OP. DR. NİYAZİ ALTINTOPRAK

PERSONAL DATA STORAGE AND DISPOSAL POLICY

1. PURPOSE

Op. Dr. Niyazi Atıntoprak **("Niyazi Altıntoprak")** is issued with this Personal Data Storage and Destruction Policy **("Storage and Destruction Policy")** in order to regulate the technical and administrative protection of personal data in accordance with the Personal Data Protection Law No. 6698 **("Law")**, and to regulate the implementation of the provisions of the Regulation on Deletion, Destruction or Anonymization of Personal Data **("Regulation")** published in the Official Gazette dated 28/10/2017 in case the conditions for processing personal data disappear.

2. MEDIA WHERE PERSONAL DATA ARE STORED

Personal data belonging to data subjects are securely stored by Niyazi Altıntoprak in the environments listed below in accordance with the relevant legislation, especially the provisions of the Law:

Electronic media

- E-Mail Box
- Microsoft Office Programs

Physical environments:

- Unit Cabinets
- Folders
- Archive

3. EXPLANATIONS ON THE REASONS FOR STORAGE

Personal data of data subjects, in particular:

a. Execution of emergency management processes,
b. Execution of information security processes,
c. Carrying out the application processes of employee candidates,
d. Fulfillment of employment contractual and regulatory obligations for employees,
e. Execution of fringe benefits and benefits processes for employees,
f. Conducting training activities,
g. Execution of access authorizations,
h. Execution of activities in accordance with the legislation,
i. Conducting financial and accounting affairs,
j. Ensuring physical space security,
k. Execution of assignment processes,
l. Follow-up and execution of legal affairs,
m. Conducting communication activities,
n. Execution/supervision of business activities,
o. Conducting occupational health/safety activities,
p. Conducting business continuity activities,
q. Execution of goods / service procurement processes,
r. Execution of risk management processes,
s. Carrying out storage and archive activities,
t. Execution of contract processes,
u. Execution of the remuneration policy,
v. Ensuring the security of data controller operations,
w. Providing information to authorized persons, institutions and organizations,
x. Fulfillment of legal obligations,

y. Provision of health services,
z. Creation and follow-up of appointment records,
aa. Prescription issuance,
bb. Conducting activities related to patient satisfaction,
cc. Providing support and information after health care,

… is stored securely in the aforementioned physical or electronic media within the limits specified in the Law and other relevant legislation by Niyazi Altintoprak.

Reasons for storage:

a. Personal data is directly related to the establishment and performance of contracts,

b. The establishment, exercise or protection of a right,

c. Provided that personal data does not harm the fundamental rights and freedoms of individuals, Niyazi Altıntoprak has a legitimate interest,

d. Fulfillment of any legal obligation of Niyazi Altıntoprak of personal data,

e. The legislation clearly stipulates the retention of personal data,

f. Explicit consent of data subjects in terms of storage activities that require the explicit consent of data subjects.

Pursuant to the Regulation, in the cases listed below, personal data belonging to data subjects shall be deleted, destroyed or anonymized by Niyazi Altıntoprak ex officio or upon request:

a. Amendment or abolition of the provisions of the relevant legislation that constitute the basis for the processing or storage of personal data,
b. The purpose requiring the processing or storage of personal data disappears,
c. The disappearance of the conditions requiring the processing of personal data under Articles 5 and 6 of the Law,
d. In cases where the processing of personal data takes place only on the basis of explicit consent, the data subject's withdrawal of consent,
e. Acceptance by the data controller of the application made by the data subject for the deletion, destruction or anonymization of his/her personal data within the framework of his/her rights under paragraphs 2 (e) and (f) of Article 11 of the Law,
f. In cases where the data controller rejects the application made by the data subject with the request for the deletion, destruction or anonymization of his/her personal data, his/her response is found insufficient or he/she does not respond within the period stipulated in the Law; a complaint is filed to the Board and this request is approved by the Board,
g. Although the maximum period of time required for the retention of personal data has elapsed, there are no circumstances justifying the retention of personal data for a longer period of time.

4. PRECAUTIONS TAKEN FOR THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the Law, Niyazi Altıntoprak takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent unlawful processing of the personal data it processes, to prevent unlawful access to the data and to ensure the preservation of the data, and to carry out or have the necessary audits carried out within this scope. In the event that the processed personal data is obtained by third parties illegally, although all technical and administrative measures have been taken, Niyazi Altıntoprak notifies the relevant units as soon as possible.

4.1. Technical Precautions:

- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- There are disciplinary regulations that include data security provisions for employees.
- Training and awareness raising activities on data security are carried out for employees at regular intervals.
- An authorization matrix has been established for employees.
- Access logs are kept regularly.
- Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
- Confidentiality undertakings are made.
- The authorizations of employees who change their duties or leave their jobs in this area are removed.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- Signed contracts contain data security provisions.
- Personal data security policies and procedures are defined.
- Personal data security issues are reported quickly.
- Personal data security is monitored.
- Necessary security measures are taken for entry and exit to physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (fire, flood, etc.).
- Security of environments containing personal data is ensured.
- Personal data is minimized as much as possible.
- Personal data is backed up and the security of backed up personal data is also ensured.
- User account management and authorization control system is implemented and monitored.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- Cyber security measures have been taken and their implementation is constantly monitored.
- Encryption is performed.
- Awareness of data processing service providers on data security is ensured.

4.2 Administrative Precautions:

- Employees are trained on the technical measures to be taken to prevent unlawful access to personal data.
- Access to personal data and authorization processes are designed and implemented within Niyazi Altıntoprak in accordance with the legal compliance requirements for processing personal data on a business unit basis. In limiting access, whether the data is of special nature or not and the degree of importance are also taken into consideration.
- Niyazi Altıntoprak has added records to all kinds of documents that regulate the relationship between Niyazi Altıntoprak and its personnel and contain personal data, stating that the obligations stipulated by the Law must be complied with in order to process personal data in accordance with the law, personal data must not be disclosed, personal data must not be used unlawfully and the confidentiality obligation regarding personal data continues even after the

termination of the employment contract with Niyazi Altıntoprak.

- Employees are informed that they cannot disclose the personal data they have learned to anyone else in violation of the provisions of the Law and cannot use it for purposes other than processing and that this obligation will continue after their resignation and necessary commitments are obtained from them in this direction.
- In the contracts concluded by Niyazi Altıntoprak with the persons to whom personal data are transferred in accordance with the law; provisions are added that the persons to whom personal data are transferred will take the necessary security measures to protect personal data and ensure that these measures are complied with in their own organizations.
- In the event that the processed personal data is obtained by others through unlawful means, it shall notify the relevant person and the Board as soon as possible.
- When necessary, it shall employ personnel who are knowledgeable and experienced in the processing of personal data and shall provide its personnel with training on personal data protection legislation and data security.
- Niyazi Altıntoprak shall conduct and have conducted the necessary audits to ensure the implementation of the provisions of the Law. It eliminates the privacy and security weaknesses that arise as a result of the audits.

5. PRECAUTIONS TAKEN REGARDING THE DESTRUCTION OF PERSONAL DATA

Although Niyazi Altıntoprak proceeds in accordance with the provisions of the relevant law, he may delete or destroy personal data based on his own decision or upon the request of the personal data owner in the event that the reasons requiring its processing disappear. Following the deletion of personal data, the relevant persons will not be able to access and use the deleted data again in any way. An effective data tracking process will be managed by Niyazi Altıntoprak regarding the identification and tracking of personal data destruction processes.
The process carried out will be the identification of the data to be deleted, the identification of the relevant persons, the identification of the access methods of the persons and the deletion of the data immediately afterwards.

Niyazi Altıntoprak may use one or more of the following methods to destroy, delete or anonymize personal data, depending on the medium in which the data is recorded:

Methods for Deletion, Destruction and Anonymization of Personal Data

5.1 Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users. As a method of deleting personal data, Niyazi Altıntoprak may use one or more of the following methods:

- Personal data on paper media will be processed by drawing, painting, cutting or erasing with the blackout method.
- The access right(s) of the user(s) for office files in the central file will be eliminated.
- The rows or columns containing personal information in the databases will be deleted with the 'Delete' command.
- When necessary, they will be securely deleted with the help of an expert.

5.2 Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and

unusable by anyone in any way.

- Physical Destruction
- Destruction with Paper Shredder
- De-magnetization: It is the method of passing magnetic media through special devices where it will be exposed to high magnetic fields, distorting the data on it in an unreadable way.

5.3 Anonymizing Personal Data

Anonymization of personal data means that personal data cannot be associated with an identified or identifiable natural person under any circumstances, even by matching it with other data. Niyazi Altıntoprak may use one or more of the following methods to anonymize personal data:

- **Masking:** Data masking is a method of anonymizing personal data by removing the basic identifying information of personal data from the data set.

- **Record Extraction:** In the de-recording method, the stored data is anonymized by removing the row of data that contains a singularity among the data from the records.

- **Regional Concealment :** In the regional hiding method, anonymization is achieved by hiding the relevant data if it is decisive because a single data creates a combination that is barely visible.

- **Global Coding:** With the data derivation method, a more general content is created from the content of the personal data and it is ensured that the personal data cannot be associated with any person. For example; specifying ages instead of dates of birth; specifying the region of residence instead of the street address.

- **Noise Insertion:** The method of adding noise to the data, especially in a data set where numerical data is predominant, anonymizes the data by adding some deviations in the plus or minus direction to the existing data at a determined rate. For example, in a data set with weight values, a deviation of (+/-) 3 kg is used to prevent the display of real values and anonymize the data. The bias is applied equally to each value.

In accordance with Article 28 of the Law; anonymized personal data may be processed for purposes such as research, planning and statistics. Such processing is outside the scope of the Law and the explicit consent of the personal data owner will not be sought.

Niyazi Altıntoprak will be able to take an ex officio decision regarding the deletion, destruction or anonymization of personal data and will be able to freely determine the method to be used according to the category he has chosen. In addition, within the scope of Article 13 of the Regulation, if the person concerned chooses one of the categories of deletion, destruction or anonymization of his personal data during the application, Niyazi Altıntoprak will be at liberty regarding the methods to be used in the relevant category.

6. PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

Niyazi Altıntoprak retains personal data for the purpose for which they are processed for the periods

specified in Annex-1 of the **Personal Data Storage and Destruction Policy**.

If a period of time is stipulated in the legislation regarding the storage of the personal data in question, this period shall be respected. In the absence of a period stipulated in the legislation, personal data will be kept for the maximum period for keeping personal data in the table in Annex 1. These periods are determined by evaluating Niyazi Altıntoprak's data categories and data owner person groups, ensuring that the data obtained as a result of this evaluation will ensure the fulfillment of the obligations stipulated in the laws and considering the maximum statute of limitations (10 years) in the Turkish Code of Obligations.

In the event that the obligation to delete, destroy or anonymize arises due to the expiration of these periods, Niyazi Altıntoprak deletes, destroys or anonymizes personal data in the first periodic destruction process following this date.

All transactions regarding the deletion, destruction and anonymization of personal data are recorded and such records are kept for at least three years, excluding other legal obligations.

7. COMPANY PERIODIC DESTRUCTION PERIODS

Niyazi Altıntoprak's periodic destruction period is 6 months. Personal data whose retention period has expired shall be destroyed in accordance with the procedures set out in this Personal Data Storage and Destruction Policy in June and December in 6-month periods within the framework of the destruction periods in Annex-1 of this Personal Data Storage and Destruction Policy. In the systems in question, the information will be deleted from the tools such as documents, files, CDs, diskettes, hard disks, if any, where the data is saved, in a way that cannot be recycled.

8. STAFF

Within the scope of the Law, Niyazi Altıntoprak as the data controller, based on paragraph 1 of Article 11 of the Regulation, the obligations of the Law in terms of the implementation of the data retention and destruction process will be fulfilled by the assigned personnel, or by the Examining Physician in case there is no personnel during the destruction period.

These persons whose boundaries have been determined are responsible for the transactions and actions that take place within their limits of authority within the scope of the Turkish Commercial Code, the Code of Obligations and the Turkish Penal Code. Niyazi Altıntoprak's Physician is authorized to represent Niyazi Altıntoprak in law enforcement, prosecution offices, public institutions and courts and to make statements.

9. REVISION AND REPEAL

In case the Personal Data Storage and Destruction Policy is amended or repealed, the new regulation will be announced on the Niyazi Altıntoprak website.

10. ENFORCEMENT

This Personal Data Storage and Destruction Policy enters into force on the date of its publication.

APPENDICES
Annex 1 - Personal Data Storage And Destruction Periods

Annex 1 - Personal Data Storage And Destruction Periods

Data Category	Storage Time	Destruction Period
Identity	10 Years	At the first periodic destruction following the end of the storage period
Contact	10 Years	At the first periodic destruction following the end of the storage period
Personnel	10 Years	At the first periodic destruction following the end of the storage period
Legal Action	10 Years	At the first periodic destruction following the end of the storage period
Patient Process	10 Years	At the first periodic destruction following the end of the storage period
Process Security	10 Years	At the first periodic destruction following the end of the storage period
Risk Management	10 Years	At the first periodic destruction following the end of the storage period
Finance	10 Years	At the first periodic destruction following the end of the storage period
Professional Experience	10 Years	At the first periodic destruction following the end of the storage period
Audio and Visual Recordings	10 Years	At the first periodic destruction following the end of the storage period
Health Information	15 Years	At the first periodic destruction following the end of the storage period
Criminal Conviction and Security Measures	10 Years	At the first periodic destruction following the end of the storage period
Genetic Data	10 Years	At the first periodic destruction following the end of the storage period
Family Information	10 Years	At the first periodic destruction following the end of the storage period
Operation Data	10 Years	At the first periodic destruction following the end of the storage period
Website Usage Data	2 Years	At the first periodic destruction following the end of the storage period
Request/Complaint Management Information	2 Years	At the first periodic destruction following the end of the storage period
Health Financing and Planning Information	10 Years	At the first periodic destruction following the end of the storage period
Audit and Inspection Information	10 Years	At the first periodic destruction following the end of the storage period
Procurement Process	10 Years	At the first periodic destruction following the end of the storage period
Forensic Case Information	10 Years	At the first periodic destruction following the end of the storage period