Dr. Berkant Oman

PRIVATE PERSÖNLICHE DATENSPEICHERUNG
UND
ENTSORGUNGSRICHTLINIE

Adresse : Kazımdirik Mah, 372/9 Straße Nr. 1 Bornova/İzmir

Telefon : +90 552 361 49 88

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

Email : oman.klinik@gmail.com

INHALT

1. ZWECK

Dr. Der Zweck dieser von der Berkant Oman Clinic erstellten Richtlinie zum Schutz und zur Verarbeitung personenbezogener Daten besteht darin, die gesetzlichen Verpflichtungen zu erfüllen, die sich aus der Entscheidung des Ausschusses für den Schutz personenbezogener Daten vom 31.01.2018 und der Nummer 2018/10 über zu ergreifende angemessene Maßnahmen ergeben durch Datenverantwortliche bei der Verarbeitung personenbezogener Daten besonderer Qualität. und die technischen und administrativen Maßnahmen, die bei der Verarbeitung personenbezogener Daten besonderer Qualität ergriffen werden. Datenbeauftragter, Dr. Berkant Oman.

2. DEFINITIONEN

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	von Dateien technisch Aspekt Lagerung, Erhaltung ein Mit Ausnahme der für die Datensicherung verantwortlichen Person oder Stelle sind es die Personen, die personenbezogene Daten innerhalb der Organisation des Datenverantwortlichen oder im Rahmen 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	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 Nr. 6698 zum Schutz personenbezogener Daten
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 Inventar verarbeiten	Daten der Verantwortlichen arbeitenzu Prozessen in Verbindung gebracht Aspekt ihre Aktivitäten zur Verarbeitung personenbezogener Daten; Zweck und Rechtsgrund der Verarbeitung personenbezogener Daten, Datenkategorie,

	Das von ihnen erstellte Inventar durch Zuordnung der übermittelten Empfängergruppe und der Gruppe der betroffenen Personen erläutert die maximale Aufbewahrungsfrist, die für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist, die für die Übermittlung ins Ausland vorgesehenen personenbezogenen Daten und die diesbezüglich ergriffenen Maßnahmen Datensicherheit.
Speziell qualifiziert **Ihre persönlichen Daten** **wird bearbeitet**	Das Beschaffen, Aufzeichnen, Speichern, Bewahren, Verändern, Umordnen, Offenlegen, Übertragen, Übernehmen, Verfügbarmachen, 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.
Speziell qualifiziert **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.
Speziell qualifiziert **Ihre persönlichen Daten** **Streichung**	Löschung personenbezogener Daten; Persönliche Daten für relevante Benutzer in irgendeiner Weise unzugänglich und unbrauchbar machen.
Speziell qualifiziert **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 privater 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, für den Fall, dass 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 **Registrierungsinformationssystem**	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

3. VERARBEITUNG VON PERSONENBEZOGENEN DATEN BESONDERER QUALITÄT

Daten über Rasse, ethnische Herkunft, politische Meinung, philosophische Überzeugung, Religion, Sekte oder andere Überzeugungen, Verkleidung und Kleidung, Mitgliedschaft in Vereinen, Stiftungen oder Gewerkschaften, Gesundheit, Sexualleben, strafrechtliche Verurteilungen und Sicherheitsmaßnahmen sowie biometrische und genetische Daten besondere Natur. sind personenbezogene Daten.

Die Praxis hält sich bei der Verarbeitung sensibler personenbezogener Daten an das Gesetz und andere gesetzliche Bestimmungen. Demnach werden besondere Kategorien personenbezogener Daten nach folgenden Grundsätzen verarbeitet:

- Einhaltung der Gesetze und Ehrlichkeitsregeln
- Bei Bedarf präzise und auf dem neuesten Stand sein
- Sie müssen mit dem Zweck, für den sie verarbeitet werden, verbunden, begrenzt und eingeschränkt sein
- Verarbeitung für bestimmte, eindeutige und legitime Zwecke
- Sie müssen für den gesetzlich vorgeschriebenen Zeitraum oder für den Zweck, für den sie verarbeitet werden, aufbewahrt werden.
- Besondere Kategorien personenbezogener Daten außer Gesundheit und Sexualleben werden von der Praxis in Fällen verarbeitet, in denen die ausdrückliche Zustimmung des Dateninhabers eingeholt wird oder in den gesetzlich vorgesehenen Fällen.
- Daten über Gesundheit und Sexualleben werden in Fällen verarbeitet, in denen die ausdrückliche Zustimmung des Dateneigentümers eingeholt wird oder zum Zweck des Schutzes der öffentlichen Gesundheit, der Durchführung medizinischer Diagnosen, Behandlungs- und Pflegedienste, der Planung und Verwaltung von Präventivmedizin, Gesundheitsdiensten und Finanzierung.

Bei der Verarbeitung von Gesundheitsdaten werden auch die Bestimmungen der Verordnung über personenbezogene Gesundheitsdaten eingehalten, die nach Veröffentlichung im Amtsblatt vom 21.06.2019 mit der Nummer 30808 in Kraft getreten ist.

4. TECHNISCHE UND ADMINISTRATIVE MASSNAHMEN ZUM SCHUTZ BESONDERER QUALITÄT PERSONENBEZOGENER DATEN

Die Praxis ergreift angemessene Maßnahmen, die von der Datenschutzbehörde erklärt wurden, um sensible personenbezogene Daten in Übereinstimmung mit dem Gesetz und den einschlägigen Rechtsvorschriften zu verarbeiten und die Sicherheit sensibler personenbezogener Daten zu gewährleisten. Nachfolgend sind die in diesem Zusammenhang getroffenen Maßnahmen aufgeführt:

4.1 ADMINISTRATIVE MASSNAHMEN

- Die Praxis führt regelmäßig Schulungen zum Thema Vertraulichkeit für Mitarbeiter durch, die an der Verarbeitung sensibler personenbezogener Daten beteiligt sind.
- Zur Gewährleistung der Datensicherheit schließt die Praxis mit ihren Mitarbeitern Vertraulichkeitsvereinbarungen ab.
- Benutzer, die Zugriff auf Daten haben, Berechtigungsumfänge und -dauern sind klar definiert und es werden regelmäßige Berechtigungsprüfungen durchgeführt.
- Mitarbeiter, die ihren Arbeitsplatz wechseln oder kündigen, werden sofort vom Zugriff auf personenbezogene Daten ausgeschlossen. In diesem Zusammenhang nimmt die Praxis die den Mitarbeitern zugeteilten Bestände unverzüglich zurück.

4.2 TECHNISCHE MASSNAHMEN

4.2.1. TECHNISCHE MASSNAHMEN IM BEZUG AUF PRIVATE QUALIFIZIERTE PERSONENBEZOGENE DATEN, DIE IN EINER ELEKTRONISCHEN UMGEBUNG GESPEICHERT UND/ODER ZUGRIFFEN WERDEN

- Besondere Kategorien personenbezogener Daten werden mit kryptografischen Verfahren gespeichert.
- Kryptografische Schlüssel werden in sicheren und unterschiedlichen Umgebungen aufbewahrt.
- Transaktionsaufzeichnungen aller mit sensiblen persönlichen Daten durchgeführten Aktionen werden sicher angemeldet.
- Sicherheitsupdates von Umgebungen mit sensiblen personenbezogenen Daten werden ständig überwacht, notwendige Sicherheitstests werden regelmäßig durchgeführt und Testergebnisse protokolliert.
- Für Software, die auf sensible personenbezogene Daten zugreift, werden Benutzerberechtigungen erteilt, Sicherheitstests dieser Software regelmäßig durchgeführt und Testergebnisse protokolliert.
- In Fällen, in denen aus der Ferne auf private personenbezogene Daten zugegriffen wird, kommt ein mindestens zweistufiges Verifizierungssystem zum Einsatz.

4.2.2. TECHNISCHE MASSNAHMEN, DIE IM BEZUG AUF PERSONENBEZOGENE DATEN BESONDERER QUALITÄT ZU ERGREIFEN SIND, DIE IN EINER PHYSISCHEN UMGEBUNG GESPEICHERT UND/ODER ZUGRIFFEN WERDEN

- Je nach Art der sensiblen Umgebung werden angemessene Sicherheitsmaßnahmen ergriffen

  Es werden personenbezogene Daten gespeichert.

- Die physische Sicherheit dieser Umgebungen wird gewährleistet und unbefugte Ein- und Ausgänge werden verhindert.

5. ÜBERMITTLUNG VON PERSONENBEZOGENEN DATEN BESONDERER QUALITÄT

Die Praxis übermittelt sensible personenbezogene Daten im Rahmen der in den Artikeln 8 und 9 des Gesetzes festgelegten Datenverarbeitungsbedingungen. Um die Datensicherheit zu gewährleisten, wendet die Praxis bei der Datenübermittlung die folgenden Regeln an und führt in diesem Rahmen regelmäßige Prüfungen durch.

5.1. ÜBERTRAGUNG PER E-MAIL

In Fällen, in denen sensible personenbezogene Daten per E-Mail übertragen werden, erfolgt die Übertragung mit einer verschlüsselten Firmen-E-Mail-Adresse oder über ein Registered Electronic Mail (KEP)-Konto.

5.2. ÜBERTRAGUNG DURCH MEDIEN, WIE TRAGBARE SPEICHER, CD, DVD

In Fällen, in denen personenbezogene Daten besonderer Qualität über Medien wie tragbare Speicher, CDs, DVDs übertragen werden, erfolgt die Verschlüsselung mit kryptografischen Methoden und der kryptografische Schlüssel wird in einer anderen Umgebung aufbewahrt.

5.3. ÜBERTRAGUNG ZWISCHEN SERVERN IN VERSCHIEDENEN PHYSISCHEN UMGEBUNGEN

Bei der Übertragung sensibler personenbezogener Daten zwischen Servern in unterschiedlichen physischen Umgebungen erfolgt die Datenübertragung durch die Einrichtung eines VPN zwischen Servern oder per SFTP-Methode.

5.4. ÜBERTRAGUNG DURCH PAPIERMEDIEN

Müssen sensible personenbezogene Daten auf Papier übertragen werden, werden die notwendigen Vorkehrungen gegen Risiken wie Diebstahl, Verlust oder Einsichtnahme des Dokuments durch Unbefugte getroffen und das Dokument in Form von „vertraulichen Dokumenten“ versendet.

6. SPEICHERUNG UND ENTSORGUNG PRIVATER PERSONENBEZOGENER DATEN

Personenbezogene Daten besonderer Qualität werden in den folgenden Fällen in Übereinstimmung mit dem Gesetz und anderen Rechtsvorschriften der Praxis sowie den vom Vorstand veröffentlichten angemessenen Vorsichtsmaßnahmen, die von Datenverantwortlichen bei der Verarbeitung personenbezogener Daten besonderer Qualität zu treffen sind, gespeichert:

- Einholung der ausdrücklichen Einwilligung der betroffenen Person

- Die Tatsache, dass die Speicherung sensibler personenbezogener Daten außer Gesundheit und Sexualleben gesetzlich vorgeschrieben ist
- Speicherung von Daten über Gesundheit und Sexualleben zum Zweck des Schutzes der öffentlichen Gesundheit, der Durchführung von Präventivmedizin, medizinischer Diagnose, Behandlungs- und Pflegediensten, Planung und Verwaltung von Gesundheitsdiensten und Finanzierung
- Private personenbezogene Daten, die von der Praxis gemäß dem Gesetz und anderen Rechtsvorschriften gespeichert werden, werden von Amts wegen oder auf Antrag des Dateneigentümers gelöscht, vernichtet oder anonymisiert, wenn folgende Gründe vorliegen:
- In Fällen, in denen die private Datenspeicherung auf der ausdrücklichen Einwilligung des Dateneigentümers beruht, wird die ausdrückliche Einwilligung widerrufen.
- Der Zweck der Speicherung sensibler personenbezogener Daten wurde erreicht, unmöglich gemacht oder auf andere Weise beseitigt.
- Änderung oder Aufhebung der gesetzlichen Bestimmungen, die die Grundlage für die Speicherung sensibler personenbezogener Daten bilden
- Sämtliche Verarbeitungsbedingungen gemäß Artikel 6 des Gesetzes sind weggefallen

- Wenn der Antrag des Dateneigentümers auf Vernichtung der ordnungsgemäß an die Praxis übermittelten sensiblen personenbezogenen Daten begründet ist und von der Praxis positiv abgeschlossen wird
- In Fällen, in denen die Praxis den Antrag des Dateneigentümers mit der Bitte um Vernichtung sensibler personenbezogener Daten ablehnt, wenn die von ihr gegebene Antwort unzureichend ist oder wenn sie nicht innerhalb der im Gesetz vorgesehenen Frist antwortet; Beschwerde beim Vorstand und Genehmigung dieses Antrags durch den Vorstand.

7. BESONDERE QUALITÄTSTECHNIKEN ZUR ENTSORGUNG PERSONENBEZOGENER DATEN

Für den Fall, dass die im Gesetz und in der Verordnung aufgeführten Zwecke der Verarbeitung personenbezogener Daten nicht mehr bestehen, werden die von der Praxis gemäß der KVKK und anderen relevanten Rechtsvorschriften erfassten personenbezogenen Daten von Amts wegen mit den folgenden Techniken verarbeitet oder auf Antrag der relevanten Person gemäß den Bestimmungen des Gesetzes und der einschlägigen Gesetzgebung. wird zerstört werden.

7.1. PRIVATE PERSONENBEZOGENE DATEN LÖSCHEN

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

7.1.1. SICHERE LÖSUNG PERSONENBEZOGENER DATEN AUF DEN 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.

Wenn jedoch die Löschung personenbezogener Daten, sofern erforderlich, dazu führt, dass andere Daten innerhalb des Systems nicht mehr zugänglich sind und diese Daten nicht verwendet werden können, gelten die personenbezogenen Daten auch dann als gelöscht, wenn die personenbezogenen Daten in einer Weise archiviert werden, die nicht möglich ist mit der betroffenen Person in Verbindung gebracht werden, sofern die folgenden Voraussetzungen erfüllt sind.

- Für den Zugriff anderer Institutionen, Organisationen oder Personen gesperrt sein,
- Ergreifen aller erforderlichen technischen und administrativen Maßnahmen, um sicherzustellen, dass personenbezogene Daten nur autorisierten Personen zugänglich sind.

7.1.2. SICHERES LÖSCHEN DURCH EINEN 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.

7.1.3. SCHWÄRZUNG PERSONENBEZOGENER DATEN IN EINER PAPIERUMGEBUNG

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: LÖSCHEN PERSONENBEZOGENER DATEN

Datenaufzeichnungsumgebung	Erläuterung
Befindet sich auf Servern **Persönliche Daten**	Der Systemadministrator entzieht den betreffenden Benutzern die Zugriffsberechtigung und löscht die personenbezogenen Daten auf den Servern derjenigen, deren Zeitspanne abgelaufen ist.
Elektronisch **Persönlich inklusive 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.
Standort in der physischen Umgebung **Feld personenbezogene 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.
Auf tragbaren 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.

7.2. Vernichtung privater personenbezogener Daten

Nachfolgend sind die von unserer Praxis anzuwendenden Entsorgungsmethoden aufgeführt.

7.2.1. ENTMAGNETISIERUNG

Dabei handelt es sich um die Methode, die darauf befindlichen Daten unleserlich zu verfälschen, indem das magnetische Medium physikalischen Veränderungen in einem starken Magnetfeld ausgesetzt wird.

7.2.2. PHYSIKALISCHE 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. Vor allem Schreibpapier, Notizbücher und Mikrofiche werden auf diese Weise vernichtet.

7.2.3. ÜBERSCHREIBEN

Überschreibmethode, zufällige Daten bestehend aus Nullen und Einsen mindestens achtmal über magnetische Medien und wiederbeschreibbare optische Medien mittels spezieller Software

Es handelt sich um eine Datenvernichtungsmethode, die es unmöglich macht, alte Daten durch Schreiben zu lesen und wiederherzustellen.

7.2.4. Cloud-Entsorgung

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.

7.2.5. ENTSORGUNG 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: ZERSTÖRUNG VON PERSONENBEZOGENEN DATEN BESONDERER QUALITÄT

Datenaufzeichnungsumgebung	Erläuterung
Standort in der physischen Umgebung **Feld personenbezogene Daten**	Von den personenbezogenen Daten auf dem Papiermedium werden diejenigen, die aufbewahrt werden müssen und abgelaufen sind, in den Büroklammermaschinen unwiderruflich zerstört.
Optisch / Magnetisch **In den Medien vorgestellt** **Persönliche 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.

7.3. Anonymisierung privater 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.

7.3.1. METHODEN DER ANKÜNDIGUNG, DIE KEINE WERTBEWÄSSERUNG BIETEN

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.

7.3.2. Methoden zur Sicherung der Wertstörung

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 Micro-Joining-Methode werden zunächst alle Daten in eine sinnvolle Reihenfolge gebracht.*(von groß nach klein)*Die Anonymisierung wird erreicht, indem die Gruppen in Gruppen aufgeteilt werden und der erhaltene Wert durch die Verwendung des Durchschnitts der Gruppen anstelle der relevanten Daten in der aktuellen Gruppe geschrieben wird.

(Zum Beispiel für Gehaltsinformationen: Wenn zwei Gruppen mit einem Gehalt von weniger als oder gleich 10.000 TL gebildet werden, gilt das Die Summe der Gehälter von Personen mit einem Gehalt von 10.000 oder weniger wird durch die Anzahl der Personen und diesen Wert geteilt Der erhaltene Betrag wird in die Gehaltsliste aller Personen eingetragen, 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.

7.3.3 ANONYME ZUSICHERUNG

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.

8. 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 sind in der Richtlinie zur Aufbewahrung und Entsorgung personenbezogener Daten enthalten.

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

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

9. AKTUALISIEREN

Die an dieser Richtlinie vorgenommenen Änderungen sind in der folgenden Tabelle aufgeführt.

Datum der Richtlinienaktualisierung	Änderungen
07.04.2021	