Dokumentation
Datenschutz-Management der
Praxis für Physiotherapie Natalie Tollas

Stand des Dokuments 24.05.2018

Die Datenschutz-Grundverordnung DSGVO bzw. EU-DSGVO verpflichtet alle Organisationen, Unternehmen und Freiberufler einen angemessenen Datenschutz für die gespeicherten bzw. „verarbeiteten“ personenbezogenen Daten sicherzustellen. Ein Datenschutz-Management ist zu implementieren und zu dokumentieren.

Das vorliegende Dokument zeigt, welche Vorkehrungen und Regelungen (Strukturen und Verfahren) in der Praxis für Physiotherapie Natalie Tollas eingerichtet wurden, um den Anforderungen des Datenschutzes gerecht zu werden.

Inhaltsverzeichnis

1 Einführung

Die Verarbeitung personenbezogener Daten unterliegt den Regelungen der Datenschutz-Grundverordnung (DSGVO). Ab dem 25.05.2018 gilt die DSGVO in allen Ländern der Europäischen Union und löst die zuvor geltende Datenschutzrichtlinie sowie das deutsche Bundesdatenschutzgesetz (BDSG) ab. Flankiert wird die DSGVO durch das BDSG-neu, in welchem sich ergänzende Regelungen befinden.

Ziel der DSGVO ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere der Schutz der personenbezogenen Daten.

Das Recht auf Schutz der personenbezogenen Daten ist jedoch kein uneingeschränktes Recht. Es steht dem gesellschaftlichen Bedarf an freiem Verkehr auch personenbezogener Daten gegenüber. Ziel und Aufgabe des Datenschutzrechtes ist daher die Schaffung eines gerechten Interessenausgleichs zwischen den Verarbeitern von Daten und den Betroffenen. So muss der Schutz der personenbezogenen Daten unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Die DSGVO verwendet in diesem Zusammenhang den Begriff „Treu und Glauben“, im Sinne einer fairen Verarbeitung von Daten.

An dieser Stelle soll darauf hingewiesen werden, dass die DSGVO keine Anwendung findet, wenn natürliche Personen personenbezogene Daten ausschließlich zu privaten oder familiären Zwecken verarbeitet werden. Auch umfasst die DSGVO nicht den Schutz der Daten von juristischen Personen oder von Verstorbenen.

„Personenbezogene Daten“ sind im Sinne der DSGVO alle Informationen, die sich auf eine (identifizierte oder identifizierbare) natürliche Person beziehen. Dies sind z.B.

- Name
- Identifikationsmerkmale wie Ausweisnummer, Geburtsdatum, Onlinekennung
- Adressdaten wie die Postanschrift, Emailadresse, Telefonnummer, Bankverbindung.
- Körperliche Merkmale wie Größe, Gewicht, Fingerabdruck, Augenfarbe, Haarfarbe, Blutgruppe, DNA-Profil, Krankheiten.
- Intellektuelle und mentale Merkmale wie Intelligenzquotient, Einstellungen, Überzeugungen, Werturteile.
- Beziehungen wie Verwandtschaftsverhältnisse, Freundschaftsbeziehungen, Arbeitgeber, Partei- oder Vereinszugehörigkeit.
- Eigentum und Rechte wie Grundbesitz, Fahrerlaubnis, Bildungsabschluss
- Weiteres wie z.B. Nutzungs- und Standortdaten

Die DSGVO spricht bei diesen natürlichen Personen von der „betroffenen Person“ und formuliert damit den Personenkreis, welcher mir besonderen Informations-, Auskunft und Abwehrrechten ausgestattet wird.

Jede Verwendung von personenbezogenen Daten wird in der DSGVO als „Verarbeitung“ personenbezogener Daten bezeichnet.

Die Verarbeitung umfasst so z.B. das Erheben, das Erfassen, die Organisation, das Ordnen, die

Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Offenlegung, die Bereitstellung, oder das Löschen von personenbezogenen Daten.

Im Gegensatz zum früheren BDSG spielt es praktisch keine Rolle, ob die Verarbeitung mit oder ohne automatisierten Verfahren (z.B. EDV) erfolgt. Letztlich kommen heute selbst im privaten Bereich früher oder später immer auch Computer oder andere Datenverarbeitungsanlagen zum Einsatz.

Vor diesem Hintergrund beschreibt das vorliegende Dokument die Konzepte sowie die organisatorische Umsetzung des Datenschutzes, also den Schutz „personenbezogener Daten“, im Unternehmen der Praxis für Physiotherapie Natalie Tollas

2 Verarbeitungstätigkeit

2.1 Verantwortlicher

„Verantwortlicher“ ist im Sinne der DSGVO die natürliche oder juristische Person, welche über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Dies ist für diesen Praxisbetrieb:

Praxis für Physiotherapie
Natalie Tollas
Hauptstr. 7
58332 Schwelm

2.2 Gesetzlicher Vertreter

Gesetzlicher Vertreter des Unternehmens ist:
Natalie Tollas

2.3 Datenschutzbeauftragter

Der vom Unternehmen benannte Datenschutzbeauftragte ist:
Natalie Tollas

3 Verarbeitungsverzeichnis

3.1 Einführung

Nach Artikel 30 DSGVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten (personenbezogener Daten) zu erstellen. Das Verarbeitungsverzeichnis soll folgende Angaben enthalten:

(a) Name und Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten. (siehe hierzu Kapitel 2).
(b) Die Zwecke der Verarbeitung.
(c) Eine Beschreibung der Kategorien betroffener Personen und
Eine Beschreibung der Kategorien der personenbezogenen Daten.
(d) Die Kategorie der Empfänger, an welche diese Daten weitergegeben werden.
(e) Eine Darstellung, ob diese Daten an Drittländer oder internationale Organisationen weitergegeben werden.
(f) Soweit möglich, eine Darstellung der vorgesehenen Fristen zur Löschung dieser Daten.
(a) Soweit möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zum Schutz der Daten.

Anlage 1 des vorliegenden Dokuments enthält eine tabellarische Aufstellung der Verarbeitungstätigkeiten der Praxis für Physiotherapie Natalie Tollas.

Die Darstellung orientiert sich an Ausführungsbeispielen des Bayrischen Landesamt für Datenaufsicht.

Im Folgenden sind verschiedene Sachverhalt zu dieser Aufstellung ergänzend dokumentiert.

3.2 Kunden-/Patientenverwaltung und Auftragsabwicklung

3.2.1 Zweck der Verarbeitung

Wie in fast jedem Dienstleistungsbetrieb mit qualifizierten und ggf. auch dauerhaften Kundenbeziehungen ist die Verarbeitung der Kundendaten sowie der Daten der Geschäftsbeziehung ein wichtiges Element des Geschäftsmodells. Dabei ist die Verarbeitung der Daten nicht das Kerngeschäft, sondern eine Nebentätigkeit.
Sie ist erforderlich, um mit Kunden und Interessenten in Kontakt zu treten und über die üblichen Kommunkationskanäle kommunizieren zu können.
Dies ist Voraussetzung der Geschäftsanbahnung, Geschäftsabwicklung und Pflege der Geschäftsbeziehung.

Wie in der Tabelle dargestellt, können im Bereich der Kunden-/Patientenverwaltung und Auftragsabwicklung die Verarbeitungen differenziert werden, insbesondere im Bereich der Abrechnung von Leistungen.

In der Tabelle sind folgende Verarbeitungen explizit ausgewiesen:
- Verwaltung der Stammdaten Patient / Kunde
- Terminverwaltung
- Medizinische Dokumentation
- Abrechnung Kostenträger
- Abrechnung Zuzahlung
- Abrechnung Privatleistung

3.2.2 Kategorie betroffener Personen

Verarbeitet werden personenbezogene Daten zu folgenden Kategorien von Personen:
- Patienten
- Gesetzliche Vertreter von Patienten
- Begleitpersonen von Patienten
- Kunden

Branchentypisch werden Personen, welche ärztliche oder andere medizinische Leistungen in Anspruch nehmen als „Patienten“ bezeichnet.

Kunden sind dann jene Personen, die Leistungen erhalten, welche keine ärztlichen oder medizinischen Leistungen erhalten, wie z.B. Sportmassagen.

Personen welche im Rahmen der Leistungserbringung Leistungen erhalten sind Kunden, Kunden können auch Patienten sein.

3.2.3 Kategorie betroffener Daten

- Stammdaten (Anrede, Vornamen, Nachnamen, Namenszusätze, Titel)
- Postalische Adresse(n)
- Kommunikationsdaten (Telefon, Fax, Email usw.)
- Daten des Kostenträgers / Versicherung ggf. inkl. Korrespondenz
- Daten der Verordnungen inklusive der Verordner (Ärzte) und ggf. Korrespondenz
- Daten der Diagnosen / Anamnesen / Therapie
- Daten der erhaltenen Leistungen und deren Abrechnung
- Daten der kaufmännischen Dokumentation des Vertragsverhältnisses
- Daten der medizinischen Dokumentation der Leistung

Bei dem Großteil der in der Praxis für Physiotherapie Natalie Tollas verarbeiteten Daten handelt es sich um sogenannte Daten besonderer Kategorien (Art. 9 DSGVO) in Form von Gesundheitsdaten (Art. 4 Nr. 15 DSGVO), welche unter dem besonderen Schutz der Rechtsordnung und der DSGVO stehen.

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO)

3.2.4 Erlaubnistatbestand

Die Verarbeitung erfolgt aufgrund der Erfüllung einer vertraglichen Verpflichtung (Art. 6 Abs. 1 b , Art. 9 Abs. 2 h, Abs. 3 DSGVO), ggf. auch auf Basis vorvertraglicher Maßnahmen. Für die Speicherung der Daten und für die Kommunikation mit Ärzten und Krankenkassen erfolgt die Verarbeitung teilweise aufgrund gesetzlicher (rahmenvertraglicher) Verpflichtung (Art. 6 Abs. 1 c DSGVO). Die Weitergabe der Daten an das Rechenzentrum (i.S. § 302 Abs. 2 S. 2 SGB V) ist zur Wahrung unserer berechtigten Interessen erforderlich (Art. 6 Abs. 1 f DSGVO).

3.2.5 Empfänger

Die Weitergabe der Daten erfolgt je nach Zweck der Verarbeitung an den Kostenträger, welche die Leistungen bezahlt und ggf. an den Arzt, der die Verordnung ausgestellt hat. Eine Datenweitergabe erfolgt ferner an das Rechenzentrum. Details siehe Tabelle der Verarbeitungstätigkeiten.

Eine Weitergabe an Drittländer oder internationale Organisationen erfolgt nicht.

3.2.6 Löschfristen

Eine Löschung der Daten erfolgt, wenn sowohl
- keine rechtliche Verpflichtung zur Verarbeitung mehr besteht (z.B. steuerliche Aufbewahrung),
- ein Bedarf zur Verteidigung von Rechtsansprüchen ausgeschlossen ist,
- eine Fortsetzung der Geschäftsbeziehung ausgeschlossen ist.

Die Löschfristen können mit einem konkreten Zeitraum / Zeitpunkt angegeben werden oder im Form von Bedingungen, zu deren Eintritt die Löschung erfolgt. Zweiteres wurde hier gewählt. So liegt es in der Regel im Interesse der Behandlungsqualität und damit des Patienten, wenn auf die Kranken- / Behandlungshistorie bei erneuter Therapie, auch nach längerer Zeit, noch zurückgegriffen werden kann.

Nach dem Patientenrechtegesetz sind Behandlungsunterlagen 10 Jahre nach Abschluss der Behandlung aufzubewahren.
Buchhaltungsrelevante Unterlagen sind 10 Jahre aufzubewahren.
Zur Beweissicherung (Abwehr von Rechtsansprüchen) bei Schadensersatzverlangen wegen der Verletzung von Leib oder Leben können Unterlagen ggf. 30 Jahre aufzubewahren sein (vgl. § 199 Abs. 2 BGB).

3.3 Zusammenarbeit mit Ärzten

3.3.1 Zweck der Verarbeitung

Die Erbringung von medizinischen Leistungen erfolgt in der Regel auf Veranlassung (Verordnung) eines Arztes und oder im Dialog mit dem Verordner oder anderen beteiligten Leistungserbringern. Daher sind im Geschäftsbetrieb auch Daten von Ärzten zu verarbeiten.

3.3.2 Kategorie betroffener Personen

Verarbeitet werden die Daten von Ärzten und ggf. von Personen, welche in den Arztpraxen Ansprechpartner sind.

3.3.3 Kategorie betroffener Daten

- Stammdaten (Anrede, Vornamen, Nachnamen, Namenszusätze, Titel) von Ärzten und ggf. dort als Ansprechpartner tätigen Personen
- Postalische Adresse(n) der Praxisadresse.
- Kommunikationsdaten (Telefon, Fax, Email usw.) der Praxisadresse
- Daten zum Fachbereich / Leistungsangebot der Praxis

3.3.4 3.3.4. Erlaubnistatbestand

Die Zusammenarbeit der Heilmittelerbringer mit Ärzten ist in den GKV-Rahmenverträgen als auch in der Heilmittelrichtlinie vorgeschrieben. Die Verarbeitung erfolgt insofern auf Grund gesetzlicher (rahmenvertraglicher) Verpflichtung (Art. 6 Abs. 1 c DSGVO i.V.m. mit dem GKV-Rahmenvertrag und der Heilmittelrichtliche HeilMRl).

3.3.5 Empfänger

Die Weitergabe der Daten erfolgt je nach Zweck der Verarbeitung an den Kostenträger, welche die Leistungen bezahlt und ggf. an den Patienten, für den eine Verordnung ausgestellt wurde und ggf. an andere Ärzte und Leistungserbringer, die an der Behandlung des Patienten beteiligt sind, für die ein Arzt eine Verordnung ausgestellt hat. Eine Datenweitergabe erfolgt ferner an das Rechenzentrum. Details siehe Tabelle der Verarbeitungstätigkeiten.

Eine Weitergabe an Drittländer oder internationale Organisationen erfolgt nicht.

3.3.6 Löschfristen

Eine Löschung der Daten erfolgt, wenn sowohl
- keine rechtliche Verpflichtung zur Verarbeitung mehr besteht (z.B. steuerliche Aufbewahrung),
- ein Bedarf zur Verteidigung von Rechtsansprüchen ausgeschlossen ist,
- eine Fortsetzung der Geschäftsbeziehung ausgeschlossen ist.
- die Daten nicht in allgemeinen Verzeichnissen (Homepage, Telefonbuch) verfügbar sind

3.4 Personalverwaltung

3.4.1 Zweck der Verarbeitungen

Organisation und Abwicklung des Beschäftigungsverhältnisses, Erfüllung steuerlicher und sozialversicherungsrechtlicher Pflichten.

3.4.2 Kategorie betroffener Personen

Mitarbeiter des Betriebes

3.4.3 Kategorie betroffener Daten

- Anrede, Vornamen, Nachnamen, Namenszusätze, Titel
- Postalische Adresse(n)
- Kommunikationsdaten (Telefon, Fax, Email usw.)
- Daten der beruflichen Qualifikation, Aus- und Fortbildung
- Bewerbungsunterlagen
- Daten der Steuerkarte
- Bankdaten für Gehaltsüberweisung
- Daten der Arbeitszeit- und Leistungserfassung
- Krankmeldungen, Krankheitstage
- Urlaubstage
- Kirchenzugehörigkeit

3.4.4 Erlaubnistatbestand

Vertragliche Grundlage in Form des Arbeitsvertrages (Art. 6 Abs. 1 b DSGVO), Erfüllung gesetzlicher Verpflichtungen (steuer- und sozialrechtlich) (Art. 6 Abs. 1 c DSGVO), Die Datenweitergabe an den Steuerberater für die Lohnbuchhaltung ist zur Wahrung unserer berechtigten Interessen erforderlich (Art. 6 Abs. 1 f DSGVO) bzw. als zulässige Weiterverarbeitung (Art. 6 Abs. 4 DSGVO).
Die durch Art. 88 DSGVO i.V.m. § 26 BDSG aufgezeigten Grenzen der Verarbeitung von personenbezogenen Daten in Beschäftigungsverhältnissen werden beachtet.

3.5 Bewerbungs- und Auswahlverfahren

3.5.1 Zwecke

Gewinnung neuer Mitarbeiter, Durchführung des Auswahlverfahrens

3.5.2 Kategorien betroffener Personen

Bewerberinnen und Bewerber

3.5.3 Kategorien betroffener Daten

- Anrede, Vornamen, Nachnamen, Namenszusätze, Titel
- Postalische Adresse(n)
- Kommunikationsdaten (Telefon, Fax, Email usw.)
- Daten der beruflichen Qualifikation, Aus- und Fortbildung
- Bewerbungsunterlagen

3.5.4 3.5.4 Erlaubnistatbestand

Vorvertragliches Rechtsverhältnis durch Eingang der Bewerbungsunterlagen (Art. 6 Abs. 1 b DSGVO i.Vm. § 26 Abs. 1 S. 1 BDSG). Die Speicherung der Bewerbungsunterlagen bis zu drei

Monate nach der Mitteilung der Nichteinstellung erfolgt in Wahrnehmung unserer berechtigten Interessen (Art. 6 Abs. 1 f DSGVO) zur Abwehr von ungerechtfertigter Inanspruchnahme aus AGG.

3.6 Lieferanten und Sonstige

3.6.1 Zweck der Verarbeitung

Im Rahmen des Geschäftsbetriebes bestehen verschiedenste Beziehungen zu anderen Wirtschaftssubjekten wie Vermieter, Verbände, Kollegenpraxen, Lieferantenpraxen.

3.6.2 3.6.2.Kategorien betroffener Personen

Lieferanten und bei Lieferanten beschäftigte Kontaktpersonen

3.6.3 3.6.3.Kategorien betroffener Daten

- Anrede, Vornamen, Nachnamen, Namenszusätze, Titel
- Postalische Adresse(n)
- Kommunikationsdaten (Telefon, Fax, Email usw.)

3.6.4 3.6.4. Erlaubnistatbestand

Vertragliches Verhältnis (Art. 6 Abs. 1 b DSGVO), Wahrung berechtigter Interessen (Art. 6 Abs. 1 f DSGVO).

3.6.5 Löschfristen

Eine Löschung der Daten erfolgt, wenn sowohl
- keine rechtliche Verpflichtung zur Verarbeitung mehr besteht (z.B. steuerliche Aufbewahrung),
- ein Bedarf zur Verteidigung von Rechtsansprüchen ausgeschlossen ist,
- eine Fortsetzung der Geschäftsbeziehung ausgeschlossen ist.
- die Daten nicht in allgemeinen Verzeichnissen (Homepage, Telefonbuch) verfügbar sind

4 Grundsätze der Verarbeitung

4.1 Rechtmäßigkeit der Verwendung

Die Verarbeitung personenbezogener Daten natürlicher Personen ist nur rechtmäßig, wenn ein Erlaubnistatbestand gegeben ist.

Die Geschäftsprozesse des Unternehmens zielen auf die Anbahnung, Durchführung und Pflege von Geschäftsbeziehungen entsprechend dem Geschäftszweck des Unternehmens. Zu diesem Zwecke werden Daten von Geschäftspartnern und potentiellen Geschäftspartnern verarbeitet.

Dies sind in der Regel Patienten, Kunden, Ärzte, Kostenträger, Mitarbeiter, Bewerber, Lieferanten sowie sonstige Wirtschaftssubjekte zu denen Kontakte bestehen oder geplant sind.

Für diese Verwendung besteht in der Regel ein Erlaubnistatbestand nach Artikel 6. Abs. 1 lit (b) DSGVO. Er umfasst die Erfüllung eines Vertrages sowie auch die vorvertraglichen Maßnahmen. Dies ist in der Regel der zwischen der Praxis und den Patienten bestehende Behandlungsvertrag gem. § 630a BGB. Abweichende Erlaubnistatbestände sind in Kapitel **Fehler! Verweisquelle onnte nicht gefunden werden.** sowie in der Tabelle (Verarbeitungsverzeichnis) ausgewiesen..

Nach Artikel 6 Absatz 1 DSGVO sind folgende Erlaubnistatbestände möglich.

- (a) Einwilligung der betroffenen Person
- (b) Erfüllung eines Vertrages
- (c) Erfüllung rechtlicher Verpflichtung
- (d) Lebenswichtige Interessen
- (e) Wahrnehmung öffentlicher Aufgabe
- (f) Wahrung berechtigten Interesses

4.2 Fairness

Bei den verarbeiteten Daten handelt es sich um die Minimaldaten, welche für eine qualifizierte Geschäftsanbahnung und Geschäftsabwicklung üblich und erforderlich sind. Die Verarbeitung entspricht im Umfang und im Inhalt dem, was der betroffene Personenkreis erwarten würde oder aus vergleichbaren Beziehungen kennt.

4.3 Transparenz

Die betroffenen Personen sind Kunden bzw. Patienten oder Vertreter dieser Personen. Die Verarbeitung erfolgt in einem von diesem Geschäftskreisen erwartbaren Umfang. Die Praxis stellt allen betroffenen Personen bereits bei Erhebung der Daten (spätestens einen Monat nach Erhebung, wenn die Daten nicht von der Person selbst erhoben worden sind) umfassende und verständliche Informationen über die Datenverarbeitung (Art. 12 ff DSGVO) zur Verfügung. Auskunftsersuchen werden entsprechend der gesetzlichen Bedingungen bedient.

4.4 Zweckbindung

Der Zweck der Verarbeitung ist die Anbahnung, Durchführung und Pflege von Geschäftsbeziehungen entsprechend dem Geschäftszweck des Unternehmens.
Die Zwecke der Verarbeitung sind in Kapitel **Fehler! Verweisquelle konnte nicht gefunden erden.** sowie in der Tabelle (Verarbeitungsverzeichnis) dokumentiert. Eine Datenverarbeitung erfolgt nur zu den hier ausgewiesenen Zwecken.

4.5 Datenminimierung

Es werden nur die Daten verarbeitet, welche im Rahmen der Leistungserbringung, der Dokumentation, der Abrechnung und für die Pflege der Geschäftsbeziehungen erforderlich sind. Daten, die zur Erfüllung der jeweiligen Zwecke nicht mehr benötigt werden und für die keine gesetzlichen Pflichten zur Speicherung bestehen, werden gelöscht.

4.6 Richtigkeit

Die Richtigkeit der Daten liegt bereits im Interesse des Unternehmens, da sonst die Unternehmenszwecke nicht erreicht werden können.

Aus falschen Daten entstehen der Person in der Regel keine Nachteile. Hinweise auf unrichtige Daten werden vom Unternehmen aufgenommen. Die Angaben werden sodann verifiziert. Die Datensätze werden entsprechend umgehend korrigiert.

4.7 Speicherbegrenzung

Personenbezogene Daten werden in Ansehung des Verarbeitungszweckes nur so lange wie unbedingt notwendig gespeichert. Für alle Datenkategorien werden allgemeine Löschfristen festgelegt. Alle Datensätze werden in regelmäßigen Abständen auf Löschungsreife hin untersucht und gegebenenfalls einer sicheren Löschung zugeführt. Bei jeder Löschung von Daten sind durch technische und organisatorische Maßnahmen angemessene Garantien zur Wahrung der Rechte und Freiheiten der Betroffenen implementiert.
So lange Daten in öffentlichen Quellen verfügbar sind, ist auch eine Speicherung in eigenen Datenbeständen angemessen.

Widerspricht eine Person der Verwendung ihrer Daten z.B. zu Werbezwecken, kann es erforderlich sein, diese Daten mit der Information des Löschungsbegehrens weiter zu speichern. Andernfalls besteht die Gefahr, diese Daten erneut aus öffentlichen Quellen zu beziehen und zu nutzen. Die Speicherung ist auf ein Minimum Begrenzt und erfolgt im Interesse der Betroffenen selbst.

Bei bestehenden Geschäftsbeziehungen werden Daten so lange gespeichert, wie dies aus handels- und steuerrechtlichen Gründen erforderlich ist.

Aus einer Geschäftsbeziehung könnten bis zu 30 Jahren Schadensersatzansprüche aus der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit resultieren. So lange eine Person Schadensersatzansprüche geltend machen kann, kann es gerechtfertigt sein, Daten aus der Geschäftsbeziehung zu Beweiszwecken zu speichern.

4.8 Integrität und Vertraulichkeit

Die Praxis für Physiotherapie Natalie Tollas hat in Ansehung des Schutzbedarfs der verarbeiteten Daten und des mit den Verarbeitungstätigkeiten einhergehenden Risikos technische und organisatorische Maßnahmen getroffen, um einen angemessenen Schutz der Rechte und Freiheiten der Betroffenen zu erreichen.

Dies ist zum einen der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Zum anderen ist

dies der Schutz vor dem Verlust und der Zerstörung personenbezogener Daten. Diese Aspekte sind weiter unter den Stichworten Zugriffsschutz und Datensicherung behandelt. Die Grundziele der Informationssicherheit, Vertraulichkeit, Integrität und Verfügbarkeit werden beachtet.

4.9 Rechenschaft

Das vorliegende Dokument beschreibt die Konzeption und Organisation des Umgangs mit „personenbezogenen Daten“ im Unternehmen.

Alle Mitarbeiter des Unternehmens werden auf diese Konzepte und organisatorischen Vorkehrungen sensibilisiert.

In regelmäßigen Audits wird überprüft, ob Konzeption und Organisation im Alltag umgesetzt werden und ob diese noch den rechtlichen Anforderungen genügen.

5 Beurteilung des Schutzbedarfs

Für die Schutzbedürftigkeit von personenbezogenen Daten können diese in Schutzstufen eingeordnet werden.

- Stufe A
  Dies sind personenbezogene Daten, welche weitgehend frei zugänglich sind, entweder aus Veröffentlichungen der Person / Organisation selbst (z.B. Homepage, Broschüre) oder über allgemeine Verzeichnisse (Telefonbuch, Adressbücher, Verbandsverzeichnis, Mitgliederverzeichnis.)
- Stufe B
  Dies sind personenbezogene Daten, deren missbräuchliche Verwendung vermutlich keine besondere Beeinträchtigung darstellen, die jedoch nicht jedermann zugänglich sind. Hierzu gehören z.B. die Telefon-Durchwahlnummer, oder die interne Zuständigkeit in einer Organisation.
- Stufe C
  Dies sind personenbezogene Daten, deren Missbrauch die betroffene Person in ihrer gesellschaftlichen Stellung, dem Ansehen oder in den wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören Daten zu Einkommen, Sozialleistungen, Steuern, Ordnungswidrigkeiten.
- Stufe D
  Dies sind personenbezogene Daten, deren Missbrauch die betroffene Person ihn ihrer gesellschaftlichen Stellung, dem Ansehen oder in den wirtschaftlichen Verhältnissen in besonderem Maße (an die Existenz gehend) beeinträchtigen kann. Hierzu gehören Daten über Straftaten, Unterbringung in Anstalten, Schulden, Pfändungen, Insolvenzen, psychologisch-medizinische Untersuchungsergebnisse, dienstliche Beurteilungen.
- Stufe E
  Dies sind personenbezogene Daten, deren Missbrauch die Gesundheit, das Leben oder die Freiheit der betroffenen Person beeinträchtigen kann. Hier geht es um die physische Existenz. Hierzu gehören z.B. die Adressen Verdeckter Ermittler, Adressen von potentiellen Anschlagsopfern.

Patientendaten bzw. Daten zur Gesundheit / Krankheit von Personen wird in der Regel der Schutzklassen D zugeordnet.

Alleine die Tatsache, z.B. in physiotherapeutischer Behandlung zu sein, führt zwar in der Regel zu keiner Schädigung des Ansehens oder zu andern Nachteilen. Im Gegenteil gehört physiotherapeutische Behandlung eher zu gesellschaftlich positive bewerteten Leistungen. Nachteile könnten aber ggf. durch die Bekanntgabe der Diagnose entstehen, wenn diese ein Hinweis auf geistige oder körperliche Einschränkungen ergibt. Je nach Inhalt der Gesundheitsinformation erwartet der Betroffene eine hohe Vertraulichkeit. Da jedoch sämtliche Informationen über die Behandlung dem Berufsgeheimnis (§ 203 Abs. 1 Nr. 1 StGB) unterliegen, ist die generelle Einordnung von Patientendaten in die Schutzklasse D gerechtfertigt.

Verarbeitet werden: Personenstammdaten, Verordnungsdaten, Daten der Behandlungshistorie oder der Daten von Anamnese und Diagnose. Der Verlust dieser Daten stellt in der Regel keine wirtschaftliche oder gesundheitliche Bedrohung für die Person dar. Diese Daten können in der Regel von anderer Stelle wieder ermittelt werden, z.B. von der betroffenen Person, dem verordnenden Arzt, dem Kostenträger und dem behandelnden Therapeuten. Hier entsteht im Wesentlichen ein Aufwand für die Praxis. Dauerhafte Schäden sind für die Betroffenen bei einer Verletzung der Vertraulichkeit nur in Ausnahmefällen zu erwarten.

In der Regel besteht auch kein Interesse Dritter an diesen Daten. Es ist anzunehmen, dass Einbrüche in Praxen in der Regel nicht zum Diebstahl von Patientendaten erfolgen, da Patientendaten in der Regel wirtschaftlich nicht verwertbar sind. Einbrüche in Praxen zielen meist auf Bargeldbestände oder elektronische Geräte ab.

Jeder Betroffene hat Anspruch auf den Schutz seiner nicht allgemein bekannten personenbezogenen Daten. Die von einer Heilmittelpraxis verarbeiteten „Gesundheitsdaten“ unterliegen einem erhöhten Schutzbedarf.

6 Technische und Organisatorische Maßnahmen

Der Datenschutz wird durch die folgenden technischen und organisatorischen Maßnahmen (TOMs) sichergestellt.

6.1 Sensibilisierung und Schulung

Ein wesentlicher Risikofaktor ist der Mensch.

Datenschutz beginnt mit der Auswahl geeigneter Mitarbeiter. Bereits im Bewerbungsprozess werden die Unterlagen der Bewerber systematisch analysiert und auf Plausibilität geprüft. Bei Anzeichen auf Unzuverlässigkeit oder Unregelmäßigkeiten bei vorherigen Arbeitgebern, werden diese hinterfragt. Bereits im Arbeitsvertrag werden Mitarbeiter auf die Einhaltung von Vertraulichkeit und Datenschutz verpflichtet.

Nach Eintritt in das Unternehmen werden alle Mitarbeiter des Unternehmens auf das Thema Datenschutz sensibilisiert. Die Konzepte und organisatorischen Vorkehrungen zum Datenschutz

werden systematisch vermittelt.

In regelmäßigen Audits wird überprüft, ob Konzeption und Organisation im Alltag umgesetzt werden.

In regelmäßigen Abständen erfolgt eine Schulung bzw. Wiederholungsschulung der Themen des Datenschutzes, der Umsetzung des Unternehmens sowie der Handlungsanweisungen, die von den Mitarbeitern zu beachten sind.

6.2 Verhalten im Tagesgeschäft

Zur Gewährleistung eines Basisschutzes werden folgende Maßnahmen im Betrieb durchgeführt. Alle Mitarbeiter sind darauf geschult und verpflichtet, diese Handlungsanweisungen zu befolgen.

- Akten und Dokumente werden im laufenden Geschäftsbetrieb immer so bewegt und abgelegt, dass Unbefugte diese nicht einsehen können.
- Monitore sind so aufgestellt, dass Unbefugte kein Unbefugter Einsicht auf die dargestellten Daten haben.
- Beim Verlassen des Arbeitsplatzes wird der Monitor in den Pause-Modus geschaltet (Bildschirmschoner).
- Telefongespräche mit personenbezogenen Inhalten werden so geführt, dass Unbefugte nicht zuhören können.
- Persönliche Gespräche, wie Gespräche im Rahmen der Therapie werden so geführt, dass Unbefugte nicht zuhören können.
- Faxgeräte und Drucker sind so aufgestellt, dass Unbefugte keine Einsicht auf Ausdrucke haben.
- Zu entsorgende Papierdokumente, die personenbezogene Daten enthalten, werden immer über einen Aktenvernichter entsorgt.

6.3 Zutrittskontrolle

Zur Gewährleistung der Zutrittskontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

- Die Türen und Fenster der Betriebsstätte werden außerhalb der Betriebszeiten verschlossen.
- Schlüssel werden nur an zuverlässige Mitarbeiter gegen Quittung übergeben.
- Es besteht eine Aufstellung, welche Personen Schlüssel zur Betriebsstätte haben.
- Es wird ein Schließsystem verwendet bei dem unbefugte nicht selbst Schlüssel nachmachen lassen können.
- Während der Betriebszeiten ist ein Zutritt der Betriebsstätte für Kunden und sonstige Personen der Betriebsstätte nur möglich, wenn auch ein Mitarbeiter gegenwärtig ist.
- Unbeobachtete Eingänge / Nebeneingänge sind immer geschlossen.

6.4 Zugangskontrolle

Zur Gewährleistung der Zugangskontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

- Computer können nur von Personen genutzt werden, welchen ein Zugang eingerichtet wurde. Es besteht eine Dokumentation, welche Personen ein Zugang eingerichtet wurde.
- Jeder eingerichtete Computer-Zugang ist über Login- und Passwort geschützt. Passworte müssen der Sicherheitsstufe X genügen und mindestens alle 3 Monate neu bestimmt werden.
- Administratorrechte für die IT erhalten nur ausgewählte Personen.
- Papierhafte personenbezogene Daten werden verschlossen aufbewahrt.

6.5 Zugriffskontrolle

Zur Gewährleistung der Zugriffskontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

- Es wird sichergestellt, dass personenbezogene Auskünfte nur an Personen geleistet werden, deren Identität verifiziert ist. Dies gilt insbesondere für telefonische Auskunftsersuchen. (Sprecherverifizierung)
- Es ist per Dienstanweisung festgelegt, dass Unterlagen mit personenbezogenen Daten, die zu entsorgen sind, immer über den Aktenvernichter entsorgt werden. (Korrespondenzentwürfe, Altakten usw.)
- Medien mit Datensicherungen oder sonstigen Daten werden nur in verschlossenen Schränken und Behältern gelagert.

6.6 Weitergabekontrolle

Zur Gewährleistung der Weitergabekontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

- Der Transport von EDV-Daten erfolgt nur auf Medien, welche mit einem Passwort gesichert sind und/oder mittels Dateien, welche über ein Passwort gesichert sind.
- Beim Transport von papierhaften Unterlagen (z.B. Patientenakten) ist besondere Sorgfalt anzuwenden. Zu Hausbesuchen sind diese Unterlagen immer in einer (abschließbaren) Aktenmappe zu transportieren.

6.7 Eingabekontrolle

Zur Gewährleistung der Eingabekontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

- Die Software THEORG ermöglicht es, die wesentlichen Änderungen an den vorn ihr verwaltenden personenbezogenen Daten nachzuvollziehen.
- Es ist per Dienstanweisung festgelegt, dass Änderungen an Patientenkarteikarten mit dem Namenskürzel gekennzeichnet sind.

6.8 Auftragskontrolle

Zur Gewährleistung der Zugriffskontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

Das Unternehmen stellt sicher, dass Dritte nicht auf die Daten des Unternehmens zugreifen können. Für die Fälle, in denen Dritte berechtigt Zugriff auf die Daten erlangen, z.B. da Sie im Auftrag Daten verarbeiten oder im Rahmen von z.B. Servicemaßnahmen in Kenntnis von personenbezogenen Daten erlangen könnten, verpflichtet das Unternehmen diese Dritte schriftlich

zur Einhaltung der Datenschutzstandards im Einklang mit der DSGVO. (AV-Vertrag gem. Art. 28 DSGVO)

Die Datenweitergabe an den Steuerberater für die Lohnbuchhaltung ist zur Wahrung unserer berechtigten Interessen erforderlich (Art. 6 Abs. 1 f DSGVO) bzw. als zulässige Weiterverarbeitung (Art. 6 Abs. 4 DSGVO).

In diesem Sinne wurden mit folgenden Unternehmen entsprechende Vereinbarungen schriftlich getroffen:

- SOVDWAER GmbH, Franckstr. 5, 71636 Ludwigsburg.
  für die Hotline zur Software THEORG
- SOVDWAER GmbH, Frankstr. 5, 71636 Ludwigsburg
  für die Verwaltung des Datenbestandes in der Cloud

6.9 Verfügbarkeitskontrolle

Zur Gewährleistung der Verfügbarkeitskontrolle werden folgende Maßnahmen im Betrieb durchgeführt:

Mögliche Ursache für den Verlust und oder die Zerstörung von Daten liegen in technischen Defekten der Systeme, in Schadsoftware (Viren), in Fehlbedienung, in Vandalismus, in Diebstahl oder in der Zerstörung der Systeme durch Naturgewalten (z.B. Feuer, Hochwasser).

Neben der Abwendung dieser Ursachen, liegt der wesentliche Schutz darin, regelmäßig Kopien der Daten herzustellen. Daher erstellt das Unternehmen von den wesentlichen Daten nächtlich eine Kopie auf ein getrenntes System. Wöchentlich wird eine Kopie der gesamten Daten auf ein externes Sicherungsmedium erstellt. Diese Sicherungsmedien werden abwechselnd an einem entfernten Ort gelagert.

- Es wird jeden Tag eine Sicherungskopie (Datensicherung) der Software THEROG auf ein externes Medium (Wechselfestplatte) erstellt. Nach dem Sicherungsvorgang wird das Medium vom Computer getrennt.
- Jede Woche wird eine Sicherungskopie der Festplatte des Computers / Servers erstellt. Nach dem Sicherungsvorgang wird das Medium (Wechselfestplatte) vom Computer entfernt.
- Sicherungsmedien werden verschlossen aufbewahrt.
- Es werden mehrere Medien (Wechselfestplatte) rollierend verwendet.
- Immer ein Medium (Wechselfestplatte) wird an einem sicheren Ort außerhalb der Geschäftsräume aufbewahrt.
- Alle Arbeitsstationen und der Server sind mit einem Virenscanner versehen. Diese Software wird regelmäßig aktualisiert.
- Arbeitsplatzcomputer, Server und Laptops sind gegen Diebstahl gesichert. (Kensington-Schloss / Abgeschlossener Serverraum)