Datenschutzkonzept zum Medizinprodukt „Tino- DTB: Digitaler Therapiebegleiter in der Onkologie“

folgender Kooperationspartner

DTB Gesellschaft für digitale Therapiebegleitung mbH

Otto-Schott-Str. 15, 07745 Jena

vertreten durch:

Geschäftsführer Ingmar Wegner,

(im Folgenden nur noch „DTBG“)

Datenschutzbeauftragte:

Frau Petra Lindstädt

Spitzweidenweg 17 - 19

07745 Jena

Der im Anhang aufgelisteten Ärzte und Patienten

(im Folgenden nur noch „Anwender“)

Version 1.0.0

Stand 3. Mai 2021

Inhaltsverzeichnis

Vorbemerkung

Dieses Datenschutzkonzept ist Bestandteil der Verträge zwischen der DTB Gesellschaft (DTBG) und den Anwendern (Ärzte) im folgenden „Vertragspartner“ genannt über die Software „Tino DTB: Digitaler Therapiebegleiter“ (im Folgenden nur noch „Tino DTB“) in der Onkologie und regelt den Schutz der Daten bei der Datenverarbeitung oder -nutzung. Es handelt sich hierbei um Daten, die im Zusammenhang mit der ärztlichen Behandlung sowie der effektiven Betreuung der Patienten bei der Anwendung einer Therapie erforderlich sind. Die DTBG ist Hersteller des Medizinprodukts Tino DTB der Klasse 1 (nach MDD).

Das Datenschutzkonzept gibt Auskunft über die Datenflüsse zwischen den beteiligten Vertragspartnern mit Darstellung der Schnittstellen und der einzelnen Nutzung bzw. Übermittlung von patienten- und personenbezogenen Daten. Darüber hinaus wird dargelegt, wie die technische Datenvorhaltung erfolgt und wie die einzelnen Zugriffsrechte durch die Mitarbeiter der Vertragspartner geregelt sind und für welche Auswertungen die Daten verwendet werden. Im vorliegenden Datenschutzkonzept werden die Anforderungen der technischen und organisatorischen Maßnahmen zum Datenschutz und Datensicherheit festgelegt.

I. Geltungsbereich

Dieses Datenschutzkonzept beschreibt und regelt jegliche Form der Verarbeitung von personenbezogenen Daten auf dem Medizinprodukt „Digitaler Therapiebegleiter“ Tino DTB der DTBG und gilt für alle Mitarbeiter der Vertragspartner, die an der Umsetzung beteiligt sind.

II. Datenschutz, Betriebs- und Geschäftsgeheimnisse

a. Vertrauliche Daten

Die Wahrung des Sozialgeheimnisses gemäß § 35 SGB I und des Datengeheimnisses gemäß § 53 BDSG ist in den Abläufen sicherzustellen. Dies bedeutet, dass die Daten nicht unbefugt verarbeitet werden und Personen, die mit der Verarbeitung betraut sind, eine entsprechende Datenschutz- und Geheimhaltungsvereinbarung unterzeichnen bzw. aufgrund ihres Berufsstandes der Schweigepflicht unterliegen.

b. Patientendatenschutz

Bei der Verarbeitung der Patientendaten sind die Regelungen über die Einhaltung der ärztlichen Schweigepflicht nach der Berufsordnung und den strafrechtlichen Bestimmungen von besonderer Bedeutung. Die ärztlichen Leistungserbringer stellen sicher,

dass die von den Patienten unterzeichneten Anmeldebögen und Einwilligungsformulare auf die Entbindung von der ärztlichen Schweigepflicht hinweisen. Die Rechtmäßigkeit der Verarbeitung ist folgend der DS-GVO Art. 6 zu gewährleisten. Die Verarbeitung spezifischer personenbezogener Daten stellt hohe Anforderungen an die Sicherstellung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO die nachweislich umzusetzen sind.

c. Aufbewahrungsfristen / Datenlöschungen

Die gespeicherten Daten werden auf der Grundlage der gesetzlichen Anforderungen bei der Ablehnung der Nutzung oder beim Ausscheiden aus dem Tino DTB bzw. der zugrunde liegende Zweck sich aufhebt von dem Medizinprodukt gelöscht, es sei denn sie werden für die Erfüllung der gesetzlichen Anforderungen weiter benötigt.

III. Strukturen, Aufgaben, Datenflüsse im Tino Digitalen Therapiebegleiter

a. Verantwortlichkeiten – DTBG

DTBG hat die Entwicklung des Medizinprodukts für den Tino DTB in die Wege geleitet und übernimmt folgende Aufgaben:

- Hilfestellung bei Problemen der Patienten und Ärzte hinsichtlich Funktionen bzw. Fehlfunktionen des Tino Digitalen Therapiebegleiters.
- Kontaktaufnahme zu dem behandelnden Facharzt der teilnehmenden Patienten zum Zwecke der digitalisierten Betreuung.
- Bereitstellung des geprüften Medizinprodukts und Sicherstellung der Funktionsfähigkeit.
- Weiterentwicklung des Medizinprodukts und Implementierung von Systemanfragen durch die Anwender.
- Bereitstellung von Schulungsinhalten in geeigneten Formaten für Patienten und Ärzte.
- Sicherstellung von Funktionsfähigkeit hinsichtlich der Sicherheitseinstellungen entsprechend den gesetzlichen Vorgaben (DS-GVO, BDSG, SGB, BfArM, BSI, gematik)

b. Verantwortlichkeiten – Ärzte

- Prüfung der Patienten hinsichtlich Eignung zur Teilnahme von Tino DTB App
- Weiterleitung der Interessensbekundung von Patienten an Tino DTB App an

die DTB GmbH

- Grundlegende informative Aufklärung der Patienten hinsichtlich Funktionen und Möglichkeiten der Tino DTB App
- Import von Medikationsplänen aus einer externen Software zur Erstellung von diesen Plänen (Bsp. Die Tino DTB Therapieplan Software) in die Tino DTB Webanwendung und Prüfung der Richtigkeit dieser importierten Planung
- Einstellung der vom Patienten zu verfolgenden Nebenwirkungen und Vitalwerte sowie Einstellung der Grenzwerte für den Erhalt von Meldungen in der Tino DTB App im Rahmen der Erstellung des zu übertragenden Therapieplans
- Prüfung der Ergebnisse der Dokumentation der Patienten in Form von Vitalparametern und Nebenwirkungen in der Tino DTB Webanwendung
- Kommunikation im Rahmen der Sprechzeiten/Öffnungszeiten der Praxen mit einem Chat mit den aktiven Patienten

Innerhalb dieser beschriebenen Verantwortlichkeiten werden alle Vertragsparteien die notwendigen datenschutzrechtlichen und sicherheitstechnischen Anforderungen nach DS-GVO und BDSG erfüllen.

c. Datenbegriff

Daten im Sinne der besonderen Versorgung sind nach Begriffsbestimmung der §§ 35 SGB I und 67 Abs. 1 SGB X GVO geschützte Sozialdaten sowie personenbezogene Patientendaten gemäß Art. 4 Nr. 1 DS-GVO i.V.m. Art. 9 Nr. 2 lit. h DS-GVO. Folgende Daten werden von den Ärzten erhoben:

- Arzt- und Praxisstammdaten (Name, Vorname, Geburtsdatum, Geschlecht, Arztnummer LANR, Betriebsstättennummer BSNR)

- Patientenstammdaten der behandelnden Patienten (Name, Vorname, Geburtsdatum, Geschlecht, Krankenversicherungsnummer – KVNR – und Krankenkasse)

- Kontaktdaten (Anschrift, E-Mail-Adresse, Telefonnummer) von Ärzten und Patienten

- Kontaktdaten von Angehörigen und Beauftragten der Patienten unter Vorbehalt

- Vertragsstammdaten (Vertragsbeziehung, Vertragsinteresse, Anmeldedatum zum Medizinprodukt)

- Auskunftsdaten aus öffentlichen Verzeichnissen (behandelnder Arzt)

- Gesundheitsdaten der Patienten (Behandlungsdaten, Therapieplan, therapeutisches Profil, Medikamentengabe und Dosierung, Grenzwerte) aus der Patienten App, die gemäß der Therapieplanung oder durch den Willen und Wunsch des Patienten selbst angelegt werden

- Therapieangaben im Rahmen des Therapieplanung, der in die Tino DTB Webanwendung übertragen wird (Behandlungsdaten, Therapieplan, therapeutisches Profil, Medikamentengabe und Dosierung, Grenzwerte)

d. Datenflüsse allgemein

Die zu liefernden bzw. auszutauschenden Daten beziehen sich im Wesentlichen auf:

a. Patienten, die am Tino DTB teilnehmen:
    i. persönliche Adressdaten,
    ii. Geburtsdaten,
    iii. Behandlungsdaten,
    iv. Gesundheitsdaten
b. Ärzte, die Tino DTB Patienten behandeln:
    i. Praxis-Adressdaten,
    ii. Name der Praxis, der Ärzte und des Personals

Die Teilnehmer am Vertrag liefern Daten auf diesen Grundlagen bzw. tauschen diese entsprechend der folgenden Übersicht aus.

Art der Daten	**Art der Daten, Umfang**	**Verwendung der Daten durch**	**Zweck**
Mitarbeiterdaten der Kooperationspartner	Vorname, Nachname	DTBG, Ärzte	Datenschutz und interne Kommunikation
Patientendaten	Vorname, Nachname, Geburtsdatum, Adresse, Versicherungsdaten, Telefonnummer	DTBG, Ärzte	Vertragsumsetzung: Therapiemanagement, Schulung durch DTBG
Angehöriger oder Beauftragter	Vorname, Nachname, Geburtsdatum, Adresse, Telefonnummer	DTBG, Ärzte	Therapiemanagement und Schulung

Art der Daten	Art der Daten, Umfang	Verwendung der Daten durch	Zweck
Vertragsstammdaten	Name, Vertragsbeziehung, Vertragsinteresse, Anmeldedatum	DTBG, Ärzte	Umsetzung des Vertrages Patientenservice
Patientenhistorie	Dokumentation und telefonischer Betreuungsverlauf	Ärzte, DTBG	Anwendersupport, Qualitätsüberprüfung, eigene Dokumentations-pflichten im Rahmen des Tino DTB
Therapieplan der Patienten im Rahmen des Tino DTB	Therapieplan mit Behandlungsdaten, Medikamentengabe, Dosierungsdaten, Vitalparametern und Nebenwirkungen	Ärzte, DTBG	Import des Therapiemanagements und Patienten-Compliance, Qualitätsüberprüfung
Arztdaten	Betriebsstätten-Nummer des Arztes, Stempel des Arztes, Unterschrift des Arztes, Adressdaten	DTBG, Ärzte	Umsetzung Therapiemanagement
Kostenträger-/ Krankenkassendaten	Name des Kostenträgers/ Krankenkasse, Kostenträgernummer/Institutions-kennzeichen der Krankenkasse	DTBG	Umsetzung Therapiemanagement und Abrechnung

IV. Datenschutz-Einwilligung - Patient

Die Teilnahme am Tino DTB beruht auf keiner gesetzlichen Grundlage und ist freiwillig. Deshalb ist es erforderlich, dass der Patient seine Einwilligung erteilt und zum Datenschutz informiert wird. Die Einwilligung ist Bestandteil der Teilnahmeerklärung.

Die Teilnahmeerklärung, Austritts- und Beendigungsbestätigung am Tino DTB werden von den versorgenden Ärzten, dem medizinischen Fachpersonal, Krankenhäusern, Angehörigen usw. (je nachdem in welcher Behandlung der Patient sich befindet bzw. wen er hierzu beauftragt) an DTBG übermittelt.

Des Weiteren gibt der Patient seine Einwilligung, dass die erforderlichen Daten für die Umsetzung des Tino DTB mit Personenbezug von den Vertragspartnern und ggf. Leistungserbringern verarbeitet werden.

Des Weiteren gibt der Patient seine Einwilligung:

- dass aufgrund der Teilnahme und Einwilligung ein Patientenkonto (Datensatz) von DTBG für die Dauer der Teilnahme angelegt wird,

- dass DTBG personenbezogene Daten (Name, Vorname, Adresse, Telefonnummer, Behandlungsdaten) an DTBG zur Durchführung einer gewünschten Schulung übermittelt,

- dass die, durch den Patienten oder Arzt erhobenen Daten ausschließlich in Havarie-Fällen durch DTBG in nicht-pseudonymisierter Form verarbeitet werden. Eine Weitergabe der Daten an Dritte findet nicht statt.

- dass die erhobenen und gespeicherten Daten entsprechend der gesetzlichen Vorschriften aufbewahrt, gelöscht nach Löschkonzept und archiviert werden.

- Es gilt das Auskunfts- & Widerrufsrecht, das Recht auf Berichtigung und Einschränkung der Verarbeitung wie auch der Mitteilungspflicht und der Datenübertragbarkeit.
- dass nach Beendigung der Teilnahme am Tino DTB alle Patientendaten gelöscht werden, soweit sie zur Erfüllung der gesetzlichen Anforderungen nicht mehr benötigt werden.

V. Umsetzung von Sicherheitsmaßnahmen

a. Zutrittskontrolle

Gewährleistung, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren; die Zutrittskontrolle ist räumlich zu verstehen.
DTBG hat folgende Maßnahmen an seinem Standort (Otto-Schott-Straße 15, 07745 Jena) ergriffen:

- Sicherheitsschlösser mit Schlüsselregelung (siehe Zutrittskontrolle)
- verschlossene Türen bei Abwesenheit (Außentüre)
- Alarmsicherung der Außentüren und Fenster
- Personenindividuelle Kennwörter und Zugangsdaten der Servicemitarbeiter
- Festlegung von Sicherheitszonen mit unterschiedlichen Sicherheitsanforderungen (Sicherheitsplan)
- Zutrittskontrollsystem (mit Schlüssel und Chip), Kontrolle und Dokumentation der Schlüsselvergabe durch den Verantwortlichen

DTBG setzt die Kontrolle wie folgt um:

- Es wird sichergestellt, dass ausschließlich befugte Personen Zutritt zu den

Räumlichkeiten erlangen können in denen Daten und Informationen verarbeitet werden.

- Die Funktionsbereichsleiter stellen sicher, dass ihre Mitarbeiter jederzeit achtsam sind, dass sich nur Personen mit Zutrittsberechtigung in den Räumlichkeiten der MP Bereiche aufhalten. Das Gelände der einzelnen Bereiche ist gegen unbefugtes Betreten besonders gesichert. Besucher und Gäste betreten nur in Begleitung von MP MA die Bereiche der MP.
- Weiterhin werden die für die Dienstleistung genutzten Räumlichkeiten durch technische Sicherheitseinrichtungen überwacht, wie elektronische Sicherung mit Kameraüberwachung durch zentralen Wachdienst. Die Sicherung der Räumlichkeiten außerhalb der Arbeitszeiten wird gewährleistet, wie Schutz vor Einbruch durch Eingangsüberwachung und Werksschutz.
- Besonders sensible Unternehmensbereiche, wie Serverräume werden zusätzlich abgesichert durch Zutrittsberechtigungen, dokumentiert, gegen unbefugten Zutritt, sie ist entsprechend auf eine erforderliche Anzahl von Personen beschränkt.

b. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können*;*

DTBG hat folgende Maßnahmen ergriffen:

- Identifizierung und Authentifizierung einschließlich Verfahrensregelungen zur Kennwortvergabe (Definiertes Kennwortalter; Definierte Kennwortlänge; Definierte Kennwortkomplexität; Definierte Kennwort-Chronik; Definierte Kontosperrungsschwelle; Definierte Kontosperrdauer)
- Begrenzung der Fehlversuche
- Protokollierung
- Systemverwalterbefugnisse /-protokollierung
- Dunkelschaltung des Bildschirms mit Passwortschutz
- Firewall
- Verschlüsselungsverfahren entsprechend dem Stand der Technik (IPSEC /SSL VPN)

DTBG setzt die Zugangskontrolle wie folgt um:

- Sämtliche IT-Systeme der DTBG sind so eingerichtet, dass ausgeschlossen werden kann, dass diese durch unbefugte Personen genutzt werden können. Zur Nutzung der Systeme kommen individuelle Anmeldedaten wie Benutzername und Passwort in Anwendung.
- Es sind personengebundene Benutzerberechtigungen eingerichtet und doku-

mentiert. Die Benutzerberechtigungen sollen verhindern das unbefugte Personen die IT-Systeme nutzen können.
- Die Verschlüsselung der IT-Systeme wird entsprechend dem Stand der Technik einem entsprechenden Verschlüsselungsverfahren vorgenommen.

c. Zugriffskontrolle

Es ist dafür zu sorgen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können;

DTBG hat folgende Maßnahmen zur bedarfsorientierten Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung ergriffen:

- Berechtigungskonzept mit differenzierten Berechtigungen (Verwaltung innerhalb des Medizinprodukts durch Systemadministratoren der DTBG)
- Identifizierung und Authentifizierung
- Verschlüsselungsverfahren entsprechend dem Stand der Technik

DTBG organisiert die Zugriffskontrolle wie folgt:

- Es ist sichergestellt, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zugriffsberechtigungen sind auf das erforderliche Minimum beschränkt. Nur die Personen, die die Daten zur Erfüllung ihrer Aufgaben unbedingt benötigen, erhalten gemäß dem Need-to-know-Prinzip - Kenntnis nur zur Aufgabenerfüllung - eine Zugriffsberechtigung.
- Prinzipiell werden Berechtigungen dokumentiert vergeben und eingerichtet. Innerhalb des Konzepts werden Zugriffsberechtigungen vergeben, die sicherstellen, dass Mitarbeiter nur auf Daten zugreifen kann, auf die er im Rahmen seiner Tätigkeit und Anforderung auch zugreifen darf.
- Eine Protokollierung der Verarbeitung sensibler Daten wird auf Auftragsebene dokumentiert und nachvollziehbar vorgenommen, wann welcher Nutzer zu welchem Zweck, Auftrag, Umgang mit den Daten hatte.
- Im gesamten Unternehmen, vor allem da wo sensible Daten verarbeitet werden, wird nach dem Clean-Desk- Prinzip gehandelt, das heißt Papierdokumente, mobile Datenspeicher werden in abschließbaren Möbeln aufbewahrt, liegen nicht unbeaufsichtigt herum und Räumlichkeiten werden vor Fremdzugriff geschützt.

d. Weitergabekontrolle

Es ist dafür zu sorgen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist;
DTBG hat folgende Maßnahmen ergriffen:

- Verschlüsselung von Daten bei der elektronischen Übertragung entsprechend dem Stand der Technik
- Festlegung der zur Abgabe von Datenträgern bzw. zur elektronischen Übertragung berechtigten Personen
- Festlegung des Empfängerkreises von Daten
- Einrichtung eines VPN (Virtual Private Network)
- Kryptographische Verschlüsselung der übertragenen Daten
- Fernwartungskonzept
- Die Protokollierung kann Datenbankbasiert oder über Log-Dateien stattfinden. Hierbei wird festgehalten, wer wann welche Daten eingegeben, verändert oder gelöscht hat.
- Festlegung der zum Export von Daten berechtigten Personen und entsprechende Überwachung dieser Zugänge und ggf. Vorgänge.

Die DTBG ergreift zur Weitergabekontrolle weiterhin folgende Maßnahmen:

- DTBG stellt sicher, dass jede Datenübermittlung oder Transport von Daten ausnahmslos verschlüsselt erfolgt.
- DTBG dokumentiert sämtliche Stellen, an denen eine Übermittlung von Daten vorgesehen ist und beschreibt die jeweilige Verschlüsselungsmethode die sicherstellt das Daten während des Transports nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
- Sollten Datenträger mit Daten eines Auftraggebers transportiert werden, erfolgt eine Dokumentation dazu, um nachzuvollziehen welche Datenträger von wem und wohin transportiert wurden. Datenträger sind ebenso entsprechend des Stands der Technik mit Verschlüsselungsverfahren zu verschlüsseln.
- Schutzwürdige Informationen werden ihrem Schutzbedarf entsprechend durch Löschen oder Vernichten entsorgt.
- Dokumente bzw. Dateien, die außerhalb des Medizinprodukts und seiner Zugriffsrechte übermittelt werden sollen, werden mit einem Passwortschutz versendet. Das Passwort wird dem Empfänger separat übermittelt.

e. Eingabekontrolle

Es ist dafür zu sorgen, dass nachträglich geprüft und festgestellt werden kann, durch wen, wann und welche personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind;

DTBG stellt die Eingabekontrolle wie folgt sicher:

- DTBG stellt sicher, dass sämtliche Eingaben von personenbezogenen Daten und dessen Kunden protokolliert werden. Ebenso werden Veränderungen und das Löschen von Daten in einem Auftrag protokolliert.
- Die Protokollierung kann Datenbankbasiert oder über Log-Dateien stattfinden. Hierbei wird festgehalten, wer wann welche Daten eingegeben, verändert oder gelöscht hat.
- Eine nachträgliche Auswertung ist sichergestellt.
- Es wird sichergestellt, dass keine Datenhistorie versehentlich gelöscht werden kann.
- Protokollierungs- und Protokollauswertungssysteme bezüglich sämtlicher Systemaktivitäten; datenschutzgerechte Aufbewahrung der Protokolle durch den Auftragnehmer für definierten Zeitraum
- Fortlaufende Dokumentation aller Änderungen und Zugriffe (Audit-Trail, Nachvollziehbarkeit: Auf Grundlage der Protokollierung wird der letzte Login erfasst mit User Name, Uhrzeit und Datumsstempel versehen.

f. Auftragskontrolle

Es sind personenbezogene Daten, die im Zusammenhang mit einer bestimmten Therapie verarbeitet werden, nur entsprechend der festgelegten Anforderungen verarbeitet. DTBG hat folgende Maßnahmen ergriffen:

- Schriftliche Festlegung der Anforderungen zur Nutzung
- Festlegung von turnusgemäßen Kontrollen der Funktionalität zwischen den Anwendern
- Regelmäßige Kontrolle und Dokumentation zur Therapiedurchführung
- Keine Nennung von Patientennamen (gegenüber Dritten), Vergabe von Patienten IDs/Pseudonymisierung

DTBG setzt zur Kontrolle der Funktionalität folgendes um:

- DTBG verpflichtet sich, dass die Anwender jederzeit Kontrollen auf Einhaltung der Grundsätze vor Ort durchführen können und stellt dazu entsprechende Informationen zur Verfügung. Kontrollen sollen im angemessenen Zeitraum angemeldet werden und die Unternehmensabläufe nicht beeinträchtigen.
- Dienstleister, die im Auftrag personenbezogene Daten verarbeiten, werden sorgfältig nach festgelegten Kriterien ausgewählt und möglichst vor Vergabe

eines Auftrages überprüft und vertragliche Vereinbarungen gemäß der DS-GVO und sonstigem anwendbaren deutschen Datenschutzrecht (BDSG u.a.) getroffen.

- Werden während einer Überprüfung vor Ort Mängel festgestellt, werden diese dokumentiert. Sind dies schwerwiegende Mängel die besonderen Risiken für die Rechte und Freiheiten von betroffenen Personen bedeuten, ist die Weisungsbefugte Person des Auftraggebers befugt Weisungen zu erteilen, die die weitere Erhebung, Verarbeitung und Nutzung der Daten einschränkt oder untersagt.
- Mit Dienstleistern werden Verträge abgeschlossen, die mindestens den Vorgaben des Art. 28 DS-GVO entsprechen. Schon bestehende Verträge werden noch entsprechend angepasst, dass sie den Mindestanforderungen der DS-GVO genügen.

g. Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen; DTBG hat folgende Maßnahmen ergriffen:

- Backup-Verfahren (mit Festlegung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- Spiegelung von Festplatten (im Zwei-Stunden-Takt)
- Unterbrechungsfreie Stromversorgung (USV)
- Notfallkonzept (in schriftlicher Form)
- Brandmeldeanlage, Brandschutzbeauftragter
- Firewall
- Intrusion Detection Systeme

DTBG setzt die Verfügbarkeit wie folgt um:

- die technischen und organisatorischen Maßnahmen sind so angelegt, dass die Daten gegen zufällige Zerstörung oder Verlust gesichert sind.
- Es existiert ein Konzept zur regelmäßigen Datensicherung (Back-up), welches die Sicherungsmethoden und die Häufigkeit der Sicherung definiert.
- Die Daten sind gegen äußerliche Umwelteinflüsse, technisches Versagen, vorsätzliche Aktionen oder höhere Gewalt geschützt.
- die technischen und organisatorischen Sicherheitseinrichtungen werden regelmäßig überprüft betreffend der Verfügbarkeit kontrolliert und dokumentiert.

h. Trennbarkeit

Die zu unterschiedlichen Zwecken erhobene personenbezogene Daten müssen getrennt verarbeitet werden könnten.

DTBG hat folgende Maßnahmen ergriffen:

- Physikalische und logische Trennung
- Interne Mandantenfähigkeit, Mandantentrennung
- Trennung von Test-/Entwicklungsumgebung und Produktivumgebung sowie deren Daten

DTBG erfüllt das Trennungsgebot wie folgt:

- die technischen und organisatorischen Maßnahmen sehen vor, dass die Daten gegen zufällige Zerstörung oder Verlust gesichert werden.
- Es existiert ein Konzept zur regelmäßigen Datensicherung (Back-up), das die Sicherungsmethode und die Häufigkeit der Sicherungen definiert.
- Die Daten sind gegen äußerliche Umwelteinflüsse, technisches Versagen, vorsätzliche Handlungen oder höhere Gewalt geschützt.
- Es erfolgt eine regelmäßige Überprüfung der technischen und organisatorischen Sicherheitseinrichtungen zur Verfügbarkeitskontrolle und dokumentiert diese Überprüfungen.

i. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

DTBG hat folgende Maßnahmen ergriffen:

- Physische Integrität
- Ablaufintegrität
- Zugriffsintegrität

j. Datenübertragung

Gewährleistung, dass bei der Übermittlung personenbezogener Daten die Vertraulichkeit und Integrität der Daten geschützt werden

DTBG hat folgende Maßnahmen ergriffen

- Datei Anhänge werde mit 256 Bit Rijndael Verschlüsselt
- Digitale E-Mail Signaturen (comodo Group)
- Datei Anhänge werden mit mindestens ZypCrypto-Verfahren oder 256 Bit AES Verfahren verschlüsselt

k. Wiederherstellbarkeit

Gewährleistung, dass die eingesetzte Software im Störungsfall wiederhergestellt werden kann.

DTBG hat folgende Maßnahmen ergriffen

- Zwei eigene Backupstandorte
- Backup Intervalle: stündlich, täglich, wöchentlich, monatlich
- Verschlüsselte Backups
- Offsite-Backup
- Failover Servercluster
- Storage Speichersystem mit mehrfach gespiegelten Festplatten

VI. Unterauftragsverhältnisse

Derzeit sind keine Subunternehmer mit der Verarbeitung von oben benannten Daten beschäftigt.

1. Wenn Subunternehmer durch die Vertragspartner eingeschaltet werden, müssen die vertraglichen Vereinbarungen mit den Subunternehmern so gestaltet werden, dass sie den Datenschutzbestimmungen der DTBG bzw. dem Tino DTB entsprechen. DTBG ist in den Verträgen mit den Subunternehmern Kontroll- und Überprüfungsrechte entsprechend Ziff. 6 dieses Datenschutzkonzeptes so einzuräumen, dass die DTBG, unbeschadet der Verantwortlichkeit der Vertragspartner für die Subunternehmer, unmittelbar auch gegenüber den Subunternehmern berechtigen. Die Vertragspartner sind verpflichtet, auf eine entsprechende Anforderung hin Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen durch die Subunternehmer zu erteilen.
2. Die Vertragspartner haben Unterauftragnehmer sorgfältig auszuwählen und die Grundlage der Auswahlentscheidung sowie die Auswahlentscheidung zu dokumentieren. Die Vertragspartner haben sicherzustellen, dass auch bei den Tätigkeiten der Unterauftragnehmer die Datenschutzvorschriften beachtet werden. Von der Einhaltung der Verpflichtungen durch den Unterauftragnehmer haben sich die Vertragspartner vor Beginn der Datenverarbeitung und sodann regelmäßig durch Kontrollen zu überzeugen und im Falle von Verstößen die Verpflichtungen des Unterauftragnehmers durchzusetzen sowie die jeweilige Kontrolle einschließlich deren Ergebnis zu dokumentieren. Die Vertragspartner weisen auf Verlangen gegenüber DTBG in geeigneter Weise die Einhaltung dieser Pflichten nach. Die Vertragspartner legen DTBG auf Verlangen die Dokumentation und das Ergebnis der Kontrolle vor.
3. Ziffer 3 dieser Vereinbarung gilt für Subunternehmer entsprechend.
4. Die Vertragspartner haben die Einhaltung der Verpflichtungen der Subunternehmer regelmäßig zu überprüfen und die Kontrollen zu dokumentieren. Die Vertragspartner

sind gegenüber DTBG für sämtliche Handlungen und Unterlassungen der von ihnen eingesetzten Subunternehmer verantwortlich.

VII. Kontrollen sicherheitstechnische Maßnahmen

1. Die Vertragspartner haben sich vor Abschluss des Vertrags von den getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz überzeugt.
2. DTBG, vertreten durch seinen Datenschutzbeauftragten oder andere von ihm benannte Prüfer, sind nach vorheriger Ankündigung berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 08:00 bis 17:00 Uhr), ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Vertragspartners die Geschäftsräume, in denen Daten des Tino DTB verarbeitet werden, zu betreten, um sich von der Einhaltung der Sicherheit der Verarbeitung nach DS-GVO Art. 32 (Sicherheit der Verarbeitung) zu überzeugen. Die Vertragspartner haben entsprechende Maßnahmen von DTBG sowie der Datenschutzbehörde zu akzeptieren und unterstützend tätig zu werden.

VIII. Mitteilungspflichten

1. Bei Verstößen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Vertrag getroffenen Festlegungen, insbesondere Störungen, Verdacht auf Datenschutzverletzungen oder sonstigen Beeinträchtigungen durch die DTBG oder der bei ihnen beschäftigten Personen, werden die Anwender sich unterrichtet.
2. DTBG ist verpflichtet, Vorfälle, die eine Informationspflicht nach Art. 33 DS-GVO (§77 BDSG) auslösen können, unabhängig von der Verursachung, unverzüglich den jeweils den Anwendern mitzuteilen. Dies gilt insbesondere in allen Fällen, in denen ein Vorfall personenbezogene Daten zu sensiblen Daten im Sinne des Art. 9 DS-GVO (§26 BDSG) betrifft. Dieselbe Informationspflicht der Vertragspartner besteht bei Kontrollhandlungen, Anordnungen von Maßnahmen oder Ermittlungen einer Datenschutzbehörde bei den Vertragspartnern.

IX. Zweckverwendung im Rahmen des Auftragsverhältnisses

1. Die DTBG als Betreiber des Tino DTB behält sich vor, Weisungen in Bezug auf die Verarbeitung von Daten des Tino Digitalen Therapiebegleiters im Rahmen des Auftragsverhältnisses zu erteilen. DTBG ist nicht berechtigt, die Daten für eigene (gemeint sind andere, als im Hauptvertrag vereinbarte) Zwecke zu nutzen und an Dritte weiterzugeben.
2. Mündliche Ergänzungen und Änderungen wird DTBG unverzüglich schriftlich, per E-Mail oder per Fax bestätigen.

X. Rückgabe/Vernichtung von Unterlagen, Datenträger

Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch DTBG entsprechend der jeweiligen gesetzlichen oder vertraglich vereinbarten Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

XI. Rechte an Daten und Datenträgern, Urheberrechte

1. Alle Rechte an den im Rahmen des Tino DTB verarbeiteten Daten stehen DTBG zu; dies gilt insbesondere für die Rechte eines Datenbankherstellers i.S.v. §87a ff. Urheberrechtsgesetz.
2. Für alle Medien, welche Daten des Tino DTB enthalten, ist von DTBG eine Sicherungsvorkehrung zum Schutz vor dem Zugriff Dritter zu treffen.
3. Sollten die Daten des Tino DTB bei DTBG durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so werden die Anwender unverzüglich darüber informiert.

XII. Kosten/Vergütung

1. DTBG trägt alle Kosten selber, die durch die Erfüllung der in dieser Vereinbarung vorgesehenen Verpflichtungen entstehen.

XIII. Sonstiges

1. Die Daten aus dem Tino DTB und der Vorgänge werden streng vertraulich behandelt, auch über das Ende der Laufzeit dieser Vereinbarung hinaus.
2. Unbeschadet des Weisungsrechts durch DTBG ziehen Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile eine schriftliche Vereinbarung und des ausdrücklichen Hinweises nach sich, dass es sich um eine Änderung bzw. Ergänzung der getroffenen Vereinbarung handelt.
3. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung der Zusammenarbeit fort. Dies gilt entsprechend für das Fernmelde-, Sozial- und Postgeheimnis. Die Parteien stellen klar, dass auch die Regelungen über die Anfragen betroffener Personen und die damit verbundene Auskunftspflicht sowie die Haftungsregelungen auch nach Beendigung dieser Vereinbarung fortgelten.
4. Im Übrigen gelten die Bestimmungen der Hauptverträge zum Tino DTB entsprechend.
5. Allgemeine Geschäftsbedingungen der Vertragspartner finden auf diese Vereinbarung keine Anwendung.
6. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Geschäftssitz der DTBG.
7. Es gilt deutsches Recht unter Ausschluss des internationalen Privatrechts und des UN-Kaufrechts.

_____	_____
Ort, Datum	Für DTBG Ingmar Wegner Geschäftsführer
_____	_____
Ort, Datum	Für Arzt