COMMITMENT OF LOYALTY AND CONFIDENTIALITY

…….. DENTAL PRACTICE
PERSONAL DATA RETENTION AND DESTRUCTION POLICY

INTRODUCTION

THE NATURE, PURPOSE AND SCOPE OF THE DESTRUCTION POLICY

This Destruction Policy (the "POLICY") has been prepared by ……. Dental Practice providing Oral and Dental Health Services (the "PRACTICE"), acting as the Data Controller Dentist (the "DATA CONTROLLER"), for the purpose of determining the procedures and principles to be applied regarding the deletion, destruction and/or anonymization of personal data obtained, in accordance with the Turkish Personal Data Protection Law No. 6698 and the relevant legislation.

Within this scope, the personal data of all real persons whose personal data are held within the PRACTICE, including PRACTICE employees, employee candidates, patients, patient companions/guardians/parents, are processed in accordance with the Constitution and applicable laws within the framework of this Personal Data Retention and Destruction Policy.

DEFINITIONS

Data Controller
The real 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 Subject
The real person whose personal data are processed.

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

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

Processing of Personal Data
Any operation performed on personal data such as obtaining, recording, storing, retaining, altering, reorganizing, disclosing, transferring, taking over, making accessible, classifying or preventing the use of personal data, whether fully or partially by automated means or by non-automated means provided that it forms part of a data recording system.

Data Processor
The real or legal person who processes personal data on behalf of the Data Controller, based on the authority granted by the Data Controller.

Destruction
The deletion, destruction or anonymization of personal data.

Erasure
The process of rendering personal data inaccessible, irretrievable and unusable in any manner by anyone.

Deletion
The process of rendering personal data inaccessible and unusable in any manner for the relevant users.

Anonymization
The process of rendering personal data incapable of being associated with an identified or identifiable real person under any circumstances, even when matched with other data.

Law / KVKK
The Personal Data Protection Law No. 6698, published in the Official Gazette dated 07.04.2016 and numbered 29677.

Regulation
The Regulation on the Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette dated 28.10.2017 and numbered 30224.

Board
The Personal Data Protection Board.

Authority
The Personal Data Protection Authority.

Recording Medium
Any environment in which personal data are processed, whether fully or partially by automated means or by non-automated means provided that it forms part of a data recording system.

Data Recording System
The recording system in which personal data are processed by being structured according to specific criteria.

RESPONSIBILITIES AND DISTRIBUTION OF DUTIES

The DATA CONTROLLER is responsible for the preparation, development, implementation, publication in relevant environments and updating of the POLICY, ensuring that employees act in compliance with the Policy, and providing the technical solutions required for the implementation of the POLICY.

PRACTICE employees shall comply with the technical and administrative measures aimed at ensuring data security in all environments where personal data are processed, in order to duly implement the technical and administrative measures adopted within the scope of the POLICY, to prevent the unlawful processing of personal data, to prevent unlawful access to personal data, and to ensure the lawful storage of personal data.

METHODS OF COLLECTING PERSONAL DATA

Personal data are obtained verbally, in writing or electronically, through automated and non-automated methods, by real or legal persons acting as data processors authorized by the DATA CONTROLLER, within the conditions and purposes specified in the Personal Data Protection Law No. 6698 and the secondary legislation issued pursuant thereto; through means such as the application of data subjects to the PRACTICE and the provision of initial information, opening a record and creating a patient file, forms and records kept in paper and electronic media, online via the SGK system, from records shared in cases where private insurance companies are used, from the records of other healthcare institutions in cases where the data subject has been referred to the PRACTICE, through the submission of CVs or job applications, and when contacting the PRACTICE for any purpose as a supplier/service provider and receiving services.

RECORDING MEDIA

Personal data are stored securely and lawfully by the PRACTICE in the media listed in Table 2.

3.1. DATA STORED IN ELECTRONIC MEDIA

Servers (domain, backup, e-mail, database, web, file sharing, etc.)
Software (office software, portals, medical software)
Information security devices (firewall, intrusion detection and prevention systems, log files, antivirus, etc.)
Personal computers (desktop, laptop)
Mobile devices (phones, tablets, etc.)
Optical disks (CD, DVD, etc.)
Removable storage media (USB, memory cards, etc.)
Printers, scanners, photocopy machines

3.2. NON-ELECTRONIC MEDIA

Paper
Manual data recording systems (patient files, protocol register, inspection and audit register, working documents, visitor entry register, and other registers required to be kept pursuant to the Regulation on Private Healthcare Institutions Providing Oral and Dental Health Services)
Written, printed and visual media

EXPLANATIONS REGARDING RETENTION AND DESTRUCTION

By the DATA CONTROLLER, the personal data of all real persons whose personal data are held within the PRACTICE for any reason, including employees, employee candidates, patients, patient companions/guardians/parents, are retained and destroyed in accordance with the Law. Within this scope, detailed explanations regarding retention and destruction are provided below in order.

4.1. EXPLANATIONS REGARDING RETENTION

In Article 3 of the Law, the concept of processing of personal data is defined; in Article 4, it is stipulated that the processed personal data must be related to, limited and proportionate to the purposes 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 in Articles 5 and 6, the conditions for processing personal data are listed. Accordingly, within the scope of the PRACTICE's activities, personal data are retained by the DATA CONTROLLER for the period stipulated in the relevant legislation or appropriate to the purposes of processing.

4.1.1. LEGAL GROUNDS REQUIRING RETENTION

At the PRACTICE, personal data processed within the scope of its activities are retained for the period required by the service provided and stipulated in the relevant legislation. Within this scope, personal data are retained for the retention periods stipulated under:

- Personal Data Protection Law No. 6698,
- Law No. 1219 on the Practice of Medicine and Its Branches,
- Turkish Code of Obligations No. 6098,
- Turkish Penal Code No. 5237,
- Social Insurance and General Health Insurance Law No. 5510,
- Basic Law on Health Services No. 3359,
- Occupational Health and Safety Law No. 6361,
- Labor Law No. 4857,
- Regulation on Private Healthcare Institutions Providing Oral and Dental Health Services,
- Regulation on Occupational Health and Safety Services,
- Regulation on Patient Rights,
- Medical Deontology Regulation,
- Turkish Dental Association Rules of Professional Ethics for Dentistry,
- Other relevant laws and secondary legislation in force pursuant to these laws.

4.1.2. PURPOSES OF PROCESSING REQUIRING RETENTION

Personal data processed within the scope of the PRACTICE's activities are retained for the following purposes:

- To perform business and transactions arising from signed contracts and protocols.
- To fulfill the burden of proof as evidence in potential future legal disputes.
- To ensure the fulfillment of legal obligations as required or mandated by legal regulations.

4.2. GROUNDS REQUIRING DESTRUCTION

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

- Amendment or repeal of the relevant legislative provisions forming the basis for the processing of personal data,
- Elimination of the purpose requiring the processing or retention of personal data,
- In cases where the processing of personal data is based solely on the explicit consent, the withdrawal of such explicit consent by the data subject,
- Acceptance by the PRACTICE of the data subject's application for the deletion or destruction of personal data within the scope of the data subject's rights pursuant to Article 11 of the Law,

- In cases where the PRACTICE rejects the data subject's application for the deletion, destruction or anonymization of personal data, finds its response insufficient or fails to respond within the period stipulated in the Law, and the data subject applies to the Board and such request is deemed appropriate by the Board,
- Expiry of the maximum period requiring the retention of personal data and the absence of any condition justifying the retention of personal data for a longer period.

TECHNICAL AND ADMINISTRATIVE MEASURES

In order to ensure the secure retention of personal data, to prevent unlawful processing and access thereto, and to ensure the lawful destruction of personal data, technical and administrative measures are taken by the PRACTICE within the framework of Article 12 of the Law and the sufficient measures determined and announced by the Board for special categories of personal data pursuant to Article 6, paragraph 4 of the Law.

5.1. TECHNICAL MEASURES

The technical measures taken by the DATA CONTROLLER regarding the personal data it processes are listed below:

- Technical controls are carried out to prevent the unlawful processing of personal data (e.g. penetration testing); risks, threats, vulnerabilities and exposures are identified, appropriate technical measures are implemented in accordance with these risks, and the results of the controls are recorded.
- Necessary measures are taken to ensure the security of all personal data, including special categories of personal data stored in electronic environments. Within this scope; firewalls, attack prevention systems, network access control, systems preventing malicious software, and security patches are used. Information systems are kept up to date, data backup programs are utilized, strong passwords are used in electronic environments where personal data are processed, electronic environments are protected using cryptographic methods, and cryptographic keys are kept in secure environments.
- Access to electronic and non-electronic storage areas containing personal data is logged, inappropriate access or access attempts are kept under control, secure logging systems are used, access authorization is implemented, and necessary measures are taken to ensure that deleted personal data are inaccessible and cannot be reused by relevant users.
- Considering that special categories of personal data are processed at the PRACTICE, employees are provided with training on the security of special categories of personal data and confidentiality agreements are executed.
- Necessary measures are taken to ensure the physical security of the information systems equipment, software, and the environments where such systems are stored and/or accessed, in which all personal data, including special categories of personal data, are kept at the PRACTICE (restriction of access by unauthorized persons, fire extinguishing systems, air conditioning systems, etc.).

5.2. ADMINISTRATIVE MEASURES

The administrative measures taken by the DATA CONTROLLER regarding the personal data it processes are listed below:

- Trainings are provided to improve the qualifications of employees on the prevention of unlawful processing of personal data, prevention of unlawful access to personal data, ensuring the retention of personal data, communication techniques, technical knowledge and skills, the Personal Data Protection Law, the Labor Law, and other relevant legislation.
- Confidentiality agreements are executed with employees regarding the activities carried out by the DATA CONTROLLER.
- Prior to commencing the processing of personal data, the DATA CONTROLLER fulfills its obligation to inform the data subjects.
- A personal data processing inventory has been prepared.
- Periodic and random internal audits are conducted within the PRACTICE.
- Information security trainings are provided to employees.

PERSONAL DATA DESTRUCTION TECHNIQUES
At the end of the retention period stipulated in the relevant legislation or required for the purposes for which personal data are processed, personal data are destroyed by the DATA CONTROLLER, ex officio or upon the application of the data subject, in accordance with the relevant legislative provisions, using the techniques specified below.

6.1. DELETION OF PERSONAL DATA
Personal data are deleted using the methods specified below:

Personal data stored on servers:
For personal data stored on servers for which the retention period has expired, deletion is carried out by the DATA CONTROLLER by removing the access authorization of the relevant users.

Personal data stored in electronic media:
Personal data stored in electronic media for which the retention period has expired are rendered inaccessible and unusable in any manner for employees other than the DATA CONTROLLER (relevant users).

Personal data stored in physical media:
For personal data stored in physical media for which the retention period has expired, such data are rendered inaccessible and unusable in any manner for persons other than the DATA CONTROLLER. In addition, redaction is applied by crossing out, painting over or erasing the data in a manner that makes them illegible.

Personal data stored on portable media:
Personal data stored on flash-based storage media for which the retention period has expired are encrypted by the DATA CONTROLLER, access authorization is granted solely to the DATA CONTROLLER, and the encryption keys are stored in secure environments.

6.2. DESTRUCTION OF PERSONAL DATA

Personal data are destroyed using the methods specified below:

Personal data stored in physical media:
Personal data stored in paper form for which the retention period has expired are destroyed in an irreversible manner using paper shredding machines.

Personal data stored in optical/magnetic media:
For personal data stored in optical and magnetic media for which the retention period has expired, physical destruction methods such as melting, burning or pulverizing are applied. In addition, data stored on magnetic media are rendered unreadable by being exposed to a high-value magnetic field through a special device.

6.3. ANONYMIZATION OF PERSONAL DATA

Anonymization of personal data means rendering personal data incapable of being associated with an identified or identifiable real person under any circumstances, even when matched with other data. The anonymization methods used at the PRACTICE are as follows:

Removal of variables:
The removal of one or more direct identifiers contained within the personal data of the relevant person that would enable the identification of the person in any manner.

Regional masking:
The process of deleting information that may have a distinguishing nature regarding exceptional data within a data table in which personal data are collectively and anonymously present.

Generalization:
The process of converting personal data belonging to many individuals into statistical data by aggregating them and removing distinguishing information.

Lower and upper bound coding:
For a specific variable, intervals belonging to that variable are defined and categorized. If the variable does not contain a numerical value, similar data within the variable are categorized. Values falling within the same category are consolidated.

Micro-aggregation:
Under this method, all records in the data set are first ordered according to a meaningful sequence and then the entire set is divided into a certain number of subsets. Subsequently, the average of the value of the specified variable for each subset is calculated and the value of that variable for the subset is replaced with the average value. As indirect identifiers contained in the data will be distorted in this way, associating the data with the relevant person is made more difficult.

Data shuffling and perturbation:
Direct or indirect identifiers within personal data are mixed with or distorted by other values, thereby severing their association with the relevant person and causing them to lose their identifying characteristics.

RETENTION AND DESTRUCTION PERIODS

With regard to the personal data processed within the scope of its activities by the DATA CONTROLLER:

- Retention periods on a personal data basis for all personal data within the scope of activities carried out depending on processes are included in the Personal Data Processing Inventory;
- Retention periods on a data category basis are included in the registration with VERBİS;
- Retention periods on a process basis are included in the Personal Data Retention and Destruction Policy.

Where necessary, the DATA CONTROLLER updates the said retention periods. For personal data whose retention periods have expired, deletion, destruction or anonymization is carried out ex officio by the DATA CONTROLLER.

PROCESS	RETENTION PERIOD	DESTRUCTION PERIOD
Fulfillment of Employer Obligations and Human Resources Processes	Retained for 10 years as of the termination of the employment contract; if a legal process is ongoing, retained until the conclusion of such process. (Article 86/1 of Law No. 5510)	At the first periodic destruction period following the end of the retention period.
Fulfillment of Obligations Related to Occupational Health and Safety	Retained for 15 years as of the termination of the employment contract; if a legal process is ongoing, retained until the conclusion of such process. (Article 7 of the Regulation on Occupational Health and Safety Services)	
Provision of Healthcare Services	Retained for 20 years in accordance with the relevant legal regulations and the requirements of healthcare services. If a legal process is ongoing, retained until the conclusion of such process. (Articles 146, 147 and 478 of the Turkish Code of Obligations No. 6098; Articles 66–72 of the Turkish Penal Code No. 5237; Article 49 of the Regulation on Private Hospitals)	
Procurement of Services from Third Parties	Retained for 10 years as of the termination of the contract; if a legal process is ongoing, retained until the conclusion of such process. (Article 146 of the Turkish Code of Obligations No. 6098)	

NOTE:
In cases where a longer period is stipulated pursuant to the Law and other legislation, or where a longer period is foreseen under the legislation for statutes of limitation, forfeiture

periods, retention periods, etc., the periods specified in the relevant legislation shall be accepted as the maximum retention period.

PERIODIC DESTRUCTION PERIOD
Pursuant to Article 11 of the Regulation, the DATA CONTROLLER has determined the periodic destruction period as 6 months. Accordingly, periodic destruction procedures are carried out at the CLINIC every year in June and December.

PUBLICATION AND STORAGE OF THE POLICY
The POLICY is prepared in printed form with a wet signature and stored in the relevant files at the CLINIC. If the CLINIC has a website, the POLICY is also disclosed to the public on the website.

POLICY UPDATE PERIOD
The POLICY is reviewed as needed and the necessary sections are updated.

ENTRY INTO FORCE AND REPEAL OF THE POLICY
The POLICY shall be deemed to have entered into force after the completion of the VERBIS registration by the DATA CONTROLLER.

In the event that a decision is made to repeal the POLICY, the old wet-signed copies of the POLICY shall be cancelled by the DATA CONTROLLER (by affixing a cancellation stamp or by writing “cancelled”), signed, and stored in the relevant files at the CLINIC for a minimum period of 5 years.

DATA CONTROLLER
NAME SURNAME
SIGNATURE