NATUREL YENİLENEBİLİR ENERJİ TİCARET ANONİM ŞİRKETİ

LPPD

PERSONAL DATA STORAGE and DESTRUCTION POLICY

Table of Contents

1. INTRODUCTION

1.1 Objective:

Personal Data Storage and Destruction Policy ("Policy"), has been prepared in order to determine the procedures and principles regarding the works and transactions related to the storage and destruction activities carried out by the NATUREL YENİLENEBİLİR ENERJİ TİC AŞ. (“Company”). In addition, the objective of this Policy is to determine the rules to be applied for the fulfillment of the obligations related to the storage and destruction of personal data and other obligations specified in accordance with articles 5 and 6 of the Regulation (Regulation) on the Deletion, Destruction or Anonymization of Personal Data, which was issued based on the Law (Law) on the Protection of Personal Data No. 6698 and published in the Official Gazette No. 30224 and dated 28.10.2017.

The Company has prioritized the processing of personal data of employees, employee relatives, employee candidates, trainers, customers, potential customers, service providers, visitors ("Related Person") and has ensured that relevant persons exercise their rights effectively in accordance with the Constitution of the Republic of Turkey, international agreements, the Law on the Protection of Personal Data No. 6698 (“Law”) and other relevant legislation.

The processes related to the storage and destruction of personal data are carried out in accordance with this policy prepared by the Company in this direction.

1.2 Scope

Personal data belonging to the relevant persons are within the scope of this Policy and this Policy is applied in all recording media where the personal data owned or managed by the Company are processed and in activities for the processing of personal data.

1.3 Abbreviations and Definitions

Company: NATUREL YENİLENEBİLİR ENERJİ TİC AŞ.

Policy : Personal Data Storage and Destruction Policy

VERBİS : Data Controllers Registry Information System

Law : Law on the Protection of Personal Data No. 6698

Personal Data : All kinds of information related to the identified or identifiable real person.

Personal Data of Special Nature: Data related to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, clothing, membership to associations, foundations or trade-unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Data Controller : Real or legal person responsible for the establishment and management of the data recording system, which determines the purposes and means of processing personal data.

Destruction : Deletion, destruction or anonymization of personal data.

Recording Media : All kinds of media where personal data are processed completely or partially automatically or in non-automatic ways provided that they are part of any data recording system.

Board : Personal Data Protection Board.

Data Recording System : refers to the recording system in which personal data are processed by structuring according to certain criteria.

Personal Data Processing Inventory: Inventory created by data controllers by associating the personal data processing activities they carry out depending on their business processes with the purposes of processing personal data, data category, transferred recipient group and data subject group and it is detailed by explaining the maximum period required for the purposes for which personal data is processed, the personal data envisaged to be transferred to foreign countries, and the measures taken regarding data security.

Related Person : The real person whose personal data is processed,

Data Processor : Real or legal person who processes personal data on his/her behalf based on the authority given by the data controller,

Periodic destruction: In the event that all the conditions of processing of personal data in the law disappear, the process of deletion, destruction or anonymization of personal data to be carried out ex officio and at repeated intervals specified in the personal data storage and destruction policy,

Explicit Consent: Expresses the consent that is based on information, related to a certain subject, and that is expressed with free will.

2. RESPONSIBILITIES AND DUTY DISTRIBUTIONS

All employees of the company support the responsible teams in taking technical and administrative measures to ensure data security in all environments where personal data is processed within the scope of the Policy.

The distribution of the titles, units and job descriptions of the personnel involved in the storage and destruction processes of personal data is given inTable 1.

Table 1: Distribution of duties for personal data storage and destruction processes

TITLE	UNIT	DUTY
General Manager	Company management	• Responsible for the employees to act in accordance with the policy.
Human Resources Manager	Human Resources	• Responsible forthe preparation, follow-up, and updating of the policy • Management of the process of destruction of personal data in the physical environment
Information Technologies	Information Technologies	• Responsible for taking the technical measures requiredin the implementation of the policy. • Management of the process of destruction of personal data in the electronic environment
Human Resources Team, Legal Affairs Team, Information Technologies Team,	Other Units	• Responsible for the execution of the Policy in accordance with the duties.

In order to manage this policy and other policies, procedures and forms related to the ISO 27001 Information Security Management System within the company, an "Information Security Committee" has been established in accordance with the decision of the senior management of the company. The duties of this committee are defined in the ISO 27001 Information Security Management System.

3. RECORDING MEDIA

Personal data of the relevant persons are securely stored by the Company in the media listed in the table below, taking into account the provisions of the LPPD, relevant legislation and international data security.

Table 2: Personal data storage media

Electronic Media	Physical Environments

• Servers
  • Domain,
  • Backup system,
  • E-Mail system,
  • Database,
  • Web application,
  • File sharing
• Software
  • SAP systems,
  • Accounting software,
  • CRM Software
  • ERP Software
• Information security systems
  • Firewall,
  • Detection and prevention of attack,
  • Log file,
  • antivirus
• Personal computers
  • Desktop,
  • On the knee,
• Mobile devices
  • Phone:
  • Tablet,
• Optical discs
  • CD, DVD
  • Cassette
	• Unit Cabinets
	• Manual data recording systems (survey forms, visitor logbook)
	• Printed, printed, visual media
	• Archive

• Removable memories
  • USB memory,
  • Memory Card
  • External Disk
• Printer, scanner, copier	

4. EXPLANATIONS ON STORAGE AND DESTRUCTION

Personal data of the relevant persons are stored and destroyed by the Company in accordance with the law. In this context, detailed explanations on storage and destruction are given below.

The concept of processing personal data is defined in Article 3 of the Law,

The personal data processed in Article 4 of the Law should;

- comply with the law and the rules of honesty,
- be accurate and up-to-date when necessary,
- be processed for specific, explicit and legitimate purposes,
- be connected, limited and moderate with the purpose for which they are processed,
- comply with the principles of preservation for the period stipulated in the relevant legislation or required for the purpose for which they are processed.

The conditions for processing personal data are listed in Articles 5 and 6 of the Law.

Accordingly, the personal data processed within the framework of the Company's activities are stored for an appropriate period in accordance with the provisions of the LPPD and other relevant legislation.

4.1 Legal Reasons Requiring Storage

Reasons for storing personal data belonging to the relevant persons;

- Sustainability of commercial activities,
- Fulfillment of legal obligations,
- Planning and performance of employee rights and benefits and
- In order to manage customer relations
- Storing personal data due to the fact that it is directly related to the establishment and performance of contracts,
- It is obligatory to keep personal data for the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of the individuals,
- Storing personal data for the purpose of establishing, using or protecting a right,
- Clearly stipulating the storage of personal data in the legislation,
- Obtaining the explicit consent of the persons concerned in terms of storage activities requiring the explicit consent of the persons concerned

it is safely stored in physical or electronic environments within the limits specified in the LPPD and other relevant legislation.

4.2 Processing Purposes Requiring Storage

The Company stores the personal data it processes within the framework of its activities for the following purposes.

- To carry out human resources processes.
- To ensure corporate communication.
- To ensure the security of the institution,
- To be able to carry out statistical studies.
- To be able to perform the works and transactions as a result of the signed contracts and protocols.
- Within the scope of verbis, to determine the preferences and needs of employees, data controllers, contact persons, data controller representatives and data processors, to organize the services provided accordingly and to update them if necessary.
- To ensure the fulfillment of legal obligations as required or required by legal regulations.
- To liaise with real / legal persons in business relationship with the institution.
- To make legal reports.
- To manage call center processes.
- Obligation to prove as evidence in legal disputes that may arise in the future

4.3 Reasons for Destruction

Personal data;

- Amendment or relevance of the provisions of the relevant legislation that constitute the basis for the processing of personal data,
- The disappearance of the purpose that requires the processing or storage of personal data,
- In cases where the processing of personal data takes place only with reference to the explicit consent condition, the person concerned withdraws his/her explicit consent,
- Pursuant to Article 11 of the Law, the data controller accepts the application for the deletion and destruction of the personal data of the person concerned within the framework of his/her rights,
- In the event that the data data controller rejects the application made to him/her with the request of deletion, destruction or anonymization of his/her personal data by the related person and finds his/her answer insufficient or does not respond within the period stipulated in the Law; if he/she makes a complaint to the Board and this request is approved by the Board,
- The maximum period for storing personal data has passed and there is no condition to justify storing personal data for a longer period,

The data is deleted, destroyed or is deleted, destroyed or anonymized by the data controller upon the request of the related person.

5.TECHNICAL AND ADMINISTRATIVE MEASURES

Technical and administrative measures are taken by the Company within the framework of the principles in Article 12 of the LPPD for the safe storage of personal data, the prevention of unlawful processing and access to personal data and the destruction of personal data in accordance with the law.

5.1 Administrative Measures

Administrative measures taken by the company:

- Confidentiality clauses have been added to the employment contracts of the employees regarding data security.
- An HR disciplinary procedure has been prepared for employees who do not comply with security policies and procedures.
- Before starting to process personal data, the Company fulfills the obligation to inform the related persons.
- Personal data processing inventory has been prepared.

- Periodic audits are made within the institution. Confidentiality and security weaknesses arising as a result of the audits are eliminated.
- Information security trainings including the issues related to the LPPD are provided to the employees.
- It limits the internal access to the stored personal data to the personnel required to access the job description. In limiting access, whether the data is of special nature and its importance is also taken into account.

5.2 Technical Measures

Technical measures taken by the company:

- Penetration tests reveal risks, threats and weaknesses for information systems and take necessary measures.
- As a result of real-time analyzes made with information security incident management, risks and threats that will affect the continuity of information systems are constantly monitored.
- Access to information systems and authorization of users are made through security policies over the corporate active directory with the access and authorization matrix.
- Necessary measures are taken for the physical security of the information systems equipment, software and data of the institution.
- In order to ensure the security of information systems against environmental threats, hardware (access control system that allows only authorized personnel to enter the system room, 24/7 monitoring system, ensuring the physical security of the edge switches that make up the local area network, fire extinguishing system, air conditioning system, etc.) and software (firewalls, attack prevention systems, network access control, systems that prevent harmful software, etc.) measures are taken.
- Risks for preventing unlawful processing of personal data are determined, technical measures are taken in accordance with these risks and technical controls are made for the measures taken.
- Access procedures are created within the institution and reporting and analysis studies are carried out regarding access to personal data.
- Access to storage areas where personal data is stored is recorded and inappropriate access or access attempts are kept under control.
- The institution takes the necessary measures to ensure that the deleted personal data are not accessible and reusable for the relevant users.
- In the event that personal data are obtained unlawfully by others, an appropriate system and infrastructure has been established by the Institution to notify this situation to the relevant person and the Board.
- By following the security vulnerabilities, appropriate security patches are installed and information systems are kept up-to-date.
- Strong passwords are used in electronic environments where personal data are processed.
- Secure logging systems are used in electronic environments where personal data are processed.
- Data backup programs are used to store personal data securely.
- Access to personal data stored in electronic or non-electronic media is restricted according to access principles.
- It is encrypted using secure protocol (HTTPS) in accessing the corporate website.

- A separate policy has been determined for the security of sensitive personal data.
- Trainings have been given on special quality personal data security for employees involved in special quality personal data processing processes, confidentiality agreements have been made, and the authorizations of the users who have access to the data have been defined.
- Electronic environments where sensitive personal data is processed, stored and/or accessed are kept by using cryptographic methods, cryptographic keys are kept in secure environments, all transaction records are logged, security updates of the environments are constantly monitored, necessary security tests are regularly performed/made, test results are recorded,
- Sufficient security measures are taken in the physical environments where sensitive personal data is processed, stored and/or accessed, and unauthorized entries and exits are prevented by ensuring physical security.
- If sensitive personal data needs to be transferred via e-mail, it is transferred encrypted via corporate e-mail address or using Kep account. If it needs to be transferred through media such as portable memory, CD, DVD, it is encrypted by cryptographic methods and the cryptographic key is kept in different media. If transfer is performed between servers in different physical environments, data transfer is performed between servers by setting up a VPN or by sFTP method. If it is necessary to transfer the document through paper media, necessary measures are taken against risks such as theft, loss or unauthorized viewing of the document and the document is sent in a "confidential" format.

6. TECHNIQUES FOR DESTROYING PERSONAL DATA

At the end of the period stipulated in the relevant legislation or the storage period required for the purpose for which they are processed, the personal data are destroyed by the Company with the following techniquesin accordance with the provisions of the relevant legislation upon the application of you or the person concerned.

6.1 Deletion of Personal Data

Personal data are deleted by the methods given in Table-3.

Table 3: Deletion of Personal Data

Data Record Media	Description
Personal Data on Servers	• For those whose period of time requiring the storage of personal data on the servers has expired; • The system administrator removes the access authorization of the relevant users on the directory where the file or file is located and deletes it.

Personal Data in Databases	• Those who have expired from the personal data in the databases are made inaccessible and unusable in any way for other employees (related users) except the database administrator. • Deleting related lines in databases with database commands
Personal Data in the Physical Environment	• For those whose period of time required to be kept from personal data kept in physical environment has expired; • It is made inaccessible and unavailable to other employees in any way except for the unit manager responsible for the document archive. Also, blackout process is applied by scratching/painting/wiping in a way that cannot be read.
On Portable Media Personal Data Found	• Expired ones that require storage from personal data stored in flash-based storage environments • Deletion of data in flash environment by the system administrator using appropriate software
Personal Data in the Cloud System	• For those who have expired the period of time that requires the storage of personal data in the cloud system • Deleting the relevant data in the cloud system by giving the delete command

6.2 Destruction of Personal Data

Personal data are destroyed by the Company by the methods given inTable-4 .

Table 4: Destruction of Personal Data

Data Record Media	Description
Physical Environment Personal Data	• For those who have expired from the personal data in the paper environment, the paper shredder is irreversibly destroyed in the devices.
In Optical / Magnetic Media Personal Data Included	• The process of physical destruction such as melting, burning or pulverization of those whose period of time has expired, which requires to be stored from personal data in optical media and magnetic media, is applied. In addition, the magnetic media is passed through a special device and the data on it is made unreadable by exposing it to a high magnetic field.

6.3 Anonymization of Personal Data

Anonymization of personal data is the process of making personal data in no way associated with an identified or identifiable real person, even if it is matched with other data.

In order for the personal data to be anonymized, it is necessary to make the personal data unassociable with an identified or identifiable real person even by using appropriate techniques in terms of the recording environment and the relevant field of activity, such as the return of the personal data by the data controller or third parties and/or the matching of the data with other data.

Pursuant to Article 28of the LPPD, if personal data are processed for purposes such as research, planning and statistics by anonymizing them with official statistics, this situation will remain outside the scope of the Law and explicit consent will not be required.

7. STORAGE AND DESTRUCTION PERIODS

Regarding the personal data processed by the Company within the scope of its activities;

- ➢ Personal data-based storage periods for all personal data within the scope of activities carried out in connection with processes are included in the Personal Data Processing Inventory;
- ➢ Storage periods on the basis of data categories are recorded in VERBIS.

The following criteria are used in determining the storage and destruction periods:

- If a period of time is stipulated in the legislation regarding the storage of the personal data in question, this period is complied with.
- In the event that the period stipulated in the legislation regarding the storage of the said personal data expires or no period is stipulated in the relevant legislation regarding the storage of the said data, respectively;
    - o Personal data are classified as personal data and sensitive personal data based on the definition in Article 6 of the LPPD. All personal data that are found to be of special nature are destroyed. The method to be applied in the destruction of the said data is determined according to the nature of the data and the importance of its storage for the Company.
    - o For example, it is questioned whether the storage of the data complies with the principles specified in Article 4 of the LPPD; whether the Company has a legitimate purpose in

storing the data. The data, which is determined to be in violation of the principles in Article 4 of the LPPD, are deleted, destroyed or anonymized.

- It is determined which of the exceptions stipulated in Articles 5 and 6 of the LPPD can be evaluated within the scope of data storage. Within the framework of the exceptions determined, reasonable periods for storing the data are determined. If the said periods expire, the data is deleted, destroyed or anonymized.
- For personal data whose storage periods have expired, the process of ex officio deletion, destruction or anonymization is carried out by Information Technologies.
- Pursuant to Article 11 of the Regulation, the Company has determined the periodic destruction period as 6 months. Accordingly, periodic destruction process is performed in June and December each year in the Agency.

Process	Storage Time	Destruction time
Planning and Execution of Corporate Communication Activities, 10 years following the termination of the business relationship		Within 180 days of the end of the storage period
Preparation of Contracts 10 years following the Termination OF the contract		Within 180 days of the end of the storage period
Responding to court/executive information requests related to personnel	10 years following the termination of the business relationship	Within 180 days of the end of the storage period
Occupational health and safety practices	10 years following the termination of the business relationship	Within 180 days of the end of the storage period
Execution of Human Resources Processes	10 years following the end of the activity	Within 180 days of the end of the storage period
Log Record Tracking Systems	2 years	Within 180 days of the end of the storage period
Execution of Hardware and Software Access Processes	2 years	Within 180 days of the end of the storage period
Registration of Visitors and Meeting Participants	15 days following the end of the event	Within 180 days of the end of the storage period
Camera Records	15 days	Within 180 days of the end of the storage period

If the purpose of the Company to use the relevant personal data has not expired, if the storage period stipulated for the relevant personal data in accordance with the relevant legislation is longer than the periods in the table, or if the limitation period of the lawsuit on the relevant subject requires the personal data to be stored longer than the periods in the table, the periods in the table above may not be applied. In this case, the purpose of use, special legislation or lawsuit, whichever expires later, will be applied.

8. PUBLISHING, STORING and UPDATING THE POLICY

The Company ensures that the principles set forth by this policy are applied within the company. This policy on the protection of personal data is also linked to the basic policies, procedures and forms of the company in the field of ISO 27001 Information Security Management System, and compatibility is ensured between the processes that the company operates with different policy principles for similar purposes.

The policy is stored in two different media as wet signed (printed paper) and electronic media. Printed paper copy is also kept in the file of the Human Resources Directorate.

The policy is reviewed when needed or at least once a year and the necessary sections are updated.