PERSONAL DATA PROTECTION AND PROCESSING POLICY

1. PURPOSE

In PETENG Petrokimya Sanayi Mühendislik Hizmetleri A.Ş. (PETENG), the purpose of this policy is to define the procedures and principles to be followed in the protection and processing of personal data in accordance with the "Personal Data Protection Law" and related secondary legislation.

2. FUNDAMENTAL PRINCIPLES

2.1 The provisions of this policy, the "Personal Data Protection Law," and other relevant legislation govern the protection and processing of personal data.

2.2 Personal data encompasses all types of information belonging to an identified or identifiable natural person. Sensitive personal data includes data on race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, association, foundation or union membership, health, sexual life, criminal convictions, security measures, as well as biometric and genetic data.

2.3 PETENG has established the necessary procedures, prepared disclosure texts, entered into confidentiality agreements, revised job descriptions, and implemented all required administrative and technical measures to ensure the protection of personal data, as outlined in this policy.

2.4 Personal data cannot be processed, transferred, used, or shared with others without the explicit consent of the data subject. Explicit consent is obtained in a clear, informed, and voluntary manner.

2.5 In cases where personal data is recorded, shared, or not deleted as required by this policy or relevant legislation, individuals will be subject to the provisions of Articles 135-140 of the Turkish Penal Code and PETENG's disciplinary actions.

2.6 All PETENG employees are personally responsible for the protection and security of personal data.

3. IMPLEMENTATION PRINCIPLES

3.1 **Ensuring the Confidentiality and Security of Personal Data**

In compliance with the Personal Data Protection Law, PETENG has implemented all technical and administrative measures specified under sections 3.1.1 and 3.1.2 of this policy to prevent unlawful processing and access to personal data and to ensure proper data storage. Necessary controls and audits are conducted.

3.1.1 Technical Measures

3.1.1.1 Technical security measures have been taken to ensure the secure processing of personal data, providing a high level of protection against potential risks. The Human Resources Department implements all technical measures.

3.1.1.2 To prevent exposure to internal and external attacks, cybercrimes, or malware, the following actions are taken:

- Records of actions on software containing personal data are maintained regularly.
- Annual penetration (breach) tests are conducted by an external, independent expert organization to assess access security to personal data storage areas, with any identified vulnerabilities being promptly addressed.
- Security software messages, access control logs, and other reporting tools are continuously monitored.
- In the event of undesirable incidents (e.g., system collapse, malware, denial-of-service attack, incorrect or incomplete data entry, or violations compromising confidentiality and integrity), evidence is collected and securely stored.
- If security issues are detected, a report is sent to senior management and the relevant consulting firm.
- Physical locations containing servers that store personal data are protected against external threats (such as fire, earthquake, etc.) and monitored by cameras.

3.1.1.3 Software with firewalls and antivirus protection systems is used.

3.1.1.4 Systems compatible with technological advancements are used for the secure storage of personal data. Risks are periodically evaluated, and necessary technological solutions are implemented.

3.1.1.5 Access control is continuously enforced on systems enabling access to personal data.

3.1.1.6 Data controllers ensure regular backups to protect against risks such as loss, destruction, theft, or corruption of personal data.

3.1.1.7 Experts with sufficient technical knowledge in data processing are employed.

3.1.1.8 Technological developments are closely monitored, and existing systems are updated and necessary measures are taken.

3.1.2 Administrative Measures

3.1.2.1 Administrative measures are taken to ensure the secure processing of personal data within the organization.

3.1.2.2 Risks related to the protection and security of personal data are accurately identified, and measures are implemented based on the potential impacts of these risks. When assessing risks and threats, the following are considered:

- Whether the data is classified as sensitive personal data,
- The level of confidentiality required by the nature of the data,
- The potential harm that a security breach may cause to the data subject.

3.1.2.3 Necessary internal control systems are established for each business unit regarding the protection and processing of personal data.

3.1.2.4 Employees are regularly educated and informed about compliance with the Personal Data Protection Law, illegal access to personal data, etc.

3.1.2.5 When administrative or technical requirements necessitate outsourcing for the processing, storage, or protection of personal data, agreements include provisions requiring the recipient to take necessary security measures to protect the data and ensure compliance within their organization in accordance with the Personal Data Protection Law.

3.1.2.6 Documents related to the Personal Data Protection Law (procedures, contracts, commitments, specifications, etc.) include obligations not to process, disclose, or use personal data outside the scope of this policy and the Law.

3.1.2.7 Employees are informed that they cannot disclose personal data they have accessed or use it for purposes other than intended, and that this obligation continues after termination of employment. Necessary precautions are taken to ensure data security.

3.2 PROCESSING OF PERSONAL DATA

3.2.1 **Methods of Data Processing**

3.2.1.1 As defined in Article 3 of the Personal Data Protection Law, any operation on personal data, such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, acquiring, making accessible, classifying, or preventing its use, is considered data processing.

3.2.1.2 PETENG adheres to principles established by the law (Article 20 of the Constitution and Article 4 of the Personal Data Protection Law) and acts in accordance with principles of trust and good faith in processing personal data. Personal data is processed for purposes including but not limited to:

- Executing human resources policies (such as recruitment, personnel management, payroll, career management, and training activities),
- Carrying out health and safety responsibilities,
- Conducting commercial and business strategy activities (such as sales, purchasing, accounting, finance, quality processes, communication, and social responsibility),
- Fulfilling obligations with authorized public entities and institutions.

3.2.1.3 Data processing activities are analyzed individually for each process/department within PETENG.

3.2.1.4 The following principles are adopted for processing personal data:

- Compliance with the law and good faith,
- Ensuring accuracy and currency,
- Processing for specific, explicit, and legitimate purposes,
- Processing in a way that is relevant, limited, and proportionate to the purpose,
- Retaining data only for as long as necessary,
- Informing data subjects prior to processing,
- Establishing systems to facilitate the exercise of data subjects' rights,
- Taking necessary measures for data protection,

- Complying with regulations for the transfer of data to third parties.

3.2.1.5 Personal data cannot be processed without the explicit consent of the data subject unless one of the following conditions applies:

- If processing is clearly stipulated by law,
- If it is mandatory for the protection of life or physical integrity,
- If it is necessary for the performance of a contract,
- If processing is required for the data controller to fulfill its legal obligation,
- If the data has been made public by the data subject,
- If processing is required for the establishment, exercise, or protection of a right,
- If processing is mandatory for the legitimate interests of the data controller.

3.2.1.6 PETENG regularly provides training and confidentiality agreements to employees regarding data protection and implements access control.

3.2.2 **Processing of Sensitive Personal Data**

3.2.2.1 As per Article 6 of the Personal Data Protection Law, sensitive personal data includes data on race, ethnicity, political opinion, philosophical beliefs, religion, and similar categories.

3.2.2.2 Sensitive data cannot be processed without explicit consent, except for public health, preventive medicine, medical diagnosis, and treatment purposes.

3.3 TRANSFER OF PERSONAL DATA

3.3.1 Personal data cannot be transferred without the explicit consent of the data subject unless one of the conditions outlined in sections 3.2.1.5 and 3.2.2.2 applies.

3.3.2 When transferring data abroad, additional conditions such as adequate protection and written guarantees between the parties apply.

3.4 DELETION, ANONYMIZATION, OR DESTRUCTION OF PERSONAL DATA

Personal data is retained only as long as required by relevant legislation. Data that has exceeded its retention period is deleted, anonymized, or destroyed in accordance with procedures specified by the law.

4. RIGHTS OF DATA SUBJECTS

PETENG acknowledges the rights of data subjects and has established systems to ensure the exercise of these rights, such as access, correction, deletion, and objection to automated processing decisions. Data subjects may submit their requests through the designated channels provided by PETENG.

5. AMENDMENTS TO THE POLICY

PETENG reserves the right to amend this policy when deemed necessary, provided it complies with applicable laws and regulations.