ETİ SODA PRODUCTION MARKETING TRANSPORTATION AND ELECTRICITY GENERATION INDUSTRY AND TRADE LIMITED COMPANY

POLICY STATEMENT ON THE PROTECTION OF SENSITIVE PERSONAL DATA

POLICY STATEMENT ON THE PROTECTION OF SENSITIVE PERSONAL DATA

ETİ SODA PRODUCTION MARKETING TRANSPORTATION AND ELECTRICITY GENERATION INDUSTRY AND TRADE LIMITED COMPANY	**ETİ SODA PRODUCTION MARKETING TRANSPORTATION AND ELECTRICITY GENERATION INDUSTRY AND TRADE LIMITED COMPANY.** **Policy on the Protection of Sensitive Personal Data**
Prepared by	**ETİ SODA PRODUCTION MARKETING TRANSPORTATION AND ELECTRICITY GENERATION INDUSTRY AND TRADE LIMITED COMPANY.**
Version	**2.0.(Date of Update: 19.12.2023)**
Approved By	**ETİ SODA PRODUCTION MARKETING TRANSPORTATION AND ELECTRICITY GENERATION INDUSTRY AND TRADE LIMITED COMPANY.**

In case of any inconsistency between the Turkish version of the policy and any translation, the Turkish version should be respected.

POLICY STATEMENT ON THE PROTECTION OF SENSITIVE PERSONAL DATA

TABLE OF CONTENTS

POLICY STATEMENT ON THE PROTECTION OF SENSITIVE PERSONAL DATA

1. PURPOSE OF THE POLICY

In accordance with the Law No. 6698 on the Protection of Personal Data ("**KVKK**" or "**Law**") and the Decision No. 2018/10 dated 31/01/2018 of the Personal Data Protection Board regarding Adequate Measures to be Taken by Data Controllers in the Processing of Sensitive Personal Data, this "**Sensitive Personal Data Protection Policy**" (ÖNVP) has been put into effect by our Company.

2. SCOPE

The aim of ÖNVP is to ensure the proper fulfillment of the requirements for compliance with the relevant legislation, recognizing the importance of the confidentiality and security of personal data obtained under the Law No. 6698 on the Protection of Personal Data (**Law/KVKK**) and other relevant legislation, and to establish a data protection and processing policy in line with international standards.

Regarding sensitive data, Article 6 of the Law is as follows:

(1) Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and attire, membership of associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data are considered sensitive personal data.

(2) Processing sensitive personal data without the explicit consent of the relevant person is prohibited.

(3) Sensitive personal data other than those related to health and sexual life listed in the first paragraph may be processed without the explicit consent of the relevant person in cases stipulated by law. Personal data related to health and sexual life may be processed without the explicit consent of the relevant person only by persons or authorized institutions and organizations who are under the obligation to maintain confidentiality, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, or the planning and management of health services and their financing.

(4) In the processing of sensitive personal data, it is also required to take adequate precautions as determined by the Board.

With ÖNVP, the principles adopted by our Company regarding the protection and processing of sensitive personal data are presented in accordance with the principles of legality, honesty, and transparency. An **Access Authorization Matrix (Annex: 1)** has been prepared to monitor the security of sensitive data and the authorization of access to the media where these data are processed within our Company.

3. DEFINITIONS

Anonymization	**:**	Making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data
Explicit Consent	**:**	The data subject's declaration of consent for the processing to be carried out after being informed about the relevant processing before it is performed.

POLICY STATEMENT ON THE PROTECTION OF SENSITIVE PERSONAL DATA

Disclosure Text	:	Disclosure to the relevant person on how long the personal data will be stored and for what purpose, how it is collected, how it is stored and whether it will be shared with third parties
Authority	:	Personal Data Protection Authority
Inventory	:	An inventory created by data controllers, linking personal data processing activities carried out in connection with their business processes to the purposes of personal data processing, data categories, recipient groups to whom data is transferred, and the group of data subjects, detailing and explaining the maximum period necessary for the purposes for which the personal data is processed, personal data intended to be transferred to foreign countries, and the measures taken regarding data security.
Relevant Person	:	Natural person whose personal data is processed
Disposal	:	Deletion, destruction or anonymization of personal data
Processing	:	Recording, storing, retaining, changing, rearranging, disclosing, transferring, taking over, making available, classifying of personal data in Article 3 of KVKK
Law/KVKK	:	Law on the Protection of Personal Data
Personal Data	:	Any kind of information regarding an identified or identifiable natural person. For example; name-surname, TR ID, e-mail, address, date of birth, bank account number, etc. Dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi KVKK kapsamında değildir.
Processing of Personal Data	:	The acquisition, recording, storage, preservation, modification, rearrangement, disclosure, transfer, takeover, making available, classification, or prevention of use of personal data, whether fully or partially by automated means or by non-automated means, provided that it is part of any data recording system, or any other operations performed on the data.
the Board	:	Personal Data Protection Board
Authority	:	Personal Data Protection Authority
Sensitive Critical Data	:	Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and attire, membership of associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data
VERBIS	:	The information system, accessible via the internet, established and managed by the Authority, which data controllers will use in applying to the Registry and for other related processes concerning the Registry.
Data Processor	:	A natural or legal person who processes personal data on behalf of the data controller based on the authority given by the data controller.
Data Controller	:	A natural or legal person who determines the purposes and means of processing personal data, and is responsible for the establishment and management of the data recording system.
Data Controllers Registry	:	The Data Controllers Registry kept by the Authority.
Data Controller Contact Person	:	The natural person notified by the data controller at the time of registration to the Registry for communication with the Authority concerning the obligations under the Law and secondary amendments to be issued based on this Law, for legal entities located in Türkiye and for the representative of legal entities not located in Türkiye
Deletion	:	Process of deleting personal data, making personal data unavailable and unusable in any way for relevant users

Destruction	:	Process of destroying personal data, making personal data unavailable and unusable in any way for relevant users

4. RELEVANT PERSONS WHOSE SENSITIVE PERSONAL DATA IS OBTAINED

A table of Relevant Persons whose sensitive personal data is obtained and processed by our Company is provided below, and the scope and application area of this Policy is limited to the relevant persons specified in the Company's Personal Data Processing Inventory. Requests from data relevant persons outside these definitions will also be processed by our Company within the framework of the KVKK and relevant legislation.

5. IMPLEMENTED CRYPTOGRAPHY/ENCRYPTION METHOD

The masking definitions included in the ÖNVP will be considered as all the methods used to transform readable numerical data into a format that cannot be understood by unwanted parties.

Digital certificates produced by certificate authorities that support international standards using mathematical methods (algorithms) for cryptography are used, aiming to provide the necessary functions for the security of important information such as confidentiality, integrity, authentication, and non-repudiation of the original. These methods are intended to protect the information and consequently the interests of the sender, receiver, carrier, subjects of the information, and any other parties against active attacks or passive perception that may occur during transmission and storage. For data the legal retention period of which has expired or the validity period of which has ended, necessary security measures are taken with the authorization mechanism on the SAP software. Additionally, when data is shared between two points, VPN or SFTP is used to ensure the confidentiality of the transmission. Since the security of encryption depends on the protection of the digital key (digital certificates), utmost care is taken in this regard. Therefore, the keys (digital certificates) used for encryption are not stored or shared in public environments.

6. MEASURES REGARDING THE PROCESSING OF SENSITIVE DATA

Access to physical and digital environments containing sensitive personal data is restricted to title holders authorized in the **Access Authorization Matrix**.

Documents and files containing personal data, especially those containing sensitive data, are stamped with a seal stating "Contains Personal Data. Confidential." and this practice aims to create awareness among personnel within the Company to prevent unauthorized access.

Controls are conducted to prevent unauthorized access to the system in cases of changes in authorization or termination of employment, and immediately upon changes in duties or termination of contractual relationships, the authorization and access of personnel are promptly revoked.

6.1. Regular training sessions are conducted on sensitive personal data security in accordance with the Law and related regulations. Personnel within our company who handle or have access to sensitive data receive training on the regulations of the Law on Protection of Personal Data (KVKK) and are brought to the maximum level of awareness.

6.2. Confidentiality agreements are established. Agreements signed with personnel include a clause containing provisions of the KVKK, and moreover, Personnel Handling Personal Data are also required to sign a Confidentiality Commitment in the course of personal data processing procedures.

6.3. Authorization and authorization period are clearly identified for users who have access to data. Access and processing permissions of users with access authority are separated from each other and are subject to approval by the superior officer (unless otherwise stipulated) throughout the term of duty. In the Access Authorization Matrix, 3 types of authorization were made on title basis. These are categorized as Viewing, Viewing & Editing and Viewing & Editing & Deleting.

6.4. Periodical authorization checks are conducted. Access to digital information is managed and monitored for each user through assigned user identities. These identities are disabled from access and use upon the termination of the personnel's service on behalf of our company. Our periodical authorization check interval is one month.

6.5. Authority in this area for personnel/employees undergoing changes in duties is promptly revoked.

6.5.1. The standard steps to be taken are listed below.

Transfer of Data from an Old PC: Data are not kept at local PCs.

The relevant department data are kept on file servers of the organization. Access authorizations are modified in the event that the position or location of the relevant employee changes.

User Settings on New Computer (Renaming/Disabling):

When a user is provided with a new computer, existing permissions are defined. Since the Active Directory domain structure is used, these definitions are automatically transferred to the user's computer based on the user.

a. Group-Specific Software Authorization Controls: Authorization controls are managed through the admin panel of the software used. If the responsible person's duty ends, the corresponding account is deleted.

b. Return of Assigned Equipment and Personnel Records: The person whose duty has ended must first return the assigned hardware and other materials along with the "Separation Form".

6.5.2. Access cards of departing personnel are collected.

6.5.3. When terminating business relationships with personnel, contractors, and external users, ongoing security requirements, legal responsibilities, responsibilities defined in confidentiality agreements if any, and conditions that will continue for a certain period after the end of the employment are communicated.

6.5.4. To perform these controls, the **Separation Form is enforced**.

6.5.5. The access cards of departing personnel are collected.

7. MEASURES FOR MEDIA WHERE SENSITIVE DATA IS STORED

In our company, sensitive data is stored in both physical and electronic media. These data are protected using secure encryption methods, and the passwords and keys (digital certificates) are kept secure and in different media. Security systems for these media are in place, and their updates are regularly carried out by our IT

Department. In the physical environment where sensitive data is stored, adequate security measures have been taken, and authorized personnel for entry and exit have been designated.

7.1. Measures Taken For Electronic Media Where Sensitive Personal Data Is Processed, Stored, And/Or Accessed are provided below.

a) Data storage using cryptographic methods: Our software does not have cryptographic data storage capabilities. However, the application is managed with a user access identity/password structure divided into modular rights.

Cryptographic **keys (digital certificates) are kept secure and in different environments.** Digital data is protected in a digital storage media (software-based "SAP") by encrypting the file containing the data or a record in a database. Additionally, when data is shared between two points, firewall and SFTP encryption is used to ensure the confidentiality of the transmission. Encryption is typically achieved with an encryption algorithm and a digital key (digital certificate) that only authorized individuals can access. The security of encryption depends on the protection of the digital key (digital certificate). Therefore, the keys (digital certificates) used for encryption are not stored or shared in public environments.

b) All actions performed on the data are securely logged.

c) Security updates for the media where the data is stored are continuously monitored, necessary security tests are regularly conducted/commissioned, and test results are recorded. Operating system updates for the systems where the data is stored are performed regularly and in a controlled manner.

d) If access to the data is through software, user authorizations for this software are performed, security tests for this software are regularly conducted/commissioned, and test results are recorded. Authorizations are carried out at the application level. Applications are integrated with Active Directory, and authorizations are made using the information from there. An authorization matrix has been obtained and checked. Users can view information they are entitled to by law.

e) If remote access to the data is required, a two-factor authentication system is provided. Secure VPN definitions have been made for external/remote access.

7.2. Measures Taken For Physical Media Where Sensitive Personal Data Is Processed, Stored, And/Or Accessed are provided below.

a. Necessary measures are taken to ensure that adequate security precautions (against electric leakage, fire, flood, theft, etc.) are in place according to the nature of the media where sensitive personal data is located. Sensitive personal data in physical form is kept in locked cabinets located in the Human Resources office and archive areas, as well as in the offices of the Occupational Health and Safety Specialist and the Workplace Physician. Office and archives are protected and secured with fire smoke detectors, extinguishing systems, alarm, and warning systems.

b. Physical security of these environments is ensured, preventing unauthorized entries and exits. Offices and archive areas containing sensitive personal data are locked outside of working hours.

8. PRINCIPLES REGARDING THE TRANSFER OF SENSITIVE DATA

Our company adheres to the following principles when transferring sensitive data:

a. If it is necessary to transfer sensitive data via email, it is done using an encrypted corporate email address or a KEP account.

b. Sensitive personal data is not transferred or stored on portable media such as USB drives, CDs, or DVDs.

c. If the transfer occurs between servers in different physical media, it is carried out via VPN or sFTP methods.

d. When transferring data in physical form, utmost care is taken to ensure that documents are not stolen, lost, or seen by unauthorized persons, and the data is transferred in a sealed envelope that is stamped.

9. IMPLEMENTATION

Our company is responsible for updating the provisions of the ÖNVP, actively monitoring the processes, increasing awareness of data security principles within our Company, and ensuring their implementation.

ANNEXES:
Annex-1: Data Access Matrix
This policy was updated on 19.12.2023 and became Version:2.

INFORMATION SECURITY, KVKK COMPLIANCE AND IMPLEMENTATION COMMITTEE

Fatma Aysun CEBİ	Legal Counselor	Member/Contact Person
Dilek ARISOY	Vice General Manager / Accounting Budget and Planning Director	Member
Çağatay MADAK	Human Resources Manager	Member
Emrah DALGIÇ	Accounting Manager	Member
Onur AKBABA	Quality Assurance & Quality Control Manager	Member
Sedat ABAKAY	Workplace Physician	Member
Metin ÖNAL	Information Technology Specialist	Member