PERSONAL DATA AND SPECIAL CATEGORY PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. INTRODUCTION

1.1 Purpose

This Personal Data Retention and Destruction Policy ("Policy") has been prepared by **Op. Dr. Kemal Uslu Private Practice ("Practice")** to determine the procedures and principles regarding the retention and destruction activities carried out within the Practice.

The Practice has adopted as a priority to process the personal data of its employees, job applicants, patients, suppliers, service providers, visitors and other third parties in compliance with the Constitution of the Republic of Türkiye, international agreements, the Turkish Personal Data Protection Law No. 6698 ("Law") and all other relevant legislation, and to ensure that data subjects can effectively exercise their rights. All procedures and actions relating to the retention and destruction of personal data are carried out in accordance with this Policy.

1.2 Scope

The personal data of the Practice's employees, job applicants, patients, suppliers, service providers, visitors and other third parties are within the scope of this Policy. This Policy applies to all recording media owned by or managed by the Practice where personal data are processed, and to all activities aimed at personal data processing.

1.3 Abbreviations and Definitions

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

Explicit Consent: Consent that is freely given, specific and informed, relating to a particular subject.

Anonymization: Rendering personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data.

Employee: The personnel of Op. Dr. Kemal Uslu Private Practice.

Patient: A person receiving health and medical diagnosis, treatment and care services from Op. Dr. Kemal Uslu Private Practice.

Electronic Media: Media in which personal data can be created, read, modified and written through electronic devices.

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

Service Provider: A natural or legal person providing services to the Practice under a specific contract (e.g., IT services, software/CRM services, web hosting, accounting, legal

consultancy, advisory services, security, cargo/logistics, call center, marketing/agency services, etc.).

Data Subject: The natural person whose personal data are processed.

Authorized User: Persons who process personal data within the data controller's organization or under the authority and instructions received from the data controller, excluding the person/unit responsible for technical storage, protection and backup of the data.

Destruction: Deletion, destruction or anonymization of personal data.

Law: Turkish Personal Data Protection Law No. 6698.

Recording Media: Any media in which personal data are processed wholly or partially automatically, or non-automatically provided that they form part of a data recording system.

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

Personal Data Processing Inventory: An inventory in which data controllers detail their personal data processing activities based on business processes by linking processing purposes and legal grounds, data categories, recipient groups and data subject groups, and by explaining maximum retention periods required for the purposes of processing, any planned cross-border data transfers, and the data security measures taken.

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

Special Category Personal Data: Data regarding a person's 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.

Periodic Destruction: The deletion, destruction or anonymization process to be carried out ex officio at recurring intervals specified in the retention and destruction policy when all processing conditions under the Law cease to exist.

Policy: Personal Data Retention and Destruction Policy.

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

Data Recording System: A recording system in which personal data are structured and processed according to specific criteria.

Data Controller: The natural or legal person who determines the purposes and means of processing personal data and who is responsible for establishing and managing the data recording system.

Data Controllers' Registry Information System: The information system created and managed by the Presidency and accessible online, used by data controllers for application to the Registry and other related procedures.

VERBIS: Data Controllers' Registry Information System.

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

(ANNEX – Data Controller Contact Details): The data controller within the scope of this Policy is **Op. Dr. Kemal Uslu Private Practice**. For applications and all questions/communications under this Policy:
E-mail: **info@drkemaluslu.com** / Phone: **+90 552 567 31 15** / Address: **Nişantaşı, Meşrutiyet Mah. Valikonağı Cad., Alp Palas No:12, Şişli/İstanbul**

---

2. RESPONSIBILITIES AND DUTY ALLOCATIONS

All units and employees of the Practice actively support responsible units in implementing technical and administrative measures taken under this Policy, increasing training and awareness of unit employees, monitoring and continuous auditing, preventing unlawful processing of personal data, preventing unlawful access to personal data, and ensuring lawful retention of personal data by taking technical and administrative measures for data security in all environments where personal data are processed. The distribution of titles, units and job descriptions of those involved in retention and destruction processes is provided in Table 1.

Table 1: Duty allocation for retention and destruction processes

TITLE — DUTY
Data Manager: Responsible for ensuring employees act in compliance with the Policy.
Data Manager: Responsible for preparing, developing, executing, publishing and updating the Policy in relevant environments, and for its cancellation by the Practice decision and retention/archiving.
Data Security Officer: Responsible for providing the technical solutions required for implementation of the Policy and for executing destruction processes.
Other Units: Responsible for execution of the Policy in line with their duties and the roles defined under internal instructions.

---

3. RECORDING MEDIA

Personal data are lawfully and securely stored by the Practice in the media listed below.

Table 2: Personal data storage media

Electronic Media:
Servers (domain, backup, e-mail, database, web, file sharing, etc.), software (office software, portal, EBYS, VERBIS), information security devices (firewalls, intrusion detection and

prevention, log files, antivirus, etc.), personal computers (desktop, laptop), mobile devices (phone, tablet, etc.), optical discs (CD, DVD, etc.), removable media (USB, memory cards, etc.), printers, scanners, photocopiers.

Non-Electronic Media:
Paper, manual data recording systems (survey forms, visitor logbook), written, printed and visual media.

---

4. EXPLANATIONS ON RETENTION AND DESTRUCTION

Personal data of employees, job applicants, patients, suppliers, visitors and employees of third parties (institutions/organizations) with whom the Practice has service provider relationships are retained and destroyed in compliance with the Law. Detailed explanations regarding retention and destruction are provided below.

4.1 Explanations on Retention

Article 3 of the Law defines the concept of processing of personal data; Article 4 states that processed personal data must be relevant, 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; Articles 5 and 6 list the conditions for processing personal data. Accordingly, personal data are retained within the scope of the Practice's activities for the period stipulated in the relevant legislation or appropriate to the purposes of processing.

4.1.1 Legal Grounds Requiring Retention

Personal data processed within the scope of the Practice's activities are retained for the period stipulated in the relevant legislation. In this context, personal data are retained pursuant to, among others:

Law No. 6698 on Protection of Personal Data,
Law No. 5651,
Turkish Code of Obligations No. 6098,
Turkish Commercial Code No. 6102,
Law No. 6563,
Private Health Insurance regulations and related legislation,
Regulation on Patients' Rights and related legislation,
Deontology Regulation,
Social Insurances and General Health Insurance Law No. 5510 and insurance legislation,
Occupational Health and Safety Law No. 6331,
Right to Information Law No. 4982,
Law on the Exercise of the Right to Petition No. 3071,
Labor Law No. 4857,
Retirement Health Law No. 5434,
Social Services Law No. 2828,
Regulation on Occupational Health and Safety Measures in Workplace Buildings and Annexes,

Regulation on Archive Services,
and other secondary legislation in force under these laws, for the retention periods prescribed therein.

4.1.2 Processing Purposes Requiring Retention

The Practice retains personal data processed within the scope of its activities for the following purposes:

Providing health services,
Billing procedures,
Conducting human resources processes,
Ensuring corporate communication,
Ensuring the Practice's security and audit,
Ensuring data security,
Ensuring physical security of the Practice's premises,
Staff training,
Performing transactions and operations arising from signed contracts and protocols,
Within the scope of VERBIS, identifying preferences and needs of employees, data controllers, contact persons, data controller representatives and data processors, arranging services accordingly and updating them when necessary,
Fulfilling legal obligations as required or mandated by legal regulations,
Maintaining communication with natural/legal persons having a business relationship with the Practice,
Informative activities on social media accounts,
Sending SMS and electronic communications and responding to questions and complaints within the scope of health services,
Receiving accounting and legal consultancy services,
Serving as evidence in potential future legal disputes.

4.2 Reasons Requiring Destruction

Personal data are deleted, destroyed or anonymized upon the occurrence of any of the following:

Amendment or repeal of relevant legislative provisions forming the basis for processing,
Disappearance of the purpose requiring processing or retention,
Withdrawal of explicit consent in cases where processing relies solely on explicit consent,
Acceptance by the Practice of the data subject's application for deletion/destruction,
Rejection by the Practice of the data subject's application for deletion/destruction/anonymization, finding the response insufficient, or failure to respond within the period stipulated by the Law; and the data subject's complaint to the Personal Data Protection Authority and acceptance of the request by the Authority,
Expiry of the maximum retention period and absence of any condition justifying longer retention.

---

5. TECHNICAL AND ADMINISTRATIVE MEASURES

In order to securely retain personal data, prevent unlawful processing and access, and lawfully destroy personal data, the Practice takes technical and administrative measures in line with Article 12 of the Law and, for special category personal data, the adequate measures determined and announced by the Board pursuant to Article 6/4.

5.1 Technical Measures

The technical measures taken by the Practice include:

Penetration tests to identify risks, threats, vulnerabilities and any gaps in the Practice's information systems and taking necessary precautions,
Continuous monitoring of risks and threats that may affect continuity of information systems through real-time analyses within information security incident management,
Taking necessary measures for physical security of information systems hardware, software and data,
Taking hardware measures (access control to system room, 24/7 monitoring system, physical security of network switches, fire suppression system, air conditioning, keeping keys of physical environments where data are located such as archives/accounting/patient files only with authorized persons, etc.) and software measures (firewalls, attack prevention systems, antivirus software, log monitoring systems, network access control, malware prevention systems, etc.) against environmental threats,
Identifying risks to prevent unlawful processing and ensuring appropriate technical measures and technical controls, and receiving regular IT support,
Creating access procedures within the Practice and performing reporting and analysis regarding access to personal data,
Recording access to storage areas where personal data are kept and controlling unauthorized access or attempts,
Taking necessary measures to ensure that deleted data are inaccessible and unrecoverable for authorized users,
Establishing a system and infrastructure to notify the data subject and the Board in case personal data are unlawfully obtained by others,
Following security vulnerabilities, applying appropriate security patches and keeping information systems up to date,
Using strong passwords in electronic environments where personal data are processed,
Using secure logging systems in electronic environments where personal data are processed,
Using data backup programs to securely store personal data,
Restricting access to personal data stored in electronic or non-electronic environments according to access principles,
Providing required disclosures for special category personal data and obtaining explicit consent where legally required,
Providing training on special category data security, signing confidentiality agreements, defining authorizations of users with access to such data,
Taking adequate security measures in physical environments where special category personal data are processed/stored/accessed and preventing unauthorized entry/exit,
Transferring special category personal data via e-mail only through encrypted corporate e-mail or KEP where necessary; encrypting portable media transfers and storing cryptographic keys separately; transferring between servers in different physical environments via VPN or secure transfer methods; and taking precautions for paper-based transfers and sending such documents in "confidential" format.

5.2 Administrative Measures

Administrative measures taken by the Practice include:

Providing internal training to employees to prevent unlawful processing and access and to ensure secure retention of personal data,
Signing confidentiality agreements with employees and real/legal persons such as suppliers/service providers from whom services are received,
Taking legal action against employees who fail to comply with security policies and procedures,
Preparing a KVKK Disciplinary Policy,
Preparing a KVKK Internal Instruction for the Practice,
Preparing a KVKK Cookie Policy,
Preparing a KVKK Application Form,
Fulfilling the obligation to inform data subjects before starting processing and obtaining consent where required by the Law,
Preparing Disclosure and Consent Forms,
Providing KVKK notices within the Practice / physical premises,
Ensuring that employment contracts are compliant with KVKK,
Preparing a personal data processing inventory,
Conducting periodic and random internal audits,
Providing information security trainings to employees,
Ensuring protection of physical media containing personal data against external risks (fire, flood, etc.),
Applying data minimization principles as far as possible,
Determining and implementing protocols and procedures for special category data security,
Where necessary, taking additional KVKK measures in compliance with health authority processes and providing required disclosures and information to patients and staff.

---

6. PERSONAL DATA DESTRUCTION METHODS

At the end of the retention period stipulated in the relevant legislation or required for the purpose of processing, personal data are destroyed by the Practice ex officio or upon the data subject’s application, in compliance with relevant legal provisions, using the methods described below.

6.1 Deletion of Personal Data

Personal data are deleted using the methods in Table 3.

Table 3: Deletion of Personal Data

Recording Media — Explanation
Personal data on servers: For data whose required retention period has expired, deletion is performed by the system administrator by removing access authorization of relevant users.
Personal data in electronic media: Data whose retention period has expired are made inaccessible and unusable for all employees (authorized users) other than the database administrator.

Personal data in physical media: Data whose retention period has expired are made inaccessible and unusable for all employees other than the unit manager responsible for the archive; additionally, a blackout/redaction process is applied by crossing out/painting/erasing to make the data unreadable.
Personal data on portable media: Data stored on flash-based media whose retention period has expired are encrypted by the system administrator, access is granted only to the system administrator, and encryption keys are stored in secure environments.

6.2 Destruction of Personal Data

Personal data are destroyed by the Practice using the methods in Table 4.

Table 4: Destruction of Personal Data

Physical media: Paper-based data whose retention period has expired are destroyed in an irreversible manner.
Optical/magnetic media: Data whose retention period has expired are physically destroyed by melting, burning or pulverizing; additionally, magnetic media may be exposed to a high-value magnetic field via a special device to render the data unreadable.

6.3 Anonymization of Personal Data

Anonymization is rendering personal data incapable of being associated with an identified or identifiable natural person in any way, even if matched with other data.

For personal data to be considered anonymized, it must be made impossible to associate with an identified or identifiable natural person, even by using techniques appropriate to the recording media and activity area, such as re-identification by the data controller or third parties and/or matching with other data.

(ANNEX – Retention of Destruction Records): Pursuant to the Regulation, records regarding deletion, destruction and anonymization processes carried out by the Practice are retained for at least **3 (three) years**.

---

7. RETENTION AND DESTRUCTION PERIODS

Regarding personal data processed within the scope of the Practice’s activities;

Personal-data-based retention periods for all personal data within activities carried out depending on processes are set out in the Personal Data Processing Inventory;
Category-based retention periods are recorded in VERBIS;
Process-based retention periods are set out in the Personal Data Retention and Destruction Policy.

Where necessary, updates may be made by the Practice Manager. For personal data whose retention period has expired, ex officio deletion, destruction or anonymization is carried out by the Data Security Officer.

Table 5: Process-based retention and destruction periods table

Preparation and performance of contracts: 10 years following termination of the contract — In the first periodic destruction period following the end of the retention period.
Conducting corporate communication activities: 10 years following the end of the activity — In the first periodic destruction period following the end of the retention period.

PROCESS — RETENTION PERIOD — DESTRUCTION PERIOD
Conducting patient registration, diagnosis and treatment processes — 20 years following completion of the process — In the first periodic destruction period following the end of the retention period.
Conducting services outside treatment processes (communication etc.) — 10 years following completion of the process — In the first periodic destruction period following the end of the retention period.
Preparation of contracts — 10 years following completion of the process — In the first periodic destruction period following the end of the retention period.
Accounting processes — 10 years following completion of the process — In the first periodic destruction period following the end of the retention period.
Conducting human resources processes — 10 years following completion of the process — In the first periodic destruction period following the end of the retention period.
Severance/notice payments, documents and payroll information of employees who left employment — 5 years following the termination date of the employment contract — In the first periodic destruction period following the end of the retention period.
Log tracking systems — 2 years following completion of the process — In the first periodic destruction period following the end of the retention period.
Conducting access processes for hardware and software — 2 years — In the first periodic destruction period following the end of the retention period.
Camera recordings — 1 month following completion of recording — In the first periodic destruction period following the end of the retention period.
Data relating to customers and potential customers (cookies) — 13 months — In the first periodic destruction period following the end of the retention period.
IYS records — 3 years from the registration date — In the first periodic destruction period following the end of the retention period.

---

8. PERIODIC DESTRUCTION PERIOD

Pursuant to Article 11 of the Regulation, the Practice has determined the periodic destruction period as **6 months**. Accordingly, periodic destruction is carried out in **June and December** each year.

---

9. PROCESSING OF SPECIAL CATEGORY PERSONAL DATA

9.1 Special care is shown in processing special category personal data considered more critical for the protection of the data subject.

Special category personal data are processed in compliance with the Law, provided that adequate measures determined by the Board are taken, under the following conditions:

If the data subject has explicit consent; or
If the data subject does not have explicit consent; special category personal data other than health and sexual life are processed in cases stipulated by law; special category personal data relating to health and sexual life are processed only for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and planning and management of health services and their financing, by persons under the obligation of confidentiality or authorized institutions and organizations.

MEASURES REGARDING PROCESSING OF SPECIAL CATEGORY PERSONAL DATA

In processing special category personal data listed in Article 6 of the Law, pursuant to the Board Decision dated 31.01.2018 and numbered 2018/10, the following measures are taken as the data controller:

A systematic, clearly rule-based, manageable and sustainable Policy has been established for the security of special category personal data. For employees involved in processing special category personal data processes:

Confidentiality agreements are executed,
Authorization scopes and durations of users who have access to the data are clearly defined,
Authorization controls are performed periodically.
Protocols and procedures for special category data security are determined and implemented.
Authorizations of employees who change roles or leave employment are immediately revoked. Within this scope, the inventory allocated by the data controller is taken back.
If the media where special category personal data are processed/stored/accessed is physical media:

- Adequate security measures are taken against risks such as electrical leakage, fire, flood, theft, etc., depending on the nature of the environment where special category personal data are located,
- Physical security of such environments is ensured and unauthorized access is prevented.

---

10. TRANSFER OF SPECIAL CATEGORY PERSONAL DATA

As a rule, special category personal data lawfully obtained are not transferred to third parties within the scope of processing purposes. In cases mandated by legislation and/or where explicit consent or other legal conditions are required, transfers may be carried out by ensuring compliance with the Law and relevant legislation.

(ANNEX – Possibility of Cross-Border Transfer): Due to communication/CRM systems, web analytics, cloud infrastructure and similar information systems used by the Practice, cross-border transfer of personal data may come into question. In such case, necessary legal

conditions under Article 9 of the Law and Board regulations are ensured and technical/administrative measures are implemented.

---

11. PUBLICATION AND RETENTION OF THE POLICY

The Policy is published in two different media: wet-signed (printed paper) and electronic. It is publicly disclosed on the website. The printed copy is retained in the file of the Data Manager.

---

12. POLICY UPDATE PERIOD

The Policy is reviewed as needed and required sections are updated.

---

13. EFFECTIVE DATE AND TERMINATION OF THE POLICY

The Policy is deemed effective as of the date it is published on the website. If it is decided to terminate the Policy, the old wet-signed copies are cancelled by a decision to be given by the Data Manager (by stamping “cancelled” or writing cancellation), signed, and retained by the Data Manager for at least **5 years**.