# Dr. Berkant Oman

# KVKK

## PERSONENBEZOGENE DATENSPEICHERUNG UND

## ENTSORGUNGSRICHTLINIE

**Adresse** : Kazımdirik Mah. 372/9 Sokak Nr. 1 Bornova/İzmir

**Telefon** : +90 552 361 49 88

**Netz** : https://www.drberkantoman.com/

**Email** :oman.klinik@gmail.com

# Inhalt

# 1. KAPITEL EINS :

1.1. Anmeldung

Gemäß dem Gesetz zum Schutz personenbezogener Daten Nr. 6698 legen wir größten Wert auf die rechtmäßige Verarbeitung und den Schutz personenbezogener Daten und gehen bei allen unseren Planungen und Aktivitäten mit dieser Sorgfalt vor. In diesem Bewusstsein legen wir Ihnen diese Richtlinie zur Verarbeitung, Speicherung und Entsorgung personenbezogener Daten zu Ihrer Information vor, um der Offenlegungspflicht im Rahmen von Artikel 10 des Gesetzes nachzukommen und Sie über alle administrativen und technischen Maßnahmen zu informieren, die wir im Rahmen dieses Gesetzes ergriffen haben Umfang der Verarbeitung und Schutz personenbezogener Daten.

Das Gesetz zum Schutz personenbezogener Daten Nr. 6698 trat am 7. April 2016 in Kraft und „enthält Vorschriften für die Verarbeitung aller Arten von Informationen über identifizierte oder identifizierbare natürliche Personen."

Der Schutz der personenbezogenen Daten unserer Kunden, Mitarbeiter und anderer realer Personen, mit denen wir in Kontakt stehen, ist uns ein wichtiges Anliegen. Für die Verarbeitung und den Schutz Ihrer personenbezogenen Daten gelten der durch diese Richtlinie geregelte Prozess und der angestrebte Zweck; ist die rechtmäßige Verarbeitung und der Schutz personenbezogener Daten unserer Kunden, Interessenten, Mitarbeiter, Mitarbeiterkandidaten, Besucher, Mitarbeiter der Institutionen, mit denen wir zusammenarbeiten, und Dritter.

## 1.2. Ziel

Der Zweck der Richtlinie zur Verarbeitung, Speicherung und Entsorgung personenbezogener Daten besteht darin, aktuelle und potenzielle Kunden, Mitarbeiter, Besucher, Aktionäre, Praxisleiter, Mitarbeiterkandidaten, Mitarbeiter kooperierender Institutionen und Beamte Dritter der Dr. Berkant Oman Clinic automatisch oder auf nichtautomatische Weise zu verarbeiten sofern sie Teil eines Datenaufzeichnungssystems sind. Festlegung der Grundsätze für die Verarbeitung aller personenbezogenen Daten, Schutz der Grundrechte und Grundfreiheiten des Einzelnen, Festlegung der notwendigen Rechte und Pflichten im Rahmen der rechtlichen und rechtlichen Verarbeitung der betreffenden personenbezogenen Daten, Sensibilisierung für den Schutz personenbezogener Daten und Datenschutz in den Augen des Praxispersonals,

## 1.3. Umfang

Die erstellte Richtlinie deckt alle Arten von Informationen und Dokumenten ab, die einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, die in der Definition „personenbezogener Daten“ des Gesetzes enthalten sind, sowie die diesbezüglich ergriffenen Maßnahmen und Vereinbarungen.

In den Geltungsbereich dieser Richtlinie fallen personenbezogene Daten unserer Mitarbeiter, Mitarbeiterkandidaten, Dienstleister, Besucher und anderer Dritter, die im bereitgestellten und auf elektronischen und/oder physischen Datenträgern gespeicherten Praxisdatenbestand enthalten sind, sowie alle Aufzeichnungsträger, auf denen personenbezogene Daten gespeichert sind Die im Besitz der Institution befindlichen oder von ihr verwalteten Daten werden verarbeitet. Diese Richtlinie wird bei Aktivitäten im Zusammenhang mit der Verarbeitung personenbezogener Daten und personenbezogener Daten angewendet.

## 1.4. Umsetzung der Richtlinie und der damit verbundenen Gesetzgebung

Zur Erfüllung unserer Verpflichtungen gemäß dieser Richtlinie zur Aufbewahrung und Entsorgung personenbezogener Daten, dem Gesetz zum Schutz personenbezogener Daten Nr. 6698 und der Verordnung über die Löschung, Vernichtung oder Anonymisierung personenbezogener Daten, die nach Veröffentlichung im Amtsblatt in Kraft traten vom 28. Oktober 2017, die die sekundäre Regelung des Gesetzes darstellt und von unserem Büro als Datenverantwortlicher erstellt wurde, um die Dateneigentümer über die Grundsätze zur Bestimmung der maximalen Speicherdauer zu informieren, die für den Zweck erforderlich ist, für den Ihre Daten gespeichert werden die Verarbeitung personenbezogener Daten sowie die Vorgänge der Löschung, Vernichtung und Anonymisierung.

## 1.5. Definitionen und Abkürzungen

| | |
|---|---|
| **Käufergruppe** | Die Kategorie der natürlichen oder juristischen Person, an die der Datenverantwortliche personenbezogene Daten übermittelt. |
| **Offene Zustimmung** | Einwilligung zu einem bestimmten Thema, basierend auf Informationen und freiwillig ausgedrückt. |
| **Verwandter Benutzer** | Mit Ausnahme der Person oder Einheit, die für die technische Speicherung, den Schutz und die Sicherung der Daten verantwortlich ist, handelt es sich dabei um die Personen, die personenbezogene Daten innerhalb der Organisation des Datenverantwortlichen oder gemäß der vom Datenverantwortlichen erhaltenen Genehmigung und Weisung verarbeiten. |
| **Verwandte Person** | Die natürliche Person, deren personenbezogene Daten verarbeitet werden. („Richtlinie“ wird auch als „Dateneigentümer“ bezeichnet). |
| **Arbeiter** | Dr. Mitarbeiter der Berkant Oman Clinic |
| **Elektronische Umgebung** | Umgebungen, in denen personenbezogene Daten von elektronischen Geräten erstellt, gelesen, geändert und geschrieben werden können. |
| **Elektronisch Nicht-Umwelt** | Alle schriftlichen, gedruckten, visuellen usw. außer elektronischen Medien. andere Umgebungen. |
| **Dienstleister (Anbieter)** | Dr. Eine natürliche oder juristische Person, die im Rahmen eines bestimmten Vertrags mit Berkant Oman Practice Dienstleistungen erbringt. |
| **Zerstörung** | Löschung, Vernichtung oder Anonymisierung personenbezogener Daten. |
| **Gesetz** | Gesetz zum Schutz personenbezogener Daten Nr. 6698. |

| | |
|---|---|
| **Aufnahmemedien** | Jede Umgebung, in der personenbezogene Daten ganz oder teilweise automatisch oder auf nichtautomatische Weise verarbeitet werden, sofern sie Teil eines Datenaufzeichnungssystems sind. |
| **Persönliche Daten** | Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. |
| **Persönliche Daten Inventar verarbeiten** | Tätigkeiten zur Verarbeitung personenbezogener Daten, die von Datenverantwortlichen in Abhängigkeit von ihren Geschäftsprozessen durchgeführt werden; Das Inventar wird erstellt, indem die Verarbeitungszwecke und der Rechtsgrund der personenbezogenen Daten, die Datenkategorie, die übermittelte Empfängergruppe und die Gruppe der betroffenen Personen miteinander verknüpft werden und die maximale Speicherdauer erläutert wird, die für die Zwecke, für die personenbezogene Daten verarbeitet werden, erforderlich ist ins Ausland übertragenen Daten und die getroffenen Maßnahmen zur Datensicherheit. |
| **Ihre persönlichen Daten wird bearbeitet** | Das Beschaffen, Aufzeichnen, Speichern, Bewahren, Verändern, Umordnen, Offenlegen, Übertragen, Übernehmen, Bereitstellen, Klassifizieren oder Nutzen personenbezogener Daten ganz oder teilweise auf automatischem oder nichtautomatischem Wege, sofern sie Teil eines Datenaufzeichnungssystems sind. Jeder Vorgang, der an den Daten ausgeführt wird, z. B. das Blockieren. |
| **Ihre persönlichen Daten Anonymer Halo einbringen** | Es ist unter keinen Umständen möglich, personenbezogene Daten einer identifizierten oder identifizierbaren natürlichen Person zuzuordnen, auch nicht durch den Abgleich mit anderen Daten. |
| **Ihre persönlichen Daten Streichung** | Löschung personenbezogener Daten; Persönliche Daten für relevante Benutzer in irgendeiner Weise unzugänglich und unbrauchbar machen. |
| **Ihre persönlichen Daten Zerstörung** | Der Prozess, bei dem personenbezogene Daten für jedermann in irgendeiner Weise unzugänglich, unwiederbringlich und unbrauchbar gemacht werden. |
| **Politik** | Richtlinie zur Verarbeitung, Speicherung und Entsorgung personenbezogener Daten |
| **Planke** | Ausschuss für den Schutz personenbezogener Daten |
| **Speziell qualifiziert Persönliche Daten** | Daten zu Rasse, ethnischer Herkunft, politischer Meinung, philosophischer Überzeugung, Religion, Sekte oder anderen Glaubensrichtungen, Tracht und Kleidung, Mitgliedschaft in Vereinen, Stiftungen oder Gewerkschaften, Gesundheit, Sexualleben, strafrechtlichen Verurteilungen und Sicherheitsmaßnahmen sowie biometrische und genetische Daten. |
| **biometrisch** | Fingerabdrücke, Handflächenabdrücke, Gesicht, Iris, Netzhaut, Ohr, Stimme, Unterschrift, Gang, Handvene, Körpergeruch und DNA-Informationen von Personen fallen in den Geltungsbereich biometrischer Daten. Allgemeines Konzept, das einzigartige physische oder Verhaltensmerkmale umfasst, die die Identifizierung von Personen ermöglichen. |
| **Periodische Zerstörung** | Der Lösch-, Vernichtungs- oder Anonymisierungsprozess, der von Amts wegen in wiederkehrenden Abständen durchgeführt und in der Richtlinie zur Speicherung und Vernichtung personenbezogener Daten festgelegt wird, sofern alle im Gesetz vorgesehenen Bedingungen für die Verarbeitung personenbezogener Daten aufgehoben werden. |
| **Dateneigentümer/bezogen Person** | Natürliche Person, deren personenbezogene Daten verarbeitet werden |
| **Datenprozessor** | Die natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet, basierend auf der vom Datenverantwortlichen erteilten Befugnis. |
| **Datencontroller** | Die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet und für die Einrichtung und Verwaltung des Datenerfassungssystems verantwortlich ist. |

| | |
|---|---|
| **Datenverantwortliche**<br>Registrierungsinformationen<br>**System** | Das Informationssystem, auf das über das Internet zugegriffen werden kann, wurde von der Präsidentschaft der Agentur für den Schutz personenbezogener Daten erstellt und verwaltet und soll von den Datenverantwortlichen bei der Anmeldung beim Register und bei anderen damit verbundenen Transaktionen im Zusammenhang mit dem Register verwendet werden. |
| **VERBIS** | Registerinformationssystem für Datenverantwortliche |
| **Verordnung** | Verordnung zur Löschung, Vernichtung oder Anonymisierung personenbezogener Daten, veröffentlicht im Amtsblatt vom 28. Oktober 2017 |

**2. ZWEITER TEIL: VERTEILUNG DER VERANTWORTLICHKEITEN UND PFLICHTEN DER SPEICHERUNG PERSONENBEZOGENER DATEN**

**UND ENTSORGUNGSMANAGEMENTSTRUKTUR**

In Übereinstimmung mit dem KVK-Gesetz Nr. 6698 und den einschlägigen Rechtsvorschriften wurde im Rahmen der Gewährleistung, Aufrechterhaltung und Aufrechterhaltung der Einhaltung der Rechtsvorschriften zum Schutz personenbezogener Daten die Datenkontaktperson der Praxis bestimmt, um die erforderliche Koordinierung innerhalb der Praxis sicherzustellen. und seine Pflichten und Verantwortlichkeiten sind in Tabelle 1 im Anhang aufgeführt.

Bei allen Aktivitäten im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten wird die Richtlinie befolgt und das mit den Aufgaben betraute Personal fungiert als Leitfaden bei der Umsetzung der Praxisrichtlinie. Alle unsere Mitarbeiter, Stakeholder, autorisierten Händler, autorisierten Dienste, Lieferanten, Lösungspartner, Berater und deren Mitarbeiter, Gäste, Besucher und verbundene Dritte, deren personenbezogene Daten in unserer Praxis verarbeitet werden, sind zur Zusammenarbeit mit der Dr. Berkant Oman Practice verpflichtet autorisierte Personen im KVK-Prozess unter Einhaltung der KVK-Richtlinie und bei der Beseitigung der rechtlichen Risiken. Alle Mitarbeiter, deren Aufgaben im KVK-Prozess verteilt sind, sind für die Einhaltung der KVK-Richtlinien aller Organe und Abteilungen unserer Praxis verantwortlich.

Alle Einheiten und Mitarbeiter der Praxis werden von den verantwortlichen Einheiten beauftragt, die im Rahmen der Richtlinie ergriffenen technischen und administrativen Maßnahmen umzusetzen, die Schulung und das Bewusstsein der Mitarbeiter der Einheit zu verbessern und die illegale Verarbeitung personenbezogener Daten durch Überwachung und kontinuierliche Kontrolle zu verhindern , um illegalen Zugriff auf personenbezogene Daten zu verhindern und personenbezogene Daten zu schützen. Sie unterstützt die verantwortlichen Stellen aktiv bei der Ergreifung technischer und administrativer Maßnahmen zur Gewährleistung der Datensicherheit in allen Umgebungen, in denen personenbezogene Daten verarbeitet werden, um eine gesetzeskonforme Speicherung sicherzustellen.

**Tabelle-1: Aufgabenverteilung der Speicher- und Vernichtungsprozesse**

| TITEL | EINHEIT | VERANTWORTUNG |
|---|---|---|
| **Management**<br>**Planke**<br>**Kopf** | Vorstand | Verantwortlich dafür, dass die Mitarbeiter im Einklang mit der Richtlinie handeln. |
| **Verwaltungsangelegenheiten**<br>**Manager** | Verwaltungsangelegenheiten<br>Abteilung | Es ist für die Vorbereitung, Entwicklung, Ausführung, Veröffentlichung und Aktualisierung der Richtlinie verantwortlich. |

### 2.1. Ansprechpartner

Der Ansprechpartner wurde bestimmt und auf der Website veröffentlicht, um die Wirksamkeit der von unserer Praxis ergriffenen Maßnahmen zur Einhaltung der Datenschutzgesetze zu überwachen. Die Hauptaufgabe des Ansprechpartners besteht in der Abstimmung mit den im KVK-Prozessmanagement eingesetzten Mitarbeitern/Führungskräften innerhalb der Praxis. Der Ansprechpartner fungiert auch als Ansprechpartner im Sinne der KVK-Gesetzgebung gegenüber dem Verantwortlichenregister unserer Praxis und der KVK-Institution. Für den Fall, dass der Ansprechpartner aufgrund einer Erlaubnis und/oder aus anderen Gründen nicht in unserer Praxis ist, wird ihm von der Praxisleitung vorübergehend ein anderer Mitarbeiter zugewiesen. In diesem Fall ist die vorübergehend ernannte Person für die Erfüllung aller der Kontaktperson im Rahmen der Richtlinie zum Schutz personenbezogener Daten übertragenen Aufgaben verantwortlich.

## 2.2. Abteilungsleiter

Der Leiter dieser Abteilung ist für die Durchführung der Datenverarbeitungsaktivitäten innerhalb der Prozesse der jeweiligen Abteilung in jeder Abteilung unserer Praxis verantwortlich. Der Abteilungsleiter erfüllt die Anforderungen der KVK-Richtlinie und der gesetzlichen Regelungen innerhalb seiner eigenen Abteilung und arbeitet dabei mit dem Ansprechpartner und den im KVK-Prozess eingesetzten Verantwortlichen zusammen. Dabei erhält er Unterstützung von anderen Mitarbeitern seiner Abteilung und kann bei Bedarf Verantwortung übertragen.

### 2.3. Alle Angestellten

Alle Mitarbeiter unserer Praxis sind verpflichtet, sich mit den KVK-Richtlinien vertraut zu machen und diese inhaltlich umzusetzen. Dabei arbeiten alle Mitarbeiter unserer Praxis im Einklang mit den im KVK-Prozess eingesetzten Verantwortlichen und Ansprechpartnern zusammen, geben Feedback zur Verbesserung der KVK-Policy und agieren kooperativ. Im Falle eines Verstoßes gegen die KVK-Richtlinien und -Verfahren werden die erforderlichen Rechtsbehelfe im Rahmen des Arbeitsgesetzes und verwandter Gesetze ergriffen.

### 2.4. Überprüfung und Audit

Die im KVK-Prozess innerhalb unserer Praxis eingesetzten und in Tabelle 1 aufgeführten Verantwortlichen verfolgen die rechtlichen, technologischen und organisatorischen Änderungen und Entwicklungen, die im Rahmen des Schutzes personenbezogener Daten eintreten können, und stellen sicher, dass die erforderlichen Maßnahmen zur Gewährleistung unserer Praxis ergriffen werden mit diesen Entwicklungen kompatibel sind. Die im KVK-Prozess eingesetzten Verantwortlichen prüfen die Verarbeitung personenbezogener Daten und alle damit zusammenhängenden Angelegenheiten von Amts wegen oder auf Antrag. Als Ergebnis der Prüfung werden die Probleme, bei denen festgestellt wird, dass sie nicht mit den in den KVK-Richtlinien festgelegten Regeln und/oder Gesetzen vereinbar sind, und die diesbezüglichen Verbesserungsvorschläge von den im KVK-Prozess zuständigen Mitarbeitern an die Geschäftsführung gemeldet. In diesem Zusammenhang überwacht die Verbindungsperson die Ausführung der erforderlichen Arbeiten.

Das im KVK-Prozess eingesetzte verantwortliche Personal führt alle sechs Monate eine Prüfung durch, um sicherzustellen, dass unsere Praxis die Rechtsvorschriften zum Schutz personenbezogener Daten einhält. Die genannte Prüfung erfolgt durch die im KVK-Prozess eingesetzten Verantwortlichen.

Bei den genannten Inspektionstätigkeiten werden mindestens folgende Sachverhalte untersucht:

a) Effektive und korrekte Umsetzung der KVK-Richtlinien, Pflichten und Verantwortlichkeiten, die von der Geschäftsführung zugewiesen, übernommen und von den Mitarbeitern erfüllt werden,

b) der Bildungs- und Sensibilisierungsgrad der Mitarbeiter ausreichend ist,

c) das Verzeichnis der Verarbeitung personenbezogener Daten, Offenlegungserklärungen und andere Dokumente korrekt, vollständig und aktuell sind,

d) Die für den Schutz personenbezogener Daten getroffenen administrativen und technischen Maßnahmen sind wirksam und ausreichend.

e) Aktualisierung der KVK-Richtlinien als Reaktion auf rechtliche, technologische und organisatorische Entwicklungen. Die im Rahmen der Überprüfung ermittelten Verbesserungspunkte werden durch die im KVK-Prozess eingesetzten Verantwortlichen an die Geschäftsführung gemeldet und die notwendigen Arbeiten durch den Ansprechpartner nachverfolgt. Die im KVK-Prozess eingesetzten Verantwortlichen sorgen dafür, dass im Rahmen dieser Festlegungen mit Zustimmung der Geschäftsführung die notwendigen Verbesserungen vorgenommen werden.

**3. AUFZEICHNUNGSUMGEBUNGEN**

Personenbezogene Daten werden von unserer Praxis in den in der folgenden Tabelle aufgeführten Umgebungen verarbeitet. werden gemäß den gesetzlichen Bestimmungen sicher aufbewahrt.

Tabelle 2: Speicherumgebungen für persönliche Daten

| **Elektronische Medien** | **Nichtelektronische Medien** |
|---|---|
| • Server (Domäne, Backup, E-Mail, Datenbank, Web, Dateifreigabe, Wolke usw.)<br>• Software (Bürosoftware, Portal, EBYS, VERBIS, Klinikverwaltungssoftware)<br>• Informationssicherheitsgeräte (Firewall, Erkennung und Verhinderung von Eindringlingen, Protokolldatei, Virenschutz usw.)<br>• Personalcomputer (Desktop, Laptop)<br>• Mobile Geräte (Telefon, Tablet usw.)<br>• Optische Datenträger (CD, DVD usw.)<br>• Wechselspeicher (USB, Speicherkarte usw.)<br>• Drucker, Scanner, Kopierer | • Auf Papier gespeicherte personenbezogene Daten,<br>• Manuelle Datenerfassungssysteme (Umfrageformulare, Besucherlogbuch)<br>• Schriftliche, gedruckte, visuelle Medien,<br>• Bewerbungsformulare,<br>• Verträge zwischen der Praxis und Dritten<br>• Manuelle Datenerfassungssysteme (Umfrageformulare, Besucherlogbuch usw.)<br>• Persönliche Daten werden in schriftlichen, gedruckten und visuellen Medien gespeichert<br>• Einheitsschränke<br>• Archivräume |

**4. ERLÄUTERUNGEN ZUR LAGERUNG UND ENTSORGUNG**

Durch unsere Praxis; Personenbezogene Daten von Mitarbeitern Dritter, Institutionen oder Organisationen, die als Mitarbeiter, Mitarbeiterkandidaten, Besucher und Dienstleister (Lieferanten) in Kontakt stehen, werden gemäß den gesetzlichen Bestimmungen gespeichert und vernichtet.

4.1. Kategorien personenbezogener Dateneigentümer

**Tabelle -3: Kategorien der Eigentümer personenbezogener Daten**

| **PERSÖNLICHE DATEN EIGENTÜMER KATEGORIE** | **BESCHREIBUNG** |
|---|---|
| **Besucher** | Dr. Echte Personen, die aus verschiedenen Gründen den physischen Campus der Berkant Oman Clinic betreten oder unsere Websites besucht haben |
| **Arbeiter** | Dr. Mitarbeiter der Berkant Oman Clinic. |
| **Mitarbeiterkandidat** | Wenn Sie sich auf irgendeine Weise für eine Stelle in unserer Praxis beworben haben oder Ihren Lebenslauf und zugehörige Informationen an Dr. eingereicht haben, handelt es sich um natürliche Personen, die die Berkant Oman Clinic zur Prüfung eröffnet haben. e |
| **Produkt oder Dienstleistung Empfänger** | Echte Personen, die die von unserer Praxis angebotenen Produkte und Dienstleistungen nutzen oder genutzt haben, unabhängig davon, ob sie in einem Vertragsverhältnis zu unserer Praxis stehen (in Behandlung befindlicher oder behandelter Patient) |
| **Potenzielles Produkt oder Service Empfänger** | Echte Personen, die das Potenzial haben, die von unserer Praxis angebotenen Produkte und Dienstleistungen zu nutzen, unabhängig davon, ob sie in einem Vertragsverhältnis mit unserer Praxis stehen (in Behandlung befindlicher Patient oder Patient) |
| **Familienmitglieder und Verwandte** | Ehepartner, Kinder und Angehörige von betroffenen Personen, deren personenbezogene Daten im Rahmen der von unserer Praxis durchgeführten Tätigkeiten im Rahmen dieser Datenschutzerklärung verarbeitet werden. |
| **Dritte Seite** | Diese Richtlinie Berkant Oman Practice-Mitarbeiter Andere natürliche Personen, die nicht unter die Richtlinie zum Schutz und zur Verarbeitung personenbezogener Daten fallen (z. B. Bürge, Begleiter, ehemalige Mitarbeiter) |
| **Lieferantenvertreter** | Echte Personen, die Bevollmächtigte oder Gesellschafter des Vertragspartners sind, der gemäß den Aufträgen und Weisungen unserer Praxis im Rahmen der Ausübung ihrer gewerblichen Tätigkeit Leistungen für die Praxis erbringt. |
| **Mitarbeiter des Lieferanten** | Bei der Ausübung der kommerziellen Tätigkeit unserer Praxis sind Dr. natürliche Personen, die Mitarbeiter der Partei sind, die auf vertraglicher Basis Dienstleistungen für die Praxis gemäß den Anordnungen und Anweisungen der Berkant Oman Inspection erbringt. |

## 4.2. Hinweise zur Lagerung

In Artikel 3 des Gesetzes wird der Begriff der Verarbeitung personenbezogener Daten definiert, in Artikel 4 heißt es, dass die verarbeiteten personenbezogenen Daten mit dem Zweck, für den sie verarbeitet werden, in Zusammenhang stehen, begrenzt und gemessen werden und für einen bestimmten Zeitraum aufbewahrt werden müssen die für den Zweck, für den sie verarbeitet werden, erforderlich sind oder wie in den einschlägigen Rechtsvorschriften sowie in den Artikeln 5 und 6, Datenverarbeitungsbedingungen, festgelegt

gezählt. Dementsprechend werden personenbezogene Daten im Rahmen der Berkant Oman Inspection-Aktivitäten für einen Zeitraum gespeichert, der in den einschlägigen Rechtsvorschriften festgelegt ist oder für Verarbeitungszwecke geeignet ist.

4.2.A Rechtliche Gründe für die Aufbewahrung

Personenbezogene Daten, die in unserer Praxis im Rahmen ihrer Tätigkeit verarbeitet werden, werden für den in den einschlägigen Rechtsvorschriften vorgesehenen Zeitraum aufbewahrt. In diesem Zusammenhang personenbezogene Daten;

- Gesetz Nr. 6698 zum Schutz personenbezogener Daten,
- Türkisches Obligationenrecht Nr. 6098,
- Gesetz Nr. 6502 zum Verbraucherschutz
- Einkommensteuergesetz Nr. 193,
- Steuerverfahrensgesetz Nr. 213
- Sozialversicherungs- und allgemeines Krankenversicherungsgesetz Nr. 5510,
- Gesetz Nr. 5651 über die Organisation von Sendungen im Internet und die Bekämpfung von durch diese Sendungen begangenen Straftaten, *
- Arbeitsschutzgesetz Nr. 6331,
- 4817 Gesetz über die Arbeitserlaubnis von Ausländern
- Arbeitsgesetz Nr. 4857,
- Gesetzesdekret Nr. 556 zum Schutz von Marken,
- Türkisches Handelsgesetzbuch Nr. 6102,
- 6563 Gesetz zur Regulierung des elektronischen Geschäftsverkehrs,
- Notargesetz Nr. 1512,
- Gesetz Nr. 5544 der Berufsqualifikationsbehörde und damit verbundene Mitteilungen, die den Erwerb eines Berufsqualifikationszertifikats verpflichtend vorschreiben,
- Verordnung über Gesundheits- und Sicherheitsmaßnahmen in Gebäuden und Anlagen am Arbeitsplatz,
- Verordnung über kommerzielle Kommunikation und kommerzielle elektronische Nachrichten, veröffentlicht im Amtsblatt Nr. 29417 vom 15.07.2015,
- Verordnung über Fernabsatzverträge Nr. 27866,
- Gesetz Nr. 2219 über private Krankenhäuser,
- Gesundheits-Grundgesetz Nr. 3359,
- Gesetzesdekret Nr. 663 über die Organisation und Aufgaben des Gesundheitsministeriums und seiner angegliederten Stellen,
- Verordnung über personenbezogene Gesundheitsdaten,
- Patientenrechteverordnung,
- Verordnung über private Krankenhäuser,
- Verordnung zur Änderung der Verordnung über private Krankenhäuser,
- Verordnung zur Entwicklung und Bewertung der Qualität im Gesundheitswesen,
- Verordnung über medizinische Laboratorien,
- Präsidialdekret Nr. 1 über die Organisation der Präsidentschaft,
- Gesetzesdekret Nr. 663 über einige Vorschriften im Gesundheitsbereich,

- Verordnung zur Änderung der Verordnung über private Gesundheitseinrichtungen, in denen ambulante Diagnosen und Behandlungen durchgeführt werden,
- Verordnung über traditionelle und komplementäre medizinische Praktiken,
- Gesundheits-Grundgesetz Nr. 3359,

- Verordnung zur medizinischen Deontologie,
- Richtlinie über Gesundheitsdienstleistungen im Rahmen des Gesundheitstourismus und der touristischen Gesundheit,
- Richtlinie über die Beschaffung von Dienstleistungen von öffentlichen Gesundheitseinrichtungen an private Gesundheitseinrichtungen (Anhang-1 für Anhang),
- Richtlinie über die Verfahren und Grundsätze für die Aufsicht über private Gesundheitseinrichtungen und -organisationen von den Gesundheitsdirektionen der Provinzen,
- Kaskadierung von Gesundheitsdienstleistern 2019/18,
- Leitfaden zur klinischen Qualitätspraxis und Datenqualitätsverbesserung 2019/15,
- Rundschreiben zu Injektionspraktiken 2019/11,

Die Speicherung erfolgt für die Dauer der im Rahmen sonstiger nach diesen Gesetzen geltenden Sekundärvorschriften vorgesehenen Aufbewahrungsfristen.

4.2.B. Verarbeitungszwecke, die eine Speicherung erfordern

Unsere Praxis speichert und verarbeitet personenbezogene Daten zu den folgenden Zwecken und Bedingungen, beschränkt auf die Zwecke und Bedingungen, die in den Bedingungen für die Verarbeitung personenbezogener Daten im 2. Absatz des 5. Artikels des KVK-Gesetzes und im 3. Absatz des 6. Artikels festgelegt sind.

Diese Zwecke und Bedingungen sind:

- Schutz der öffentlichen Gesundheit, Präventivmedizin, medizinische Diagnostik, Durchführung von Behandlungs- und Pflegediensten, Planung und Verwaltung von Gesundheitsdiensten und Finanzierung.
- Durchführung von Notfallmanagementprozessen
- Durchführung von Informationssicherheitsprozessen
- Durchführung von Auswahl- und Vermittlungsprozessen für Mitarbeiter, Praktikanten und Studenten
- Durchführung von Bewerbungsprozessen von Mitarbeiterkandidaten
- Durchführung von Prozessen zur Mitarbeiterzufriedenheit und -bindung
- Erfüllung arbeitsvertraglicher und gesetzlicher Pflichten für Arbeitnehmer
- Durchführung von Benefits und Benefit-Prozessen für Mitarbeiter
- Durchführung von Audits/ethischen Aktivitäten
- Durchführung von Bildungsaktivitäten
- Ausführung von Zugangsberechtigungen
- Ausführung der Tätigkeiten in Übereinstimmung mit der Gesetzgebung
- Ausführung von Finanz- und Buchhaltungsangelegenheiten
- Durchführung von Unternehmens-/Produkt-/Dienstleistungsbindungsprozessen
- Bereitstellung physischer Raumsicherheit
- Durchführung von Zuordnungsprozessen
- Nachverfolgung und Ausführung rechtlicher Angelegenheiten
- Durchführung interner Audit-/Ermittlungs-/Intelligence-Aktivitäten
- Durchführung von Kommunikationsaktivitäten
- Planung von Personalprozessen
- Durchführung/Überwachung von Geschäftsaktivitäten
- Durchführung von Arbeitsschutzaktivitäten
- Entgegennahme und Bewertung von Verbesserungsvorschlägen für Geschäftsprozesse
- Durchführung von Aktivitäten zur Gewährleistung der Geschäftskontinuität
- Durchführung von Waren-/Dienstleistungsbeschaffungsprozessen

- Ausführung von Waren-/Dienstleistungen, After-Sales-Support-Services
- Durchführung von Waren-/Dienstleistungsverkaufsprozessen
- Ausführung von Waren-/Dienstleistungsproduktions- und Betriebsprozessen
- Durchführung von Customer-Relationship-Management-Prozessen
- Durchführung von Aktivitäten zur Kundenzufriedenheit
- Organisation und Eventmanagement
- Durchführung von Leistungsbewertungsprozessen
- Durchführung von Risikomanagementprozessen
- Durchführung von Speicher- und Archivierungsaktivitäten
- Durchführung sozialer Verantwortung und zivilgesellschaftlicher Aktivitäten
- Durchführung von Vertragsabwicklungen
- Durchführung strategischer Planungsaktivitäten
- Nachverfolgung von Anfragen/Beschwerden
- Gewährleistung der Sicherheit von beweglichem Eigentum und Ressourcen
- Durchführung von Supply Chain Management Prozessen
- Ausführung der Lohnpolitik
- Gewährleistung der Sicherheit des Datencontrollerbetriebs
- Durchführung von Talent-/Karriereentwicklungsaktivitäten
- Bereitstellung von Informationen an autorisierte Personen, Institutionen und Organisationen
- Durchführung von Managementaktivitäten
- Erstellen und Verfolgen von Besucherdatensätzen

## 4.3. Gründe für die Zerstörung

Persönliche Daten;

- Änderung oder Aufhebung der Bestimmungen der einschlägigen Rechtsvorschriften, die der Verarbeitung zugrunde liegen,
- Wegfall des Zwecks, der seine Verarbeitung oder Speicherung erfordert,
- In Fällen, in denen die Verarbeitung personenbezogener Daten nur auf Grundlage einer ausdrücklichen Einwilligung erfolgt, widerruft die betroffene Person ihre ausdrückliche Einwilligung,
- Gemäß Artikel 11 des Gesetzes wird der Antrag auf Löschung und Vernichtung personenbezogener Daten im Rahmen der Rechte der betroffenen Person von der Praxis angenommen.
- In Fällen, in denen die Praxis den Antrag der betroffenen Person auf Löschung, Vernichtung oder Anonymisierung ihrer personenbezogenen Daten ablehnt, die Antwort für unzureichend hält oder nicht innerhalb der gesetzlich vorgesehenen Frist antwortet; Einreichen einer Beschwerde beim Vorstand und Genehmigung dieses Antrags durch den Vorstand,
- Die maximale Aufbewahrungsfrist für personenbezogene Daten ist abgelaufen und es liegen keine Bedingungen vor, die eine längere Aufbewahrung personenbezogener Daten rechtfertigen.

In solchen Fällen werden sie auf Wunsch des Betroffenen von der Praxis gelöscht, vernichtet oder von Amts wegen gelöscht, vernichtet oder anonymisiert.

**5. TECHNISCHE UND ADMINISTRATIVE MASSNAHMEN**

Dr. Berkant Oman Inspection ergreift im Rahmen der Möglichkeiten je nach Art der zu schützenden Daten alle erforderlichen Maßnahmen, um die unrechtmäßige Offenlegung, den Zugriff, die Übertragung oder andere Sicherheitsmängel personenbezogener Daten zu verhindern. In diesem Zusammenhang wird Dr. Alle erforderlichen administrativen und technischen Maßnahmen werden von Berkant Oman Inspection ergriffen, in der Praxis wird ein Auditsystem eingerichtet und im Falle einer rechtswidrigen Offenlegung personenbezogener Daten wird gemäß den im KVK-Gesetz festgelegten Maßnahmen gehandelt .

- Dr. Berkant Oman Practice schult und sensibilisiert seine Mitarbeiter hinsichtlich der Gesetzgebung zum Schutz personenbezogener Daten.
- In den Fällen, in denen eine Übermittlung personenbezogener Daten erforderlich ist, werden den von der Praxis mit den Personen, an die die personenbezogenen Daten übermittelt werden, geschlossenen Verträgen Aufzeichnungen hinzugefügt, aus denen hervorgeht, dass die Partei, an die die personenbezogenen Daten übermittelt werden, ihren Pflichten zur Datensicherung nachkommt Sicherheit.

- Dr. Die von der Berkant Oman Clinic durchgeführten Aktivitäten zur Verarbeitung personenbezogener Daten werden eingehend untersucht und in diesem Zusammenhang Maßnahmen festgelegt, um die Einhaltung der im KVK-Gesetz festgelegten Bedingungen für die Verarbeitung personenbezogener Daten sicherzustellen.
- Dr. Berkant Oman Practice legt die Praktiken fest, die befolgt werden müssen, um die Einhaltung des KVK-Gesetzes sicherzustellen, und regelt diese Praktiken durch interne Richtlinien.
- Dr. In Bezug auf den Schutz personenbezogener Daten werden von der Berkant Oman Clinic technische Maßnahmen ergriffen, soweit die Technologie dies zulässt, und die ergriffenen Maßnahmen werden parallel zu den Entwicklungen aktualisiert und verbessert.
- In technischen Belangen wird fachkundiges Personal eingesetzt.
- Zur Umsetzung der getroffenen Maßnahmen werden in regelmäßigen Abständen Audits durchgeführt.
- Zur Gewährleistung der Sicherheit werden Software und Systeme installiert.
- Der Zugriff auf die in der Praxis verarbeiteten personenbezogenen Daten ist entsprechend dem angegebenen Verarbeitungszweck auf die jeweiligen Mitarbeiter beschränkt.

5.1. Technische Maßnahmen

Nachfolgend sind die technischen Maßnahmen aufgeführt, die die Praxis hinsichtlich der von ihr verarbeiteten personenbezogenen Daten trifft:

- Mit Penetrationstests werden notwendige Vorkehrungen getroffen, indem etwaige Risiken, Bedrohungen, Schwachstellen und Schwachstellen in Bezug auf die Informationssysteme unserer Praxis aufgedeckt werden.
- Durch Echtzeitanalysen mit Information Security Incident Management werden Risiken und Bedrohungen, die die Kontinuität von Informationssystemen beeinträchtigen, kontinuierlich überwacht.
- Der Zugriff auf Informationssysteme und die Autorisierung von Benutzern erfolgen über Sicherheitsrichtlinien über die Zugriffs- und Autorisierungsmatrix und das Unternehmens-Active Directory.
- Es werden die notwendigen Vorkehrungen für die physische Sicherheit der Informationssysteme, Software und Daten unserer Praxis getroffen.
- Um die Sicherheit von Informationssystemen vor Umweltbedrohungen zu gewährleisten, ist Hardware erforderlich (Zugangskontrollsystem, das nur autorisiertem Personal den Zutritt zum Systemraum ermöglicht, Mitarbeiterüberwachungssystem rund um die Uhr, physische Sicherheit der Edge-Switches, aus denen das lokale Netzwerk besteht).

Feuerlöschanlage, Klimaanlage etc.) und Software (Firewalls, Angriffsschutzsysteme, Netzwerkzugriffskontrolle, Systeme zur Abwehr von Schadsoftware etc.) werden Maßnahmen ergriffen.

- Es werden Risiken zur Verhinderung einer rechtswidrigen Verarbeitung personenbezogener Daten ermittelt, geeignete technische Maßnahmen gegen diese Risiken ergriffen und technische Kontrollen der getroffenen Maßnahmen durchgeführt.
- Durch die Einrichtung von Zugriffsverfahren in der Praxis werden Reporting- und Analysestudien zum Zugriff auf personenbezogene Daten durchgeführt.
- Unzulässige Zugriffe oder Zugriffsversuche werden durch die Protokollierung der Zugriffe auf die Speicherbereiche, in denen personenbezogene Daten gespeichert sind, unter Kontrolle gehalten.
- Die Praxis ergreift die erforderlichen Maßnahmen, um die gelöschten personenbezogenen Daten für die betreffenden Nutzer unzugänglich und wiederverwendbar zu machen.
- Für den Fall, dass personenbezogene Daten von anderen unrechtmäßig erlangt werden, hat die Praxis ein System und eine Infrastruktur eingerichtet, um die betroffene Person und den Vorstand zu benachrichtigen.
- Sicherheitslücken werden verfolgt, entsprechende Sicherheitspatches installiert und Informationssysteme auf dem neuesten Stand gehalten.
- In elektronischen Umgebungen, in denen personenbezogene Daten verarbeitet werden, werden sichere Passwörter verwendet.
- Systeme zur sicheren Aufzeichnung (Protokollierung) werden in elektronischen Umgebungen eingesetzt, in denen personenbezogene Daten verarbeitet werden.
- Zur Sicherung persönlicher Daten werden Datensicherungsprogramme eingesetzt.

- Der Zugriff auf personenbezogene Daten, die in elektronischen oder nichtelektronischen Medien gespeichert sind, ist gemäß den Zugriffsgrundsätzen eingeschränkt.
- Es ist mit dem SHA 256-Bit-RSA-Algorithmus verschlüsselt und verwendet ein sicheres Protokoll (HTTPS) für den Zugriff auf die Webseite der Institution.
- Für den Schutz sensibler personenbezogener Daten wurde eine gesonderte Richtlinie festgelegt.
- Für Mitarbeiter, die an der Verarbeitung personenbezogener Daten von besonderer Qualität beteiligt sind, wurden spezielle Schulungen zum Schutz personenbezogener Daten durchgeführt, Vertraulichkeitsvereinbarungen getroffen und die Berechtigungen der Benutzer festgelegt, die Zugriff auf die Daten haben.
- Elektronische Umgebungen, in denen sensible personenbezogene Daten verarbeitet, gespeichert und/oder abgerufen werden, werden mithilfe kryptografischer Methoden geschützt, kryptografische Schlüssel werden in sicheren Umgebungen aufbewahrt, alle Transaktionsaufzeichnungen werden protokolliert, Sicherheitsaktualisierungen der Umgebungen werden ständig überwacht, notwendige Sicherheitstests werden regelmäßig durchgeführt/ die Untersuchungsergebnisse protokollieren lassen, nachvollziehen lassen,
- Für physische Umgebungen, in denen sensible personenbezogene Daten verarbeitet, gespeichert und/oder abgerufen werden, werden angemessene Sicherheitsmaßnahmen ergriffen, und unbefugtes Betreten und Verlassen wird durch Gewährleistung der physischen Sicherheit verhindert.
- Sofern sensible personenbezogene Daten per E-Mail übermittelt werden müssen, erfolgt die Übermittlung verschlüsselt über die Firmen-E-Mail-Adresse. Wenn es über Medien wie tragbare Speicher, CDs oder DVDs übertragen werden muss, wird es mit kryptografischen Methoden verschlüsselt und der kryptografische Schlüssel wird in einer anderen Umgebung aufbewahrt. Wenn die Übertragung zwischen Servern in unterschiedlichen physischen Umgebungen erfolgt, erfolgt die Datenübertragung durch die Einrichtung eines VPN zwischen Servern oder mithilfe der sFTP-Methode. Wenn die Übermittlung über Papiermedien erforderlich ist, werden die erforderlichen Vorkehrungen gegen Risiken wie Diebstahl, Verlust oder Einsichtnahme des Dokuments durch Unbefugte getroffen und das Dokument in einem „vertraulichen“ Format versendet.

5.2. Verwaltungsmaßnahmen

Nachfolgend sind die von der Praxis ergriffenen Verwaltungsmaßnahmen zur rechtmäßigen Verarbeitung und zum Schutz personenbezogener Daten aufgeführt:

- Das Praxispersonal wird über das Gesetz zum Schutz personenbezogener Daten und die gesetzeskonforme Verarbeitung personenbezogener Daten informiert und geschult.
- Alle von der Praxis durchgeführten Tätigkeiten zur Verarbeitung personenbezogener Daten; Die Durchführung erfolgt auf Grundlage des Personendatenverzeichnisses und seiner Anhänge, das durch eine detaillierte Analyse aller Geschäftsbereiche erstellt wird.
- Tätigkeiten zur Verarbeitung personenbezogener Daten durch die zuständigen Abteilungen innerhalb der Praxis; Die Pflichten, die erfüllt werden müssen, um sicherzustellen, dass diese Aktivitäten den von der KVKK geforderten Anforderungen an die Verarbeitung personenbezogener Daten entsprechen, sind an schriftliche Richtlinien und Verfahren der Praxis gebunden, und jede Geschäftseinheit wurde über dieses Problem und die zu berücksichtigenden Punkte informiert insbesondere der von ihm ausgeübten Tätigkeit ermittelt wurden.
- Bevor mit der Verarbeitung personenbezogener Daten begonnen wird, kommt das Amt seiner Informationspflicht gegenüber den betroffenen Personen nach.
- Die Überwachung und Verwaltung der Abteilungen innerhalb der Praxis hinsichtlich der Sicherheit personenbezogener Daten wird von den Informationssicherheitsausschüssen organisiert. Es wird Bewusstsein geschaffen, um die auf Basis der Geschäftseinheit festgelegten rechtlichen Anforderungen zu erfüllen, und die erforderlichen Verwaltungsmaßnahmen werden durch praxisnahe Richtlinien, Verfahren und Schulungen umgesetzt, um die Überwachung dieser Themen und die Kontinuität der Anwendung sicherzustellen..
- Die Dienstleistungsverträge und zugehörigen Dokumente zwischen der Praxis und den Mitarbeitern, einschließlich Informationen zu personenbezogenen Daten und Datensicherheit, werden erfasst und ergänzende Protokolle erstellt. Um bei den Mitarbeitern hierfür das nötige Bewusstsein zu schaffen, wurden Studien durchgeführt.

- Die Zugriffsrechte auf physische Umgebungen, die personenbezogene Daten enthalten, sind begrenzt.
- Besonders qualifizierte personenbezogene Daten werden in dem für das bestehende Gesundheitsteam reservierten physischen Bereich innerhalb der Praxis gespeichert und sind für den Zugriff gesperrt.
- Die in der Praxis durchgeführten Tätigkeiten zur Verarbeitung personenbezogener Daten werden regelmäßig überprüft.
- Die unterzeichneten Verträge enthalten Datenschutzbestimmungen.
- Bei der Übermittlung personenbezogener Daten auf Papier werden zusätzliche Sicherheitsmaßnahmen ergriffen und das entsprechende Dokument im vertraulichen Dokumentenformat versendet.
- Interne regelmäßige und/oder stichprobenartige Audits werden durchgeführt und durchgeführt.
- Die Sicherheit physischer Umgebungen, die personenbezogene Daten enthalten, vor externen Risiken (Feuer, Überschwemmung usw.) ist gewährleistet.

## 5.2.A. Überwachung der Maßnahmen zum Schutz personenbezogener Daten

Gemäß Artikel 12 Absatz 3 des Gesetzes zum Schutz personenbezogener Daten ist der Datenverantwortliche ist verpflichtet, in der eigenen Einrichtung oder Organisation die erforderlichen Kontrollen durchzuführen oder durchführen zu lassen, um die Umsetzung der Bestimmungen dieses Gesetzes sicherzustellen.

Die Praxis führt bzw. lässt die erforderlichen Kontrollen durchführen, um die oben beschriebene Datensicherheit herzustellen und die Regelmäßigkeit und Kontinuität der getroffenen Maßnahmen sicherzustellen.

5.2.B. Maßnahmen im Falle einer unrechtmäßigen Offenlegung personenbezogener Daten

Im Rahmen der von der Praxis durchgeführten Verarbeitung personenbezogener Daten Wenn die personenbezogenen Daten von Unbefugten unrechtmäßig erlangt werden, wird die Situation unverzüglich dem KVK-Vorstand und den betreffenden Dateneigentümern gemeldet.

**6. TECHNIKEN ZUR ENTSORGUNG PERSÖNLICHER DATEN**

Von der Praxis erhobene personenbezogene Daten gemäß KVKK und anderen relevanten Rechtsvorschriften werden durch die Praxis von Amts wegen oder auf Antrag der relevanten Person mit den unten angegebenen Techniken in Übereinstimmung mit den Bestimmungen des Gesetzes und der einschlägigen Gesetzgebung vernichtet, sofern die im Gesetz aufgeführten Zwecke der Verarbeitung personenbezogener Daten und die Die Regulierung hört auf zu existieren. .

6.1. Löschung personenbezogener Daten

Die Verfahren und Grundsätze bezüglich der Techniken zur Löschung und Vernichtung personenbezogener Daten Die Daten der Praxis sind unten aufgeführt.

**Sicheres Löschen personenbezogener Daten auf Servern aus der Software:**Beim Löschen von Daten, die vollständig oder teilweise automatisiert verarbeitet und in digitalen Medien gespeichert wurden; Sie werden gelöscht, indem die Methoden zum Löschen der Daten aus der entsprechenden Software verwendet werden, sodass sie für die relevanten Benutzer in keiner Weise zugänglich und unbrauchbar sind.

Im Falle der Löschung der relevanten Daten im Cloud-System durch Erteilung eines Löschbefehls; Entfernen der Zugriffsrechte des betreffenden Benutzers auf die Datei oder das Verzeichnis, in dem sich die Datei auf dem zentralen Server befindet; Löschen relevanter Zeilen in Datenbanken mit Datenbankbefehlen oder Löschen von Daten in tragbaren Medien, also in Flash-Medien, mit geeigneter Software.

Allerdings ist eine Löschung personenbezogener Daten in der Praxis ggf. erforderlich Bei Unzugänglichkeit anderer Daten innerhalb des Systems und der Unmöglichkeit der Nutzung dieser Daten gelten personenbezogene Daten als gelöscht, wenn die personenbezogenen Daten in einer Weise archiviert werden, die nicht mit der betroffenen Person in Verbindung gebracht werden kann, sofern die folgenden Voraussetzungen erfüllt sind.

Ergreifen aller Arten technischer und administrativer Maßnahmen, um sicherzustellen, dass personenbezogene Daten nur autorisierten Personen zugänglich sind.

**Sicheres Löschen durch Experten:**Die Praxis kann mit einem Experten vereinbaren, personenbezogene Daten in ihrem Namen zu löschen, wenn sie dies für erforderlich hält. In diesem Fall werden die personenbezogenen Daten von der Person, die sich mit diesem Thema auskennt, sicher gelöscht, sodass sie für die relevanten Benutzer nicht zugänglich und in keiner Weise wiederverwendet werden können.

**Schwärzung personenbezogener Daten in Papiermedien:**Um die unbeabsichtigte Verwendung personenbezogener Daten zu verhindern oder die zu löschenden Daten zu löschen, können personenbezogene Daten durch physisches Ausschneiden und Entfernen der relevanten personenbezogenen Daten aus dem Dokument oder durch Unsichtbarmachen und Verschließen mit fester Tinte gelöscht werden können mit technischen Lösungen nicht wiederhergestellt und gelesen werden.

**Tabelle -4: Löschung personenbezogener Daten**

| Datenaufzeichnungsumgebung | Erläuterung |
|---|---|
| **Standort auf Servern Feldpersonal Daten** | Der Systemadministrator entzieht den betreffenden Benutzern die Zugriffsberechtigung und löscht die personenbezogenen Daten auf den Servern derjenigen, deren Zeitspanne abgelaufen ist. |
| **Elektronisch** Platzieren Sie in der Umgebung **Feldpersonal Daten** | Unter den personenbezogenen Daten in der elektronischen Umgebung werden diejenigen, die aufbewahrt werden müssen, für andere Mitarbeiter (zugehörige Benutzer) mit Ausnahme des Datenbankadministrators unzugänglich und in keiner Weise wiederverwendbar gemacht. |
| In der physischen Umgebung **Persönlich inklusive Daten** | Persönliche Daten, die in der physischen Umgebung aufbewahrt werden, werden für andere Mitarbeiter unzugänglich und in keiner Weise wiederverwendbar gemacht, mit Ausnahme des für das Dokumentenarchiv verantwortlichen Abteilungsleiters für diejenigen, deren Zeitspanne abgelaufen ist. Darüber hinaus wird der Prozess der Schwärzung durch Zeichnen/Malen/Radieren in einer nicht lesbaren Weise angewendet. |
| **tragbar** in den Medien **Persönlich gefunden Daten** | Von den persönlichen Daten, die auf Flash-basierten Speichermedien gespeichert sind, werden die abgelaufenen Daten vom Systemadministrator verschlüsselt und die Zugriffsberechtigung wird nur dem Systemadministrator erteilt, und sie werden in sicheren Umgebungen mit Verschlüsselungsschlüsseln gespeichert. |

6.2. Vernichtung personenbezogener Daten

Nachfolgend sind die von unserer Praxis anzuwendenden Entsorgungsmethoden aufgeführt:

**Entmagnetisieren** **:**Magnetische Medien im hohen Magnetfeld

Dabei handelt es sich um eine Methode, die darauf befindlichen Daten durch physische Veränderungen unleserlich zu verfälschen.

**Physische Zerstörung:**Personenbezogene Daten können auch auf nichtautomatische Weise verarbeitet werden, sofern sie Teil eines Datenaufzeichnungssystems sind. Dabei handelt es sich um den Prozess der physischen Zerstörung solcher Daten, sodass sie später nicht mehr verwendet werden können. Insbesondere werden auf diese Weise beschriebene Papiere und Notizbücher sowie Mikrobelege vernichtet.

**Überschreiben** **:**Überschreibmethode, magnetische Medien mittels spezieller Software

Es handelt sich um eine Datenvernichtungsmethode, die es unmöglich macht, alte Daten zu lesen und wiederherzustellen, indem zufällige Daten, die aus Nullen und Einsen bestehen, mindestens achtmal auf wiederbeschreibbare optische Medien geschrieben werden.

**Wolkenzerstörung:**Hierbei handelt es sich um den Prozess der Vernichtung aller Kopien der Verschlüsselungsschlüssel personenbezogener Daten, nachdem die Vernichtung der in Cloud-Systemen gespeicherten personenbezogenen Daten an den beauftragten Dienstleister erfolgt ist.

**Zerstörung personenbezogener Daten in Umweltsystemen:**Geräte, die personenbezogene Daten in Systemen wie Druckern, Fingerabdruckgeräten oder Drehkreuzen enthalten, werden durch Überschreiben, Magnetisieren oder physische Zerstörung zerstört. Diese Zerstörungsprozesse werden durchgeführt, bevor die Geräte Sicherungs-, Wartungs- und ähnlichen Prozessen unterzogen werden.

**Tabelle -5: Vernichtung personenbezogener Daten**

| **Datenaufzeichnung**<br>**Umfeld** | **Erläuterung** |
|---|---|
| **Physisch**<br>**Platzieren Sie in der Umgebung**<br>**Feldpersonal**<br>**Daten** | Von den personenbezogenen Daten auf dem Papiermedium werden diejenigen, die aufbewahrt werden müssen und abgelaufen sind, in den Büroklammermaschinen unwiderruflich zerstört. |
| **Optisch / Magnetisch**<br>**In den Medien platzieren**<br>**Feldpersonal**<br>**Daten** | Dabei kommt die physische Zerstörung personenbezogener Daten auf optischen und magnetischen Datenträgern zum Beispiel durch Einschmelzen, Verbrennen oder Pulverisieren zum Einsatz. Darüber hinaus werden magnetische Medien durch ein spezielles Gerät geleitet und die darauf befindlichen Daten werden unlesbar, indem sie einem hohen Magnetfeld ausgesetzt werden. |

## 6.2. Anonymisierung personenbezogener Daten

Die Anonymisierung personenbezogener Daten bedeutet, dass personenbezogene Daten, auch wenn diese mit anderen Daten verknüpft werden, in keinem Fall einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können.

Damit personenbezogene Daten anonymisiert werden; Personenbezogene Daten dürfen nicht mehr einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden, auch wenn geeignete Techniken für das Aufzeichnungsmedium und den jeweiligen Tätigkeitsbereich eingesetzt werden, wie z. B. die Rückgabe der personenbezogenen Daten durch den Verantwortlichen oder Dritte und/oder der Abgleich der Daten mit andere Daten.

## 6.3.A. Anonymisierungsmethoden, die keine Wertverzerrung gewährleisten

Ohne Änderung oder Ergänzung/Löschung der gespeicherten personenbezogenen Daten; sind Methoden der Anonymisierung, bei denen eine beliebige Gruppe personenbezogener Daten verallgemeinert, durch eine andere ersetzt oder eine bestimmte Daten- oder Teildatengruppe aus der Gruppe entfernt wird.

**Variablensubtraktion:**Der vorhandene Datensatz wird anonymisiert, indem die „hochgradig beschreibenden“ Variablen aus den Variablen im Datensatz entfernt werden, der nach der Datenerfassung durch die Extraktionsmethode deskriptiver Daten erstellt wurde.

**Datensätze extrahieren:**Bei der Deregistrierungsmethode werden die gespeicherten Daten anonymisiert, indem Datenzeilen subtrahiert werden, die Singularitäten zwischen den Daten enthalten. Wenn es in einem Unternehmen beispielsweise nur einen leitenden Manager gibt, können die verbleibenden Daten anonymisiert werden, indem die zu dieser Person gehörenden Daten aus den Aufzeichnungen entfernt werden, in denen Dienstalters-, Gehalts- und Geschlechtsdaten der Mitarbeiter auf derselben Ebene gespeichert sind.

**Regionales Versteck:**Da bei der Methode des regionalen Ausblendens einzelne Daten eine sehr selten sichtbare Kombination erzeugen, sorgt das Ausblenden der relevanten Daten für eine Anonymisierung, wenn sie ein entscheidendes Merkmal aufweisen. Wenn beispielsweise nur eine Person unter den relevanten Datenverantwortlichen in der Reserveliste der Fußballmannschaft des Unternehmens 65 Jahre alt ist, in einem Datensatz, in dem die Informationen darüber enthalten sind, ob sie oder er im Hinblick auf Alter, Geschlecht und Gesundheitszustand Fußball spielen kann Wenn alle Daten zusammen gespeichert werden, wird „Alter:65“ als „Unbekannt“ geschrieben oder dieser Teil bleibt leer. sorgt für Anonymisierung.

**Codierung der unteren und oberen Grenze:**Bei der Unter- und Obergrenzen-Kodierungsmethode werden die Werte in einer Datengruppe, die vordefinierte Kategorien enthält, anonymisiert, indem ein bestimmtes Kriterium ermittelt und kombiniert wird.

**Verallgemeinerung:**Bei der Datenaggregationsmethode werden viele Daten aggregiert und personenbezogene Daten werden nicht mehr einer Person zugeordnet. Zum Beispiel; Dies zeigt, dass es bis zu Z Mitarbeiter im Alter von X gibt, ohne das Alter der Mitarbeiter einzeln anzugeben.

**Globale Codierung:**Mit der Datenableitungsmethode wird ein allgemeinerer Inhalt als der Inhalt der personenbezogenen Daten geschaffen und sichergestellt, dass die personenbezogenen Daten keiner Person zugeordnet werden können. Zum Beispiel; Angabe des Alters statt Geburtsdatum, Angabe der Wohnregion statt offener Adresse.

### 6.3.B. Anonymisierungsmethoden, die zu Wertverzerrungen führen

Anonymisierungsmethoden, die Wertunregelmäßigkeiten bereitstellen, führen im Gegensatz zu Methoden, die keine Wertunregelmäßigkeiten bereitstellen, zu Korruption, indem sie einige Daten in Gruppen personenbezogener Daten ändern. Bei der Verwendung dieser Methoden müssen Abweichungen entsprechend dem erwarteten/gewünschten Nutzen sorgfältig angewendet werden. Indem sichergestellt wird, dass sich die Gesamtstatistik nicht verschlechtert, kann der erwartete Nutzen aus den Daten fortgesetzt werden.

**Rauschen hinzufügen:**Die Methode zum Hinzufügen von Rauschen zu den Daten wird anonymisiert, indem einige positive oder negative Abweichungen mit einer bestimmten Rate zu den vorhandenen Daten hinzugefügt werden, insbesondere in einem Datensatz, in dem numerische Daten vorherrschen. Beispielsweise wird in einem Datensatz mit Gewichtswerten (+/−) eine Abweichung von 3 kg verwendet, um die Anzeige der tatsächlichen Werte zu verhindern und die Daten zu anonymisieren. Die Abweichung gilt für jeden Wert gleichermaßen.

**Mikro-Join:**Bei der Mikroaggregationsmethode werden alle Daten zunächst in einer sinnvollen Reihenfolge (von groß nach klein) gruppiert und der durch die Durchschnittsbildung der Gruppen erhaltene Wert anstelle der relevanten Daten in der aktuellen Gruppe geschrieben, wodurch Anonymität gewährleistet wird .

(Zum Beispiel für Gehaltsinformationen: Wenn zwei Gruppen mit einem Gehalt von weniger als oder gleich 10.000 TL gebildet werden, wird die Summe der Die Gehälter von Personen mit einem Gehalt von 10.000 oder weniger werden durch die Anzahl der Personen dividiert und dieser erhaltene Wert wird in die Tabelle eingetragen Gehaltssatz für alle, die ein Gehalt von weniger als 10.000 TL erhalten.)

**Datenaustausch:**Bei der Datenaustauschmethode werden die Werte einer Variablen zwischen den aus den gespeicherten Daten ausgewählten Paaren ausgetauscht. Ziel dieser Methode, die für allgemein kategorisierbare Daten eingesetzt wird, ist die Transformation der Datenbank durch den Austausch der Daten der Dateneigentümer.

### 6.3.C. Anonymitätssicherung

Damit personenbezogene Daten anonymisiert und nicht gelöscht oder vernichtet werden können, müssen die folgenden Bedingungen erfüllt sein.

- Die Anonymität kann nicht durch die Kombination des anonymisierten Datensatzes mit einem anderen Datensatz gebrochen werden,
- Ein oder mehrere Werte können kein sinnvolles Ganzes bilden, das einen Datensatz einzigartig machen könnte.
- Die Werte im anonymisierten Datensatz fügen sich nicht zu einer Annahme oder einem Ergebnis zusammen.

## 7. LAGERUNGS- UND ENTSORGUNGSZEITEN

Über die von der Praxis im Rahmen ihrer Tätigkeit verarbeiteten personenbezogenen Daten;

- Die Aufbewahrungsfristen auf der Grundlage personenbezogener Daten für alle personenbezogenen Daten im Rahmen der im Zusammenhang mit den Prozessen durchgeführten Aktivitäten sind im Verzeichnis der Verarbeitung personenbezogener Daten aufgeführt.
- Speicherfristen auf Basis von Datenkategorien werden in Verbis erfasst;
- Prozessbasierte Aufbewahrungsfristen finden Sie in der Richtlinie zur Aufbewahrung und Entsorgung personenbezogener Daten.

stattfinden.

Bei Bedarf erfolgt eine Aktualisierung der genannten Aufbewahrungsfristen durch die Praxisleitung.

Für personenbezogene Daten, deren Aufbewahrungsfrist abgelaufen ist, erfolgt eine Löschung, Vernichtung oder Anonymisierung von Amts wegen durch die im KVK-Verfahren eingesetzten Verantwortlichen mit Zustimmung der Praxisleitung.

**Tabelle 6: Prozessbasierte Lagerungs- und Entsorgungszeitentabelle**

| ZEITRAUM | AUFBEWAHRUNGSZEITRAUM | ENTSORGUNGSZEIT |
|---|---|---|
| **Operation** Transaktionen | 10 Jahre | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **von Verträgen Vorbereitung** | Vertragsende 10 nach Ablauf Jahr | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **Operation** Kommunikation **der Aktivitäten** Ausführung | Ende der Aktivität 10 nach Ablauf Jahr | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **Personalwesen von Prozessen Ausführung** | Ende der Aktivität 10 nach Ablauf Jahr | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **Protokollverfolgung Systeme** | 2 Jahre | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **Hardware und** Zugriff auf die Software **von Prozessen Ausführung** | 2 Jahre | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **von Verträgen Vorbereitung** | 10 Jahre | Innerhalb von 180 Tagen nach Ende der Aufbewahrungsfrist |
| Lohn- und Gehaltsabrechnung | Ende der Geschäftsbeziehung nach dessen Ablauf 10 Jahre | Innerhalb von 180 Tagen nach Ende der Aufbewahrungsfrist |
| **Bildungsunterlagen** Einreichung | 10 Jahre | Innerhalb von 180 Tagen nach Ende der Aufbewahrungsfrist |
| **Besucher und Treffen seiner Teilnehmer** Anmeldung | Ende der Veranstaltung seit dessen Ablauf 2 Jahre | Bei der ersten periodischen Entsorgungsperiode nach dem Ende der Lagerzeit |
| **Zahlungsverkehr** | Ende der Geschäftsbeziehung seit dessen Ablauf 1 Jahr | Innerhalb von 180 Tagen nach Ende der Aufbewahrungsfrist |

## 8. REGELMÄßIGE ENTSORGUNGSZEIT

Gemäß Artikel 11 der Verordnung hat unsere Praxis den Zeitraum der regelmäßigen Vernichtung auf 6 Monate festgelegt. Dementsprechend wird in unserer Praxis jedes Jahr im Juni und Dezember eine periodische Vernichtung durchgeführt.

## 9. VERÖFFENTLICHUNG UND SPEICHERUNG DER POLITIK

Die Richtlinie wird in zwei verschiedenen Medien veröffentlicht, mit Nasssignatur (gedrucktes Papier) und elektronisch, und der Öffentlichkeit auf der Website zugänglich gemacht. Das gedruckte Papierexemplar wird ebenfalls im Praxisverwaltungszentrum aufbewahrt.

## 10. AKTUALISIERUNGSZEITRAUM DER RICHTLINIE, DURCHSETZUNG UND WIDERRUF DER RICHTLINIE

Diese Richtlinie wird dem Vorstand zur Genehmigung vorgelegt und tritt nach der Genehmigung durch den Vorstand in Kraft. Der Vorstand kann bei Bedarf jederzeit Änderungen an dieser Richtlinie vornehmen. Ihre Policehttps://www.drberkantoman.com/ bei
tritt unmittelbar nach seiner Veröffentlichung in Kraft. Wird die Aufhebung der Police beschlossen, werden alte Kopien der Police mit nassen Unterschriften gekündigt und unterzeichnet (mit Kündigungsstempel oder schriftlicher Kündigung) und mindestens 5 Jahre aufbewahrt.