**DATA STORAGE AND DESTRUCTION POLICY**
**NOVA DENTAL AND MEDICAL SERVICES LIMITED COMPANY**

**PERSONAL DATA STORAGE, DESTRUCTION, AND ANONYMIZATION POLICY**

**PURPOSE AND SCOPE**

The Personal Data Storage and Destruction Policy ("Policy") has been prepared to establish the procedures and principles regarding the data storage and destruction activities conducted by NOVA DENTAL AND MEDICAL SERVICES LIMITED COMPANY ("My Nova Oral and Dental Health Center" or "Company").

Our fundamental principle as a company is the processing of personal data of company customers, employees, candidates, service providers, visitors, and other third parties in compliance with the Constitution of the Republic of Turkey, international agreements, the Personal Data Protection Law No. 6698 ("Law"), and other relevant legislation. In this context, the priority is to ensure that the data subjects do not suffer any rights violations and can effectively use their rights.

This Personal Data Storage and Destruction Policy has been prepared in compliance with the Personal Data Protection Law No. 6698, the Regulation on Deletion, Destruction, or Anonymization of Personal Data published in the Official Gazette on 28 October 2017, and other relevant legislation.

**DEFINITIONS**

- **Recipient Group**: The category of natural or legal persons to whom personal data is transferred by the data controller.
- **Explicit Consent**: The consent given freely and based on information regarding a specific subject.
- **Anonymization**: The process of making personal data irreversibly unidentifiable to any specific or identifiable person, even when matched with other data.
- **Employee**: The staff of My Nova Oral and Dental Health Center.
- **Electronic Environment**: Environments where personal data can be created, read, modified, and written using electronic devices.
- **Non-Electronic Environment**: All written, printed, visual, etc., environments that are not electronic.
- **Service Provider**: A natural or legal person providing services to the Personal Data Protection Authority within a specific contractual framework.
- **Data Subject**: The natural person whose personal data is processed.

- **Relevant User**: Persons within the data controller's organization or those processing personal data based on authorization from the data controller, except for those responsible for technical data storage, protection, and backup.

- **Destruction**: The deletion, destruction, or anonymization of personal data.

- **Law**: The Personal Data Protection Law No. 6698.

- **Record Environment**: Any environment where personal data is processed, either automatically or manually, as part of a data recording system.

- **Personal Data**: Any information that can identify a person.

- **Personal Data Processing Inventory**: A detailed inventory created by data controllers that associates personal data processing activities with their purposes, legal basis, data categories, and the groups of persons whose data is being processed, along with the maximum retention periods for the data and the security measures taken.

- **Personal Data Processing**: Any operation performed on personal data, including collection, recording, storage, modification, retrieval, disclosure, transfer, and erasure.

- **Board**: The Personal Data Protection Board.

- **Sensitive Personal Data**: Data concerning a person's race, ethnic origin, political opinions, philosophical beliefs, religion, sect, or other beliefs, clothing, membership in associations, foundations, or trade unions, health, sexual life, criminal convictions, and security measures, as well as biometric and genetic data.

- **Periodic Destruction**: The deletion, destruction, or anonymization process carried out automatically at regular intervals when all the conditions for processing personal data, as outlined in the Law, are no longer applicable.

- **Policy**: The 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 data controller's authority.

- **Data Recording System**: A system for processing personal data structured according to specific criteria.

- **Data Controller**: The natural or legal person responsible for determining the purposes and means of personal data processing and managing the data recording system.

- **Data Controllers Registry Information System (VERBIS)**: A system accessible online, created and managed by the authority, where data controllers can apply and conduct other relevant operations.

**RECORD ENVIRONMENTS**

The following table shows the environments in which personal data stored by My Nova Oral and Dental Health Center are recorded. The personal data stored by our company is kept in the most appropriate record environment according to its nature and legal status.

**Data Record Environment**
**Description**

**Electronic Environments**

- Servers (Domain, backup, email, database, web, file sharing, etc.)
- Software (Office software, Intranet Portal, ERP software, "Netsis," etc.)
- Information security devices (Firewall, intrusion detection and prevention, log files, antivirus, etc.)
- Company computers (Desktop, laptop)
- Company mobile devices (Phone, tablet, etc.)
- Optical disks (CD, DVD, etc.)
- Removable storage devices (USB, memory cards, etc.)

**Non-Electronic Environments**

- Paper
- Manual data recording systems (Notebooks, telephone directories, etc.)
- Written, printed, visual environments

---

**RESPONSIBILITIES AND TASK DISTRIBUTION**

According to Article 6(f) of the Regulation, it is stipulated that the titles, duties, and departments of individuals involved in the storage and destruction processes of personal data should be specified. In this context, to prevent the unlawful processing and access to personal data, and to ensure the lawful storage of personal data, the titles, duties, and departments of the persons responsible for managing the data security, storage, and

destruction processes, as well as the implementation of technical and administrative measures, are outlined below.

**Title | Job Description**

**Personal Data Manager**

Responsible for directing all planning, analysis, research, and risk assessment activities related to projects conducted for compliance with the law; managing processes that need to be executed under the Personal Data Protection Law, Personal Data Processing and Protection Policy, Personal Data Storage and Destruction Policy, and other policies and procedures; and making decisions on requests from the relevant persons.

**My Nova Oral and Dental Health Center Personal Data Protection Specialist** (Technical and Administrative)

Responsible for reviewing and reporting the requests of the data subjects to the Personal Data Manager; performing the actions regarding the requests of data subjects as decided by the Personal Data Manager; overseeing the storage and destruction processes; reporting the audits to the Personal Data Manager; and ensuring that storage and destruction processes are executed.

**Human Resources Manager, Legal Affairs Department Head, Quality Director**

Responsible for implementing policies in line with their job descriptions and conducting audits regarding the protection, storage, and destruction of personal data.

---

## STORAGE AND DESTRUCTION EXPLANATIONS

Within the company, personal data of the persons served is processed in accordance with the requirements set forth by the Law, stored in the record environments mentioned in this policy, and destroyed as specified in this policy. Additionally, personal data of our company staff is stored and destroyed in compliance with the same procedures.

Personal data is stored based on one or more of the personal data processing conditions specified in Articles 5 and 6 of the Law. In this context, personal data is stored for as long as the conditions for processing personal data are valid. When these conditions no longer apply, or upon the request of the data subject (after checking other legal obligations that the Company must comply with), the stored personal data will be deleted, destroyed, or anonymized upon request.

### Legal Reasons for Storage

The personal data processed by the Company is kept for the period prescribed by the relevant legislation. The personal data is stored for the following legal periods, according to the applicable laws:

- Labor Law No. 4857
- Turkish Commercial Code No. 6102

- Turkish Code of Obligations No. 6098
- Consumer Protection Law No. 6502
- Vocational Education Law No. 3308
- Occupational Health and Safety Law No. 6331
- Personal Data Protection Law No. 6698
- Tax Procedure Law No. 213
- Social Security and General Health Insurance Law No. 5510
- Basic Health Services Law No. 3359
- Decree Law No. 663 on the Organization and Duties of the Ministry of Health and Its Affiliated Institutions
- Regulation on the Improvement and Evaluation of Quality in Health Services No. 29399
- Regulation on Private Hospitals
- Regulation on the Processing of Personal Health Data and Protection of Privacy
- Regulation on Archive Services
- And other applicable secondary regulations.

**Purposes for Storing Personal Data**

The company stores the personal data it processes within the scope of its activities for specific purposes. The purposes are listed below:

- Management of Emergency Response Processes
- Management of Information Security Processes
- Management of Employee Candidate / Intern / Student Selection and Placement Processes
- Management of Employee Candidates' Application Processes
- Management of Employee Satisfaction and Engagement Processes
- Fulfillment of Employment Contract and Legal Obligations for Employees

- Management of Employee Benefits and Perks Processes
- Management of Audit / Ethics Activities
- Management of Training Activities
- Management of Access Permissions
- Ensuring Activities are Carried Out in Compliance with Legislation
- Management of Finance and Accounting Operations
- Management of Company / Product / Service Loyalty Processes
- Ensuring Physical Facility Security
- Management of Assignment Processes
- Management and Tracking of Legal Affairs
- Management of Internal Audits / Investigations / Intelligence Activities
- Management of Communication Activities
- Planning of Human Resources Processes
- Management / Supervision of Business Activities
- Management of Occupational Health / Safety Activities
- Collecting and Evaluating Suggestions for Improving Business Processes
- Management of Business Continuity Activities
- Management of Logistics Activities
- Management of Goods / Services Procurement Processes
- Management of Post-Sale Support Services for Goods / Services
- Management of Goods / Services Sales Processes
- Management of Goods / Services Production and Operations Processes
- Management of Customer Relations Processes
- Managing Activities for Customer Satisfaction

- Organization and Event Management
- Conducting Marketing Analysis Studies
- Management of Performance Evaluation Processes
- Managing Advertising / Campaign / Promotion Processes
- Management of Risk Management Processes
- Management of Storage and Archiving Activities
- Management of Social Responsibility and Civil Society Activities
- Management of Contract Processes
- Managing Sponsorship Activities
- Management of Strategic Planning Activities
- Tracking Requests / Complaints
- Ensuring the Safety of Movable Assets and Resources
- Management of Supply Chain Processes
- Implementation of Compensation Policy
- Management of Marketing Processes for Goods / Services
- Ensuring the Security of Data Controller Operations
- Managing Foreign Employee Work and Residence Permit Procedures
- Management of Investment Processes
- Management of Talent / Career Development Activities
- Providing Information to Authorized Persons, Institutions, and Organizations
- Managing Management Activities
- Creation and Tracking of Visitor Records

---

**Reasons for Data Destruction**

Personal data will be destroyed under the following conditions:

- Changes or abolition of the relevant legal provisions on which the data processing is based,
- The purpose for which the data was processed or stored has ceased to exist,
- In cases where the processing of personal data is based solely on explicit consent, if the data subject withdraws their explicit consent,
- Upon the request of the data subject for the deletion and destruction of their personal data, if the request is accepted under Article 11 of the Law,
- If the Company rejects the request of the data subject to delete, destroy, or anonymize their personal data, considers the response insufficient, or fails to respond within the time specified in the Law; or if the request is submitted to the Personal Data Protection Authority and the request is found appropriate by the Authority,
- The maximum period required for storing personal data has passed, and there is no valid reason to keep the data for a longer period,
- The storage periods prescribed in the relevant regulations have expired.

In these cases, the personal data will be deleted, destroyed, or anonymized upon the request of the data subject or automatically by the Company.

---

**Technical and Administrative Measures Taken to Secure Personal Data, Prevent Unlawful Processing and Access**

My Nova Oral and Dental Health Center takes all necessary technical and administrative measures appropriate to the nature of the personal data and the environment in which it is stored, to ensure the secure storage of personal data and prevent unlawful processing and access. In addition, the company takes technical and administrative measures within the framework of sufficient measures determined and announced by the Personal Data Protection Authority for sensitive personal data, as required by Article 12 of the Law and the 4th paragraph of Article 6 of the Law.

These measures, which are not limited to the following, include the necessary administrative and technical measures according to the nature of the personal data and the environment in which it is kept.

---

**5.1. Technical Measures**

My Nova Oral and Dental Health Center takes the following technical measures for all environments in which personal data is stored:

- Ensuring network security and application security.
- Implementing key management.
- Taking security measures in the procurement, development, and maintenance of IT systems.
- Creating a permission matrix for employees.
- Ensuring the security of personal data stored in the cloud.
- Keeping access logs regularly.
- Removing access rights of employees who change roles or leave the company.
- Using up-to-date antivirus systems.
- Taking necessary security measures regarding access to physical environments containing personal data.
- Backing up personal data and ensuring the security of the backed-up data.
- Implementing user account management and access control systems and tracking them.
- Keeping log records without user intervention.
- Encrypting sensitive personal data when sent by email via secure methods such as KEP (secure electronic postal service) or corporate email accounts.
- Using secure encryption/cryptographic keys for sensitive personal data, which are managed by different units.
- Implementing cybersecurity measures, continuously monitored and applied.
- Encrypting sensitive personal data transferred via portable storage devices, CDs, and DVDs.

**5.2 Administrative Measures**

My Nova Oral and Dental Health Center implements the following administrative measures for all environments in which personal data is stored, based on the nature of the data and the environment in which it is kept:

- Disciplinary regulations for employees containing provisions on data security.
- Regular training and awareness activities for employees regarding data security.
- Developing and implementing institutional policies on access, information security, usage, storage, and destruction.
- Obtaining confidentiality agreements.
- Contracts signed include provisions on data security.
- Taking additional security measures for personal data transferred by paper, and ensuring that documents are sent in confidentiality-rated formats.
- Establishing personal data security policies and procedures.
- Quickly reporting personal data security issues.
- Monitoring personal data security.
- Ensuring the security of physical environments containing personal data against external risks (fire, flood, etc.).
- Ensuring the security of environments containing personal data.
- Minimizing personal data collection whenever possible.
- Identifying existing risks and threats.
- Establishing and applying protocols and procedures for the security of sensitive personal data.
- Raising awareness of data security among service providers who process data.
- Ensuring the audit of data processing service providers regarding data security.
- Conducting internal periodic and/or random audits.

Here is the English translation of the "Kişisel Verileri İmha Teknikleri" section, covering the Personal Data Destruction Techniques:

---

**PERSONAL DATA DESTRUCTION TECHNIQUES**

My Nova Ağız ve Diş Sağlığı Merkezi, in accordance with the Law and other relevant legislation as well as the Personal Data Processing and Protection Policy, will delete, destroy, or anonymize personal data that it stores when the reasons for processing the data

no longer exist, upon the request of the individual concerned, or within the timeframes specified in this Personal Data Storage and Destruction Policy.

The deletion, destruction, and anonymization techniques used by My Nova Ağız ve Diş Sağlığı Merkezi are listed below:

### 6.1 Deletion Methods

Personal data deletion refers to the process of making personal data inaccessible and unusable for the relevant users in any way.

The personal data can be deleted by using one or more of the methods listed in the table below.

**Deletion Methods for Personal Data Stored in Physical Media**

- **Obscuring**: Personal data in physical environments is deleted using the obscuring method. The process involves either cutting the data from the document when possible or, when not possible, making it unreadable by applying indelible ink, ensuring that it cannot be restored or read by technological solutions.

**Deletion Methods for Personal Data Stored in Cloud and Local Digital Environments/Software**

- **Secure Deletion from Software**: Personal data stored in cloud or local digital environments is deleted digitally in a way that makes it inaccessible and unusable for anyone except the database administrator once the retention period has ended.

**Deletion Methods for Personal Data on Servers**

- **Deleting by Removing Access Permission**: For personal data on servers that no longer require storage, the system administrator removes access permissions for the relevant users, and the data is then deleted.