are made.
5	Data classification software has been installed on all employee computers.
6	A data classification system has been established to prevent the removal of any data from the Company and it is tried to prevent data leaks through the channels such as mail, USB, printer, etc.
7	Non-disclosure commitments are obtained. It is ensured that information security commitment letters are signed by the companies we cooperate with/outsource services from; and audits regarding information security and lawful processing of personal data are planned with reference to our right of audit.
8	Efforts are made to develop systems for recording the approvals obtained for the processing of personal data, transfer details, etc.
9	The Company's common area authorizations are reviewed.
10	Network security and application security are ensured.
11	Closed system network is used in the 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	The security of personal data stored on the cloud is ensured.
15	There are disciplinary regulations in place, containing data security provisions for employees.
16	Training and awareness-raising activities regarding data security are conducted for employees at certain intervals.
17	An authorization matrix has been established for employees.
18	Access logs are kept regularly.
19	Corporate policies have been prepared and started to be implemented on the issues such as access, information security, use, storage and destruction.
20	The relevant authorizations are revoked for the employees whose positions are changed or who leave their jobs.
21	Current anti-virus systems are used.
22	Firewalls are used.
23	Signed agreements incorporate data security provisions.
24	Personal data security policies and procedures have been established.
25	Personal data security issues are reported swiftly.
26	Personal data security is monitored.
27	Necessary security measures are taken for entries and exits to/from physical locations containing personal data.

28	Physical locations containing personal data are secured against external risks (fire, flood, etc.).
29	The security of media containing personal data is ensured.
30	Personal data are reduced as much as possible.
31	Personal data are backed up and the security of personal data backups is also ensured.
32	User account management and authorization control system are implemented and also monitored.
33	Internal periodic and/or random audits are conducted and outsourced.
34	Log records are kept in a way preventing any user intervention.
35	Current risks and threats have been identified.
36	If special categories of personal data are to be sent via electronic mail; they are absolutely sent encrypted and via KEP or corporate mail account.
37	Secure encryption / cryptographic keys are used for special categories of personal data and they are administered by different units.
38	Attack detection and prevention systems are used.
39	Penetration tests are conducted.
40	Cyber security measures have been taken; and their implementation is constantly monitored.
41	Encryption is made.
42	Special categories of personal data transferred on portable drives, CDs or DVDs are transferred with encryption.
43	Service providers processing data are audited at certain intervals in terms of data security.
44	The awareness of service providers processing data is raised in terms of data security.
45	Data loss prevention software is used.
46	Locked archive rooms are provided, thus trying to prevent unauthorized third persons from accessing personal data on physical documents.
47	Physical documents stored in the archive are categorized.
48	Documents obtained together with agreements, applications, etc. have been limited pursuant to the principle of proportionality.

3.4. TECHNICAL AND ORGANIZATIONAL MEASURES FOR LAWFUL DESTRUCTION OF PERSONAL DATA

	Measures
1	Personal data covered by the Policy are identified on all systems.
2	Data to be deleted are notified and it is ensured that due decisions are taken with the controllers of relevant data.
3	Destruction measures specified in this Policy are applied to the data identified in line with the decisions taken.

4. PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

4.1. TABLE SHOWING PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

Personal data storage and destruction periods are shown in the table below on an individual category basis and by indicating the longest periods.

Personal Data Categorization	**Storage and Destruction Period**
Identity Data	14 Years after the end of employment
Contact Data	15 Years after the end of employment
Location Data	10 Years after the end of employment
Personnel Data	15 Years after the end of employment
Legal Action	10 Years
Physical Location Security	10 Years
Process Security	10 Years
Finance	10 Years
Professional Experience	15 Years after the end of employment
Audio-Visual Records	15 Years after the end of employment
Philosophical Belief, Religion, Sect and Other Beliefs	15 Years after the end of employment
Association Membership	6 Months
Foundation Membership	6 Months
Trade-Union Membership	6 Months
Health Data	15 Years after the end of employment
Criminal Convictions and Security Measures	15 Years after the end of employment
Other Data – Vehicle details	10 Years after the end of employment

Pursuant to the relevant process of the People & Culture department, personal data of employee candidates such as CVs, etc. collected and processed during job application process are stored for 6 months; upon expiration of this period, such data are destroyed in accordance with periodic destruction processes.

In case that the data subject applies to our Company and requests for destruction of their personal data, our Company takes the following actions:

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

(i) our Company concludes the data subject's request within thirty days at the latest and informs the data subject; and

(ii) if the personal data that is subject to the request has been transferred to third parties, our Company notifies this situation to the relevant third party and ensures that necessary actions are taken by the third party.

(b) If all of the conditions for processing of personal data have not disappeared, our Company may reject the data subject's request by explaining the reasons of rejection pursuant to the third paragraph of article 13 of the Law and notifies the response of rejection to the data subject in writing or electronically within thirty days at the latest.

4.2. INFORMATION ON PERIODIC DESTRUCTION PERIODS

Periodic destruction shall be performed every 6 (six) months starting from the effective date of the By-Law and the logs of the actions taken shall be stored for a period of 3 (three) years.

5. ROLES AND RESPONSIBILITIES

All bodies and departments of the Company are responsible to observe compliance with the Personal Data Storage and Destruction Policy and to cooperate with the Personal Data Protection Committee. The processes regarding the storage and destruction of personal data shall be conducted by the Information Technologies and People & Culture departments. Every relevant unit and department processing personal data, including, particularly, the Information Technologies and People & Culture units, are directly responsible for implementation of this Policy. The Legal Consultancy department serves as a consultant, guide and source of recommendations in the execution of processes.

6. REVIEW

This Policy Document enters into effect upon its approval by the Company's Executive Vice President for People and Culture. Amendments to be made in this Policy and enforcement of such amendments are subject to the approval of the Company's Executive Vice President for People and Culture.

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

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

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

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