Buse Çolpan

Oral and Dental Health Polyclinic

BUSE ÇOLPAN ÖZEL SAĞLIK HİZMELERİ SANAYİ ve TİCARET LİMİTED ŞİRKETİ

PERSONAL DATA STORAGE, DESTRUCTION AND CONFIDENTIALITY POLICY

1. NATURE AND PURPOSE OF THE POLICY

This Personal Data Storage and Destruction Policy (hereinafter referred to as the "Policy") has been prepared by Buse Çolpan Özel Sağlık Hiz. San.Ve Tic. Ltd. Şti. (hereinafter referred to as the "Clinic") in its capacity as data controller in order to determine the procedures and principles to be applied by the Clinic regarding the deletion, destruction and anonymisation of personal data in accordance with the Personal Data Protection Law No. 6698 ("KVKK") and other legislation.

This Policy covers all departments, employees, employee candidates, customers and third parties involved in any process in which the Clinic processes Personal Data.

2. DEFINITIONS

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

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

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

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

Service Provider: A natural or legal person who provides services under a specific contract with the Personal Data Protection Authority.

Contact Person: The natural person whose personal data is processed.

Related User: Persons who process personal data within the organisation of the data controller or in accordance with the authority and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and backup of the data.

Disposal: Deletion, disposal or anonymisation of personal data.

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

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

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

Personal Data Processing Inventory: Inventory in which data controllers detail the personal data processing activities they carry out depending on their business processes by associating them with the purposes and legal grounds for processing personal data, the data category, the group of recipients transferred and the group of data subjects, and by explaining the maximum retention period required for the purposes for which personal data are processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security.

Processing of Personal Data: All kinds of operations performed on personal data such as obtaining, recording, storing, storing, changing, rearranging, 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 they are part of any data recording system.

The Board: Personal Data Protection Board

Personal Data Protection Committee: The committee formed by the relevant persons within the company and under the chairmanship of the Data Controller. It is authorised and tasked to carry out the necessary procedures for the storage, destruction and processing of Personal Data in accordance with the law, the Personal Data Storage and Destruction Policy and the Personal Data Inventory and to supervise the processes.

Sensitive Personal Data: Data on 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, and biometric and genetic data.
Periodic Disposal: In the event that all of the conditions for processing personal data specified in the law disappear, the deletion, disposal or anonymisation process to be carried out ex officio at recurring intervals specified in the personal data retention and destruction policy.
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 transactions related to the Registry.
Data Controller: Data controller refers to the 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.
VERBİS: Data Controllers Registry Information System

3. PRINCIPLES

The Clinic acts with the following principles in the storage and destruction of personal data within the framework of the Law and this policy.

a) In the storage, deletion, destruction and anonymisation of personal data, the principles listed in Article 4 of the Law and the measures to be taken within the scope of Article 12 of the Law, relevant legislation and Board decisions and this policy text are acted in accordance with.
b) All transactions regarding the deletion, destruction, anonymisation of personal data are recorded by the Clinic within the framework of the provisions of the Law, the relevant legislation and this policy, and such records are kept for 3 years in accordance with Article 7/3 of the Regulation, excluding other legal obligations.
c) Unless otherwise decided by the Board, the appropriate method of deletion, destruction or anonymisation of personal data is chosen by the Clinic.
d) In the event that all of the conditions for the processing of personal data specified in the Law disappear, personal data are deleted, destroyed or anonymised by the Clinic or upon the request of the data subject.

4. PRECAUTIONS

The Clinic takes all necessary technical and administrative measures in accordance with the nature of the relevant personal data and the environment in which the data is stored and maintained in order to store personal data securely and to prevent unlawful processing and access.

4.1. Technical Measures

The clinic takes the following appropriate technical measures:

- It uses secure systems in accordance with technological developments
- It uses security systems according to the environments where personal data is kept
- Access to the media where personal data is stored is restricted and only authorised persons are allowed access to this data limited to the purpose for which the personal data is stored (Data Controller and Personal Data Protection Committee and other personnel designated by the data controller)
- It has sufficient number of personnel to ensure the security of the environments/systems where personal data are located
- It uses authorisation matrix, authorisation control, access logs, encryption, firewall, penetration test and log records measures in the systems where personal data are processed.

4.2. Administrative Measures

The Clinic takes the following appropriate administrative measures:

- Efforts are being made to raise awareness and raise awareness of all Clinic employees who have access to personal data on information security, personal data and privacy.
- In order to follow the developments in the field of protection of personal data and to take necessary measures, internal and external and internal and external audits will be carried out.
- In case personal data are transferred to third parties in case of necessity, protocols are signed with the relevant third parties for the protection of personal data and all necessary care is taken to ensure that these third parties comply with their obligations in these protocols.
- Clarification and consent texts have been prepared and signed by all personal data subjects.

- Confidentiality Undertakings have been prepared and signed.
- Personal Data Processing Inventory has been prepared.
- This Retention and Destruction Policy has been prepared and published.
- Data Breach Policy has been prepared.

4.3. Internal Audit

In accordance with Article 12 of the Law, obligations regarding data security, internal audits are carried out immediately or in any case in 6-month periods regarding the implementation of the provisions of the Law and the provisions of this Policy, if an update is required.

These audits are carried out by the Data Controller and the Personal Data Protection Committee, and if a deficiency or defect regarding the obligations and/or a violation of the provisions of the law is detected as a result of these audits, this deficiency or defect shall be corrected immediately.

In the event that it is understood during the audit or otherwise that the personal data under the responsibility of the Clinic has been obtained by others illegally, this situation shall be notified by the Clinic to the relevant person and the Personal Data Protection Board as soon as possible.

5. RECORDING MEDIA

With this Policy, the Clinic agrees to include Personal Data in the scope of the Policy in the following environments containing Personal Data and in other environments that may arise in addition to these:

- Computers/servers/systems allocated by the Clinic and/or used on behalf of the Clinic
- Network devices
- Shared/unshared disc drives used for data storage on the network
- Cloud Systems
- Mobile phones and all storage areas
- Paper
- Peripherals such as printer, fingerprint reader
- Optical discs
- Archive
- Flash memories
- Camera recordings

6. DESTRUCTION OF PERSONAL DATA

6.1. Reasons for Storage and Destruction

In the event that all of the conditions for processing personal data specified in Articles 5 and 6 of the Law are no longer applicable, personal data are deleted, destroyed or anonymised by the Clinic ex officio or upon the request of the data subject.

The reasons listed in Articles 5 and 6 of the Law are as follows:

- Explicitly stipulated in the law
- It is necessary for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid.
- Provided that it is directly related to the establishment or performance of a contract, it is necessary to process personal data belonging to the parties to the contract.
- It is mandatory for the data controller to fulfil its legal obligation.
- It has been made public by the data subject himself/herself.
- Data processing is mandatory for the establishment, exercise or protection of a right.

6.2. Disposal Methods

The Clinic will store the personal data obtained in accordance with the KVKK and the relevant legislation within the scope of this Policy. However, in the event that the reasons requiring the processing of Personal Data listed in the Law and Regulation disappear or upon the request of the data subject, it is deleted, destroyed or anonymised ex officio with the techniques specified below within the periods determined by the Law, the relevant legislation and this Policy. The deletion, destruction and anonymisation techniques used by the Clinic are as follows:

6.2.1. Deletion Methods

- Deletion methods for personal data stored in cloud and local digital media consist of secure deletion from software. When deleting the data, which are processed in whole or in part automatically and stored in digital media, methods are used to ensure that the relevant users cannot access and reuse them in any way. In short, personal data stored in the cloud or local digital environments are deleted by digital command in such a way that they cannot be recovered again and the data deleted in this way cannot be accessed again.

  However, if the deletion of personal data will result in the inability to access and use other data as a result of deletion of personal data, personal data will also be deemed to be deleted if the personal data is archived by making it unrelated to the person if the following conditions are met.

- The method of erasing personal data in paper media is blackout. Personal data in printed media are erased using the blackout method. Blackout is a method of preventing misuse, removing the personal data on the relevant document from the document by physically cutting it out of the document where possible, and making it invisible/covering it by using fixed ink in a way that cannot be reversed and cannot be read with technological solutions.

6.2.2. Destruction Methods

In order to destroy personal data kept in printed form, it is necessary to physically destroy it in such a way that it cannot be reassembled with document shredders.

The methods that can be used to destroy personal data kept in digital and cloud environment are as follows:

Physical disposal: This method consists of physical disposal, such as melting, incineration or pulverisation of the optical and magnetic media containing the personal data. Melting, burning, pulverising or passing the media in question through a metal grinder renders the personal data inaccessible.

De-magnetisation: It is a method of distorting the magnetic media by exposing it to higher magnetic fields and passing it through special devices so that the data on it cannot be read. However, if this method fails and the data on the media is still readable, the media can be physically destroyed and the destruction process is completed.

Overwriting: This method is a data destruction method that makes it impossible to read and recover old data by writing random data consisting of 0s and 1s at least seven times on magnetic media and rewritable optical media by means of special software.

Secure deletion from software: In this method, personal data is deleted by digital command so that it cannot be recovered again.

6.2.3. Anonymisation

Anonymisation is the process of making personal data impossible to be associated with a specific or identifiable natural person under any circumstances, even by matching them with other data.

The procedures and principles regarding the Clinic's anonymisation techniques of personal data are listed below:

- With the method of removing variables, the existing data set is anonymised by removing the "highly descriptive" ones from the variables in the data set created after the data collected with the method of descriptive data are brought together. For example, anonymisation can be achieved by removing the data groups that are highly descriptive of personal data from the environment (documents, tables, etc.) where personal data are available.
- In the regional hiding method, it is the process of deleting the information that may be distinctive for the data that is in an exceptional situation in the data table where personal data are collectively anonymised.
- With the lower and upper limit coding method, ranges for a certain variable are defined and categorised. For example, the personnel working in a workplace can be anonymised by combining them as 'very experienced', 'experienced' or 'inexperienced' according to whether their working years in the workplace are less than 5 years, between 5 and 10 years or more than 10 years.
- Generalisation is the process of bringing together personal data belonging to many people and turning them into statistical data by removing distinguishing information.
- With the data mixing and distortion method, direct or indirect identifiers in personal data are compared or distorted with other values and their relationship with the person concerned is severed and they lose their identifying characteristics.

6.3. Storage Periods

Physical and digital data that have completed the legal retention and destruction periods specified in the Clinic, Personal Data Inventory, this Policy and the relevant legislation are periodically destroyed. The Clinic deletes, destroys or anonymises personal data in the first periodic destruction process following the date on which the obligation to delete, destroy or anonymise the personal data for which it is responsible in accordance with the Personal Data Inventory, the Law, the relevant legislation and this Policy arises.

DATA OWNER	DATA CATEGORY	STORAGE TIME
Employee	Social Security Institution with recruitment documents personal data on the basis of notifications on length of service and remuneration	It shall be retained for the continuation of the service contract and for 10 years after its expiry
Employee	Data in the workplace personal health file	It shall be retained for the continuation of the service contract and for 10 years after its expiry
Employee Candidate	Personal health data in the job application form	It is kept for 5 years from the receipt of the application.
Employee Candidate	The information contained in the CV and job application form of the employee candidate	It is kept for 5 years from the receipt of the application.
Employee	Criminal conviction, personal data relating to lawsuits filed by the employee against the company or by the company against the employee	It is kept for 10 years from the date of termination of the employee's employment contract.
Employee	Personal data received for the fulfilment of the activity/work (visa, hotel, contract, etc.)	It is kept for 10 years from the termination of the employee's employment contract.
Visitor	Visitor's name, surname, Turkish ID number, camera footage taken at the entrance to the building belonging to the Clinic, telephone audio recordings taken during searches	Stored for 3 months
Patient/Patient Relative	Personal data such as name, surname, Turkish ID., contact information, identity information obtained with the registration form of the patient and special quality data such as laboratory analysis results, medical anamnesis results, medication information used	It is kept for 10 years from the end of the service contract with the patient.
Patient	Patient's name, surname, Turkish ID number, contact information, payment information and methods, voice recordings of telephone calls, patient requests and complaints, transaction history, electronic correspondence, signature declaration information	From the presentation of each product / service purchased by the Customer, the Turkish Code of Obligations. 146 and Article 82 of the Turkish Commercial Code for a period of 10 years

Patient/Patient Relative	CCTV footage and patient/caretaker information taken at the entrance to the Clinic's building	Stored for 3 months
Institutions/Companies with which the Clinic is in co-operation (Suppliers, companies that provide medical support and materials, etc.)	Identity information, contact information, financial information, voice recordings received in telephone calls, Institution/Firm employee data regarding the execution of commercial and service relations between the Clinic and the Institutions/Firms with which the Clinic cooperates	The business/commercial relationship of the Institutions/Firms with which the Clinic is in cooperation with the Clinic shall be kept for 10 years during and after the termination of the business/commercial relationship with the Clinic.
Operations of the Board of Shareholders	Identity information obtained during the Board of Shareholders procedures, personal data information in electronic correspondence, telephone audio recordings taken during calls, data on the members of the Board	Stored for 10 years

6.4. Disposal Periods

The Clinic deletes, destroys or anonymises personal data in the periodic destruction process following the date on which the obligation to delete, destroy or anonymise the personal data for which it is responsible in accordance with the Personal Data Inventory, the Law, the relevant legislation and this Policy arises.

The person whose personal data is processed may request the deletion or destruction of his/her personal data by applying to the Clinic in accordance with Article 13 of the Law.

If the data subject makes such a request and all of the conditions for processing personal data have been eliminated, the Clinic will delete, destroy or anonymise the personal data within 30 days from the day of receipt of the request by explaining the justification by appropriate destruction method. However, if all of the conditions for processing personal data have not been eliminated, this request may be rejected by the Clinic by explaining the reason in accordance with the third paragraph of Article 13 of the Law and the rejection response will be notified to the data subject in writing or electronically within 30 days at the latest.

The Clinic deletes, destroys or anonymises personal data for which the conditions for clinical processing have been eliminated by a process specified in this Policy and which will take place ex officio at recurring intervals. Periodic destruction processes start for the first time on 31 January 2021 and repeat every 6 (six) months.

7. CONFIDENTIALITY POLICY

The Clinic informs that it will keep Personal Data within the Clinic in line with the purposes of its activities and for the period required for the fulfilment of this purpose and during the continuation of the commercial relationship with the business partner / supplier / consultant / auditor or third party and / or limited to the period specified in the legislation, and that it may transfer Personal Data to third parties if it uses the services of third party providers for the fulfilment of the said purpose, but in this case, it will ensure that such third parties comply with the provisions of the Law.

The Clinic is obliged to take technical and administrative measures in accordance with the Law and Regulation in order to prevent unauthorised access to Personal Data by its personnel or third parties and the use of Personal Data for purposes other than the purpose of transferring Personal Data.

8) EFFECTIVENESS

This Policy shall enter into force as of the date of its publication.

A Personal Data Protection Committee has been established within the Clinic in order to monitor and manage the necessary actions for compliance with the Law.

Office Management consists of at least two (2) people, including physicians, employees to be selected from the Accounting and Finance Department and the Human Resources Department.