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 procedures and procedures regarding the storage and destruction activities carried out by **PREDO SAĞLIK SAN. VE TİC. A.Ş. (hereinafter referred to as "PREDO SAĞLIK").**

In line with the mission, vision and basic principles set out in the strategic plan, our company has prioritized the processing of personal data belonging to company employees, employee candidates, service providers, visitors and other third parties in accordance with the Constitution of the Republic of Turkey, international conventions, the Personal Data Protection Law No. 6698 ("Law") and other relevant legislation and ensuring that the relevant persons use their rights effectively.

Businesses and transactions regarding the storage and destruction of personal data are carried out in accordance with the Policy prepared by our company in this direction.

1.2 Scope

Personal data belonging to company employees, employee candidates, service providers, visitors and other third parties are within the scope of this Policy and this Policy is applied in all recording media and activities for personal data processing where personal data owned or managed by our company are processed.

1.3 Abbreviations and Definitions

Recipient Group: The category of natural or legal person to whom personal data is transferred by the data controller.

Explicit Consent: Consent regarding a specific subject, based on information and expressed with free will.

Anonymization: Making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

Employee: Company personnel.

EBYS: Electronic Document Management System

Electronic Media: Media where personal data can be created, read, changed and written with electronic devices.

Non-Electronic Media: All written, printed, visual, etc. media other than electronic media.

Service Provider: A natural or legal person who provides services under a specific contract with our Company.

Relevant Person: The real person whose personal data is processed.

Relevant User: 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 for the person or unit responsible for the technical storage, protection and backup of the data.

Destruction: Deletion, disposal or anonymization of personal data.

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

Recording Medium: Any medium in which personal data processed by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system

Personal Data: Any information relating to an identified or identifiable natural person.

Personal Data Processing Inventory: The inventory that data controllers create by associating the personal data processing activities they carry out depending on their business processes with the purposes and legal reason for processing personal data, data category, transferred recipient group and data subject group, and detailing the maximum retention period required for the purposes for which personal data are processed, personal data foreseen to be transferred to foreign countries and the measures taken regarding data security.

Processing of Personal Data: Any operation performed on personal data such as obtaining, recording, storing, retaining, changing, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system.

Sensitive Personal Data: Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Periodic Destruction: The process of deletion, disposal or anonymization to be carried out ex officio at recurring intervals specified in the personal data storage and destruction policy in the event that all of the conditions for processing personal data specified in the Law are eliminated.

Policy: Personal Data Storage and Destruction Policy

Data Processor: A natural or legal person who processes personal data on behalf of the data controller based on the authorization granted by the data controller.

Data Recording System: The recording system where personal data is structured and processed according to certain criteria.

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 Information System: The information system created and managed by the Presidency, accessible via the internet, which data controllers will use in the application to the Registry and other related transactions regarding the Registry.

VERBIS: Data Controllers Registry Information System

Regulation: Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017.

2. RESPONSIBILITY AND DISTRIBUTION OF DUTIES

All units and employees of our Company actively support the responsible units in taking technical and administrative measures to ensure data security in all environments where personal data is processed in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure that personal data is stored in accordance with the law, with the proper implementation of the technical and administrative measures taken by the responsible units within the scope of the Policy, training and awareness of the unit employees, monitoring and continuous supervision.

3. RECORDING MEDIA

Personal data is securely stored by our company in accordance with the law in the following environments.

Personal data storage environments:

- Electronic Media, Non-Electronic Media Servers (domain, backup, e-mail, database, web, file sharing, etc.)
- Software (office software,
- Information security devices (firewall, intrusion detection and prevention, log file, anti-virus, etc.)
- Personal computers (desktop, laptop)
- Mobile devices (phones, tablets, etc.),
- Optical disks (CD, DVD, etc.)
- Removable memories (USB, Memory Card, etc.)
- Printer, scanner, photocopier,
- Paper,
- Manual data recording systems (survey forms, visitor logbook)
- Written, printed, visual media

4. EXPLANATIONS ON STORAGE AND DISPOSAL

Personal data belonging to employees, employee candidates, visitors and employees of third parties, institutions or organizations with whom our Company has a relationship as a service provider are stored and destroyed in accordance with the Law.

In this context, detailed explanations regarding storage and destruction are given below respectively.

4.1 Explanations on Storage

Article 3 of the Law defines the concept of processing personal data, Article 4 states that the personal data processed must be linked, limited and measured for the purpose for which they are processed and must be retained for the period stipulated in the relevant legislation or required for the purpose for which they are processed, and Articles 5 and 6 list the conditions for processing personal data.

Accordingly, within the framework of our Company's activities, personal data are stored for the period stipulated in the relevant legislation or in accordance with our processing purposes.

4.1.1 Legal Reasons Requiring Storage

Personal data processed within the framework of our Company's activities are retained for the period stipulated in the relevant legislation. In this context, personal data are stored for the storage periods stipulated within the framework of the following:

- Law No. 6698 on the Protection of Personal Data,
- Turkish Code of Obligations No. 6098,
- Public Procurement Law No. 4734,
- Law No. 657 on Civil Servants,
- Law No. 5510 on Social Security and General Health Insurance,
- Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through These Publications,
- Law No. 5018 on Public Financial Management,
- Law No. 6331 on Occupational Health and Safety,
- Law No. 4982 on Access to Information,
- Law No. 3071 on the Exercise of the Right to Petition,
- Labor Law No. 4857,
- Law No. 2547 on Higher Education,
- Law No. 5434 on Retirement Health,
- Law No. 2828 on Social Services
- Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Annexes,
- Regulation on Archive Services
- Other secondary regulations in force under these laws

4.1.2 Processing Purposes Requiring Storage

Our 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 provide company security,
- To be able to do statistical studies.
- To be able to perform works and transactions as a result of signed contracts and protocols.
- To ensure the fulfillment of legal obligations as required or mandated by legal regulations.
- To liaise with real/legal persons who have a business relationship with our Company.
- To make legal reports.
- Obligation of proof as evidence in legal disputes that may arise in the future.

4.2 Reasons for Destruction

Personal data shall be deleted, destroyed or ex officio deleted, destroyed or anonymized by our company upon the request of the data subject in the following cases:

- In the event that the provisions of the relevant legislation that constitute the basis for processing are amended or abolished,
- In the event that the purpose requiring its processing or storage disappears,
- In cases where the processing of personal data takes place only on the basis of explicit consent, the data subject may withdraw his/her explicit consent,
- In accordance with Article 11 of the Law, if the application made by the person concerned regarding the deletion and destruction of his personal data within the framework of his rights is accepted by our Company,
- In cases where our Company rejects the application made by the relevant person with the request for the deletion, destruction or anonymization of his/her personal data, finds the answer insufficient or does not respond within the period stipulated in the Law, he/she makes a complaint to the Board and this request is approved by the Board,
- In the event that the maximum period for which the personal data is required to be retained has elapsed and there are no circumstances that would justify retaining the personal data for a longer period.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

Technical and administrative measures are taken by our company within the framework of adequate measures determined and announced by our company for special quality personal data in accordance with Article 12 of the Law and Article 6, paragraph four of the Law for the safe storage of personal data, prevention of unlawful processing and access and destruction of personal data in accordance with the law.

5.1 Technical Measures

The technical measures taken by our Company regarding the personal data it processes are listed below:

• Penetration tests reveal risks, threats, vulnerabilities and gaps, if any, in our company's information systems and necessary measures are taken.

• Risks and threats that will affect the continuity of information systems are continuously monitored as a result of real-time analysis with information security incident management.

• Access to information systems and authorization of users are carried out through access and authorization matrix and security policies through the corporate active directory.

• Necessary measures are taken for the physical security of our company's information systems equipment, software and data.

• 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 malware, etc.) measures are taken.

• Risks to prevent unlawful processing of personal data are identified, technical measures are taken in accordance with these risks and technical controls are carried out for the measures taken.

• Access procedures are established within our company and reporting and analysis studies on access to personal data are carried out.

• Access to the storage areas containing personal data is recorded and inappropriate access or access attempts are kept under control.

• Our Company takes necessary measures to ensure that deleted personal data is inaccessible and non-reusable for the relevant users.

• Security vulnerabilities are monitored, appropriate security patches are installed and information systems are kept up-to-date.

• Strong passwords are used in electronic media where personal data is processed.

• Secure logging systems are used in electronic media where personal data is processed.

• Data backup programs are used to ensure that personal data is stored securely.

• Access to personal data stored in electronic or non-electronic media is restricted according to access principles.

• A separate policy has been determined for the security of special categories of personal data.

• Trainings on special categories of personal data security have been provided for employees involved in special categories of personal data processing processes, confidentiality agreements have been made, and the authorizations of users authorized to access data have been defined.

• Electronic media where sensitive personal data are processed, stored and/or accessed are maintained 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 / conducted, and test results are recorded,

• Adequate security measures are taken for the physical environments where sensitive personal data are processed, stored and/or accessed, and unauthorized entry and exit are prevented by ensuring physical security.

• If sensitive personal data is required to be transferred via e-mail, it is transferred encrypted with a corporate e-mail address or using a KEP account. If it needs to be transferred via media such as portable memory, CD, DVD, etc., it is encrypted with cryptographic methods and the cryptographic key is kept in different media. If data is transferred between servers in different physical environments, a VPN is established between the servers or data is transferred via FTP method. If it is necessary to transfer via paper media, necessary precautions are taken against risks such as theft, loss or unauthorized viewing of the document and the document is sent in "confidential" format.

5.2 Administrative Measures

The administrative measures taken by our Company regarding the personal data it processes are listed below:

- In order to improve the quality of employees, trainings are provided on preventing unlawful processing of personal data, preventing unlawful access to personal data, ensuring the

protection of personal data, communication techniques, technical knowledge skills, Law No. 657 and other relevant legislation.

- Confidentiality agreements are signed by employees regarding the activities carried out by our Company.
- A disciplinary procedure has been prepared for employees who do not comply with security policies and procedures.
- Before starting personal data processing, our company fulfills the obligation to inform the relevant persons.
- Personal data processing inventory has been prepared.
- Periodic and random audits are conducted within the company.
- Information security trainings are provided for employees.

6. PERSONAL DATA DESTRUCTION TECHNIQUES

At the end of the period stipulated in the relevant legislation or the retention period required for the purpose for which they are processed, personal data are destroyed by our company ex officio or upon the application of the person concerned, in accordance with the provisions of the relevant legislation, by the following techniques.

6.1 Deletion of Personal Data

Personal data is deleted by the methods described below.

• Personal Data on Servers:

For the personal data on the servers, deletion is made by the system administrator by removing the access authorization of the relevant users for those whose retention period has expired.

• Personal Data in Electronic Media:

The personal data in electronic media that expire after the expiration of the period for which they are required to be stored shall be rendered inaccessible and non-reusable in any way for employees (relevant users) other than the database administrator.

• Personal Data in Physical Environment:

For the personal data kept in physical media, those that have expired for the period required to be kept are rendered inaccessible and non-reusable in any way for other employees, except for the unit manager responsible for the document archive. In addition, the blackout process is also applied by scratching/painting/erasing in such a way that it cannot be read.

• Personal Data on Portable Media

The personal data kept in flash-based storage media, which expires after the period of time required for storage, is encrypted by the system administrator and access authorization is given only to the system administrator and stored in secure environments with encryption keys.

6.2 Destruction of Personal Data

Personal data is destroyed by the methods described below.

• Personal Data in Physical Media:

Personal data on paper media, which expire after the period of time required for their storage, are irreversibly destroyed in paper shredding machines.

• Personal Data in Optical / Magnetic Media:

Personal data on optical media and magnetic media that expire after the expiry of the retention period are physically destroyed, such as melting, incineration or pulverization. In addition, the magnetic media is passed through a special device and the data on it is rendered unreadable by exposing it to a high magnetic field.

6.3 Anonymization of Personal Data

Anonymization of personal data means making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even if the personal data is matched with other data.

In order for personal data to be anonymized, personal data must be rendered unattributable to an identified or identifiable natural person even through the use of appropriate techniques for the recording medium and the relevant field of activity, such as the return of personal data by the data controller or third parties and/or matching the data with other data.

7. RETENTION AND DESTRUCTION PERIODS

Regarding the personal data processed by our Company within the scope of its activities, the relevant information is available in the following:

- Retention periods on the basis of personal data related to all personal data within the scope of activities carried out depending on the processes are included in the Personal Data Processing Inventory;
- Retention periods on the basis of data categories are included in the record in VERBIS;
- Retention periods on process basis are included in the Personal Data Retention and Destruction Policy.

For personal data whose retention periods have expired, the process of ex officio deletion, destruction or anonymization is carried out by our company.

8. PERIODIC DESTRUCTION PERIOD

Our Company has set the periodic destruction period as 6 months.

9. PUBLICATION AND PRESERVATION OF THE POLICY

The Policy is published on our website and disclosed to the public on the website. The printed paper copy is also kept in the relevant department within our company.

10. PERIOD FOR UPDATING THE POLICY

The Policy is reviewed as needed and the necessary sections are updated.

11. ENFORCEMENT AND ABROGATION OF THE POLICY

The Policy is deemed to have entered into force upon its publication on our company's website.