ENERGO PRO TURKEY HOLDİNG A.Ş.
PERSONAL DATA PROTECTION AND DESTRUCTION POLICY

I. INTRODUCTION AND PURPOSE OF THE POLICY

This Personal Data Storage and Destruction Policy ("**Policy**") is prepared by Energo Pro Turkey Holding A.Ş ("**Company**") Prepared as data controller with the purpose of fulfilling our obligations and determining the maximum storage period required for the purpose of processing personal data in accordance with Law No. 6698 on Protection of Personal Data ("**LPPD**" or "**Law**") and the Regulation on Erasure, Destruction or Anonymization of Personal Data ("**Regulation**") which includes the second regulation of Law and using it as a basis for Erasure, destruction and anonymization operations and informing the relevant persons about these operations.

II. DEFINITIONS

Abbreviation	Description
Customer	The real or legal person to whom personal data is transferred by the data controller.
Explicit Consent	Consent about a specific subject based on information and expressed in free will.
Related User	The persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, except the person or unit responsible for the technical storage, protection and backup of the data.
Destruction	Erasure, destruction or anonymization of personal data.
Law/LPPD	Law on Protection of Personal Data of 24/3/2016 and No. 6698
Recording Medium	Any media in which personal data are processed, which are fully or partially in automated ways or non-automated ways provided that being part of any data recording system.
Personal Data	Any information related to a real person who is identified or identifiable.
Personal Data Processing Inventory	The inventory that data controllers detail by explaining the personal data processing activities: the purposes of processing personal data and the legal reason, the data category, the transferred recipient group and the maximum retention period necessary for the purposes for which the personal data are processed, the personal data intended to be transferred to foreign countries and the measures taken regarding data security, that they carry out depending on their business processes.
Processing of Personal Data	All kinds of processes performed on personal data including obtaining them in fully or partially automatic ways or non-automatic ways provided that is i apart of a data recording system, recording, storing, keeping, changing, re-arranging, disclosure, transmission, acquisition, making available, classification or prevention of use.
Anonymization of Personal Data	Making personal data not to be associated with any identified or identifiable real person in any way, even when paired with other data.

Erasure of Personal Data	Erasure of personal data is the process of making personal data inaccessible and unusable for the relevant users in any way.
Destruction of Personal Data	The process of rendering personal data inaccessible, unrecoverable and unusable by anyone in any way.
Board	Personal Data Protection Board
Sensitive Personal Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership of associations, foundations or trade-unions, information relating to health, sexual life, convictions and security measures, and the biometric and genetic data of individuals.
Periodic Destruction	In the event that all the processing conditions of personal data in the Law disappear, the process of erasure, destruction, or anonymization of the personal data that will be carried out at regular intervals specified in the storage and destruction policy.
Data Subject/ Related Person	The real person whose personal data is processed.
Data Controller	Real or legal entity responsible for identifying the purposes and means of personal data processing, and installing and managing data recording system.
Regulation	Regulation on Erasure, Destruction or Anonymization of Personal Data published in the Official Gazette on October 28, 2017.

III. PRINCIPLES

Our company acts within the framework of the following principles in the storage and disposal of personal data:

1. In the erasure, destruction and anonymization of personal data, company acts in full compliance with the provisions of the relevant legislation and the decisions of the Board and this Policy.
2. All transactions regarding the Erasure, destruction and anonymization of personal data are carried out by Company and the said records are kept for at least 3 years, excluding other legal obligations.
3. In the event that all the conditions for processing personal data stipulated in Articles 5 and 6 of the Law are eliminated, personal data will be erased, destructed or anonymized by Company, either on its own motion or upon the request of the related person. If related person applies to Company regarding this subject;
   a. Submitted requests are concluded within 30 (thirty) days at the latest and the relevant person is informed,
   b. If the data which is subject to the request has been transferred to third parties, this will be reported to the third party to whom the data has been transferred and it will be ensured that the necessary actions are taken by the third parties.

A. REASONS REQUIRING STORAGE AND DESTRUCTION

1. The Reasons Requiring Storage

The personal data belonging to the data subjects are stored securely in physical or electronic environments within the framework of the limits specified in the LPPD and other relevant legislation within the scope of the following reasons.

a. Storage of personal data as it is directly related to the establishment and execution of contracts,
b. Storing personal data for the purpose of establishing, exercising or protecting a right,
c. Provided that personal data does not harm the fundamental rights and freedoms of individuals, it is mandatory to be stored for the legitimate interests of the Company,
d. Storing personal data with the purpose of fulfilling any legal obligation of the Company,
e. Storage of personal data is clearly foreseen in the legislation,
f. Having the explicit consent of the data subjects in terms of storage activities that require the explicit consent of data subjects.

2. Reasons for Erasing, Destruction or Making an Anonymizing

The personal data belonging to the data subjects are erased, destructed or anonymized by the Company ex officio or on demand in the following cases:

- **a.** Amendment or abolition of relevant legislative provisions that constitute the basis for the processing or storage of personal data,
- **b.** Abolition of the purpose that requires the processing or storage of personal data,
- **c.** Abolition of conditions that require the processing of personal data in Articles 5 and 6 of the Law.
- **d.** The relevant person's withdrawal of his/her consent in cases where the processing of personal data takes place only in accordance with the explicit consent condition,
- **e.** Acceptance of the application of the relevant person regarding the erasure, destruction or anonymization of his/her personal data within the framework of the rights of Article 11 of the Law in paragraphs (e) and (f), by data controller,
- **f.** In cases where the data controller rejects the application made by the relevant person on the request of erasure, destruction or anonymization of his/her personal data, his response is found inadequate, or does not respond within the period envisioned by the Law; making a complaint to the Board and approval of this request by the Board,
- **g.** Although the maximum time requiring personal data to be stored has expired, the non-existence of any conditions to justify storing personal data for longer.

B. PERIOD OF STORAGE AND DESTRUCTION

Company uses the following criteria in determining the storage and destruction periods of your personal data obtained in accordance with the provisions of LPPD and other relevant legislation:

1. If a period is envisioned in the legislation regarding the storage of the said personal data, this period is complied with. Following the expiration of the said period, the data is processed within the scope of the 2nd paragraph.
2. In the event that the period stipulated in the legislation regarding the storage of the relevant personal data has expired or no period stipulated in the relevant legislation regarding the storage of such data, respectively;
   - **a.** Personal data are classified as personal data and sensitive personal data based on the definition in Article 6 of LPPD. All personal data determined to be of sensitive nature are destructed. The method to be applied in the destruction of the data in question is determined according to the quality of data and importance level of storage of the data for the Company.
   - **b.** Compliance of data storage with the principles specified in Article 4 of the LPPD, for example; it is questioned whether Company has any legitimate purpose in the storage of data. Data whose storage is determined to have a possibility of constituting a contradiction against the principles set out in Article 4 of the Law shall be erased, destructed or anonymized.
   - **c.** It is determined which one of the exclusions envisioned in Article 5 and Article 6 of the Law will be taken as basis for the evaluation scope of the data storage. Reasonable periods are determined for data storage within the framework of the exceptions determined. If these periods expire, the data shall be erased, destructed or anonymized.
3. Personal data, the issues specified in Article 4 of the Policy, will be stored for the periods specified in the table below, will be anonymized or destructed at the end of the period:

Process	Storage Period	Destruction Period
Data stored under the Labor Law (e.g. performance records, etc.)	5 years after the end of the business relationship	within 180 days after the expiration of storage period
Data collected under occupational health and safety legislation (health reports, etc.)	15 years after the end of the business relationship	within 180 days after the expiration of storage period
Data held under SSI legislation.	10 years after the end of the business relationship	within 180 days after the expiration of storage period
Documents that can be used in a demand / case related to a work accident / occupational disease	10 years after the end of the business relationship	within 180 days after the expiration of storage period
Data collected in accordance with other relevant legislation	As long as the period envisioned in the relevant legislation	within 180 days after the expiration of storage period
The relevant personal data is the subject of a crime under the Turkish Penal Code or other legislation that imposes a criminal provision	During the Prescription of case	within 180 days after the expiration of storage period
Customer data	10 Years after recording	within 180 days after the expiration of storage period

If the purpose of the Company to use the relevant personal data has not expired, if the storage period foreseen for the relevant personal data is longer than the periods specified in the table in accordance with the relevant legislation, or if the relevant statute of repose period requires the personal data to be stored longer than the periods specified in the table, the periods which are defined in the table above may not be applied. In this case; the purpose of use, special legislation or period of statute of repose, whichever expires later, shall be applicable.

IV. METHODS OF STORAGE AND DESTRUCTON OF PERSONAL DATA BY COMPANY

A. RECORDING MEDIA

Personal data belonging to data subjects, is stored in media listed below by Company in compliance with provisions of LPPD, related legislation and within the scope of international data security principles:

Electronic media:

- Web server,
- File server,
- FTP server,
- E-mail server,
- Application server,
- Portable disks, company computers,
- CD/DVD/Media

Physical Media:

- Unit Cabinets
- ARCHIVE

B. TECHNICAL AND ADMINISTRATIVE MEASURES

All administrative and technical measures taken by Company within the framework of the principles in article 12 of the LPPD in order to keep your personal data securely, to process it illegally, to prevent access and to destroy the data in accordance with the law are listed below:

1. Administrative Measures:

Within the scope of administrative measures, Company;

a. Limits the internal access to stored personal data to the personnel required to access it in accordance with the job description. In limitation of access, it is taken into consideration whether the data is sensitive personal data and its importance degree.

b. In the event that the processed personal data is obtained by others unlawfully, it will notify this situation to the relevant person and the Board as soon as possible.

c. Regarding the sharing of personal data, signs a framework contract with the persons with whom personal data is shared, or the provisions added to the existing contract on the protection of personal data and data security.

d. In case of necessity, it employs personnel with knowledge and experience on the processing of personal data, and provides necessary training to its personnel within the scope of personal data protection legislation and data security.

e. In order to ensure the enforcement of the provisions of the Law in its own legal entity, it shall perform necessary inspections and have them performed. It shall remove the privacy and security weaknesses that arise as a result of inspections.

f. According to the medium in which personal data is located, adequate security measures (against situations like electricity leakage, fire, flood, theft, etc.) and prevents unauthorized entry and exit to these mediums.

2. Technical Measures:

Within the scope of technical measures, Company;

a. Makes the necessary internal controls within the scope of the installed systems.

b. Performs the processes of information technology risk assessment and business impact analysis within the scope of installed systems.

c. Provides the technical infrastructure which will prevent or observe data leakage out of the institution and create the relevant matrix.

d. Provides control of system weaknesses by receiving penetration test services regularly and when necessary.

e. Ensures that the access rights of employees in information technology units are kept under control.

f. Ensures that the destruction of personal data is provided in the manner that it cannot be recycled and leaves no audit trail.

g. Pursuant to 12th Article of the Law, all kinds of digital media where personal data are stored are protected by encrypted or cryptographic methods to meet information security requirements.

h. It ensures that the transaction records of all transactions that take place on their sensitive personal data are securely logged.

i. It continuously monitors the security updates of the mediums where the data is located and ensures that the necessary security tests are carried out regularly.

j. In cases where sensitive personal data is accessed through a software, it ensures that the security tests of these software are carried out regularly by making user authorizations for this software.

k. In cases where remote access to sensitive personal data is required, it provides at least a two-stage authentication system.

l. In cases where sensitive personal data is transferred;

- If it is necessary to transfer the data by e-mail, they should be transferred encrypted with the corporate e-mail address or using the REM account,
- If it is necessary to transfer data via media such as portable memory, CD, DVD, it should be encrypted with cryptographic methods,
- If the transfer is taking place between servers in different physical mediums, Decoupling the transfer between servers by installing a VPN or FTP method is ensured,

If it is necessary to transfer the data on paper, it ensures that the documents are sent in the format of "classified documents".

3. Intracompany Audit

Our Company conducts internal audits regarding the implementation of the provisions of the Law and the provisions of this Personal Data Protection and Destruction Policy and the Processing and Protection of Personal Data Policy in accordance with Article 12 of the Law.

In the event that deficiencies or defects related to the implementation of these provisions are detected as a result of internal audits, these deficiencies or defects shall be rectified immediately.

If it is understood that the personal data under the responsibility of our Company has been obtained by others by illegal means during the audit or otherwise, our Company notifies the relevant person and the Board as soon as possible.

C. DESTRUCTION PROCEDURES OF PERSONAL DATA

If the purposes for personal data processing stipulated in LPPD and Regulation are abolished, the personal data obtained by Company in accordance with the LPPD and other relevant legislation will be destroyed by Company on its own motion or upon request of related person, with the following techniques and in compliance with the provisions of Law and related legislation.

1. Techniques for Deleting and Destruction of Personal Data

The procedures and principles regarding the erasure and destruction of personal data by Company are listed below:

Secure Erasure from Software: The Personal Data stored in the digital mediums within our company are deleted from the related software in such a way that they cannot be accessed and reused for the Related Users in any way.

Deletion of the data by giving the deletion command to electronic recording media such as Tiger and LOGO Programs, Yöneteam Purchasing Program databases that we use, removing the access rights of the Relevant Users to the files located on our central server or on the directory where the files are located; deleting the relevant lines in the databases, including backups, if any, with database commands or on portable media (USB, HDD, etc.) the data can be deleted by deleting the Personal Data found using the appropriate software. However, if the erasure of personal data will result in the inability to access and use other data within the system, personal data will also be deemed erased if personal data are archived by making them unrelated to the relevant person, provided that the following conditions are met. In such cases, our Company takes all necessary technical and administrative measures to ensure that Personal Data is accessed only by authorized persons.

Blackening of Personal Data on Paper Media: It is a method of physically cutting the relevant personal data out of the document by physically cutting the personal data out of the document in order to prevent the unintended use of personal data or to erase the data requested to be erased, or to make it invisible using fixed ink in a way that cannot be recycled and cannot be read with technological solutions.

Physical Destruction: Personal data can be processed in non-automatic ways, provided that it is a part of any data recording system. When destructing such data, the system of physical destruction of personal data is applied in a manner that it could not be used afterwards. The destruction of data on paper and microfiche media should also be carried out in this way, since it is not possible to destruct them in any other way.

2. Techniques for Anonymization of Personal Data:

Anonymization means that personal data cannot be associated with a specific or identifiable real person under any circumstances, even by matching it with other data.

Variable Extraction: It is the extraction of one or more of the direct identifiers contained in the personal data of the person concerned that will serve to identify the person concerned in any way. This method can be used to anonymize personal data, or it can also be used to delete this information if there is information in the personal data that is not suitable for the purpose of data processing.

Regional Hiding: It is the process of deleting information that may be of a distinctive qualification that related to the data that is in an exceptional situation in the data table where personal data are anonymously stored collectively.

Generalization: The method of generalization of Personal Data is used in our Company in order to aggregate many data available in the database so that they cannot be associated with any real person, and thus to ensure that our Company can track a number of results that depend on the Data subjects, but without storing any Personal Data. By this means, for example, if the labor contract is terminated employees without showing credentials and dates of Birth, what year range, in which position, in which the results can be followed more productive age range of employment.

Data mixing and corruption: The direct or indirect identifiers in the personal data are confused with other values or corrupted, the relationship with the relevant person is severed and they lose their identifying qualities.

V. IMPLEMENTATION AND ENFORCEMENT

In case of incompatibility between the provisions of the LPPD and other relevant legislation and this Policy, the provisions of the LPPD and other relevant legislation will be applied decisively.

This Policy prepared by the Company has entered into force on the date of publication.
In case of amendments in the Policy, the relevant articles will be updated accordingly.