Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

1. GEGENSTAND DER VEREINBARUNG

(1) Die gegenständliche Vereinbarung wird zwischen [Name/Firma der datenverarbeitenden Stelle/Einrichtung] (als „**Verantwortlicher**“ im Sinne des Art 4 Z 7 DSGVO) und der EKROMED Bandagist GmbH, FN 503763 d, (als „**Auftragsverarbeiter**“ im Sinne des Art 4 Z 8 DSGVO) abgeschlossen und dient als Grundlage für die bestehende Kooperation bzw. Geschäftsbeziehung (insbesondere auch für die Nutzung der vom Auftragsverarbeiter zur Verfügung gestellten Softwarelösung „*FutureCare*“).

(2) Gegenstand dieser Vereinbarung ist die Verarbeitung (Art 4 Z 2 DSGVO) von personenbezogenen Daten (Art 4 Z 1 DSGVO) sowie auch Gesundheitsdaten (Art 4 Z 15 DSGVO) durch den Auftragsverarbeiter im Auftrag des Verantwortlichen.

(3) Die vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von *einem Monat* zum Monatsende gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt davon unberührt.

3. DETAILS ZUR VERARBEITUNG

(1) Zweck der Verarbeitung ist die digitale Unterstützung von Pflegeprozessen und Arbeitsprozessen, insbesondere über die Softwarelösung „*Future Care*“.

(2) Art der Verarbeitung gemäß Art 4 Z 2 DSGVO: Erheben, Erfassen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen, Einschränken, Löschen.

(3) Art der personenbezogenen Daten:
- Stammdaten (Name, Geburtsdatum, Geschlecht),
- Kontaktdaten (Adresse, Telefonnummer, E-Mail),
- Gesundheitsdaten (z. B. Wundstatus, Diagnosen, Medikation, Vitalwerte),
- Dokumentationsdaten (Zeitstempel, Nutzerkennung, Anmerkungen),
- Bild- und Audiodateien im Rahmen der Fallverarbeitung (z. B. Wundbilder),
- ggf. Daten zur sozialen Situation, rechtlicher Betreuung oder Angehörigen.

(4) Kategorien betroffener Personen:
- Ärzte,
- Patient:innen, Kund:innen und Pflegebedürftige,
- Mitarbeitende des Verantwortlichen (Pflegepersonal),
- Angehörige oder gesetzliche Vertreter:innen der Betroffenen.

4. RECHTSGRUNDLAGE DER VERARBEITUNG

(1) Die Verarbeitung erfolgt auf Grundlage folgender Vorschriften:
- Art. 6 Abs 1 lit c DSGVO (gesetzliche Verpflichtung),
- Art. 6 Abs 1 lit e DSGVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse),
- Art. 9 Abs 2 lit. h DSGVO (Verarbeitung zu Zwecken der Gesundheitsvorsorge, medizinischen Diagnostik und Versorgung).

(2) Ergänzend gelten nationale Rechtsgrundlagen wie das Gesundheits- und Krankenpflegegesetz (GuKG) und weitere berufsrechtliche Vorschriften.

5. RECHTE UND PFLICHTEN DER PARTEIEN

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art 6 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach Art 12-22 DSGVO ist allein der Verantwortliche zuständig.

(2) Die Verarbeitung erfolgt ausschließlich nach dokumentierten Weisungen des Verantwortlichen im Sinne von Art. 28 Abs 3 lit a DSGVO sowie nach Maßgabe der Bedingungen und Garantien des Art 9 Abs 3 DSGVO. Weisungen werden schriftlich oder in dokumentierter elektronischer Form erteilt. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(3) Änderungen des Verarbeitungsgegenstands sowie Verfahrensänderungen sind zwischen den Parteien abzustimmen und zu dokumentieren.

(4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn bei der Prüfung der Auftragsergebnisse Unregelmäßigkeiten oder Fehler festgestellt werden.

(5) Der Auftragsverarbeiter verarbeitet die vereinbarungsgegenständlichen Daten ausschließlich nach Maßgabe der mit dem Verantwortlichen getroffenen Vereinbarung. Soweit der Auftragsverarbeiter aufgrund unionsrechtlicher oder nationaler Vorschriften zu einer darüber hinausgehenden Verarbeitung verpflichtet ist (z. B. im Rahmen von Ermittlungen durch Strafverfolgungsbehörden oder staatliche Stellen), informiert er den Verantwortlichen darüber vorab, sofern das einschlägige Recht eine solche Mitteilung nicht aus Gründen eines wichtigen öffentlichen Interesses untersagt (Art. 28 Abs 3 Satz 2 lit a DSGVO).

(6) Der Auftragsverarbeiter gewährleistet die technisch-organisatorische sowie vertraglich vereinbarte Verarbeitung der Daten und stellt sicher, dass die im Auftrag des Verantwortlichen verarbeiteten Datenbestände strikt von anderen Daten getrennt bleiben.

(7) Der Auftragsverarbeiter erklärt, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (siehe **Anlage ./1**).

6. EINSATZ VON SUB-AUFTRAGSVERARBEITERN

(1) Der Auftragsverarbeiter darf zur Erfüllung seiner vertraglichen Leistungen Subunternehmer nur dann einsetzen, wenn der Verantwortliche zuvor schriftlich oder in dokumentierter elektronischer Form zugestimmt hat. Der Verantwortliche erteilt hiermit die Zustimmung zur Beauftragung folgender Subunternehmer:

- **TZMO Austria GmbH**, FN 490361 w, Wienerbergerstraße 11/12a, 1100 Wien (Speicherung der Daten vom „Seniomat“ auf einem hauseigenen Server);
- **TrefflingerKling(IT) OG** („TKIT“), FN 464826v, Christophorusgrund 33, 8053 Graz;
- **Ewald Kroboth GmbH**, FN 503755t, Hütteldorferstraße 8, 1150 Wien;
- **FutureCare GmbH**, FN 662886 h, Straßgangerstraße 291, 8053 Graz.

Art der jeweiligen Verarbeitung gemäß Art 4 Z 2 DSGVO: Erheben, Erfassen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen, Einschränken, Löschen.

(2) Weitere Subunternehmer dürfen ausschließlich mit vorheriger schriftlicher Genehmigung des Verantwortlichen beauftragt werden. Der Auftragsverarbeiter hat dem Verantwortlichen hierfür rechtzeitig die Firma, Anschrift, die vorgesehene Tätigkeit sowie den geplanten Umfang der Datenverarbeitung mitzuteilen.

(3) Der Verantwortliche hat nach Zugang dieser Mitteilung das Recht, innerhalb von 14 Kalendertagen Einspruch gegen die geplante Beauftragung zu erheben. Im Falle eines rechtzeitigen und sachlich gerechtfertigten Einspruchs ist die Beauftragung unzulässig.

(4) Der Auftragsverarbeiter verpflichtet sich, mit sämtlichen Subunternehmern einen Vertrag nach Maßgabe des Art. 28 Abs. 4 DSGVO abzuschließen, in dem die Datenschutzpflichten mindestens im gleichen Umfang übernommen werden, wie sie im vorliegenden Vertrag geregelt sind. Die datenschutzrechtlichen Verantwortlichkeiten sind klar und eindeutig zu trennen.

……, am ……

Für den Auftragsverarbeiter:

.....

(Firmenmäßige Zeichnung)

……, am ……

Für den Verantwortlichen:

.....

(Firmenmäßige Zeichnung)

Anlage ./1 – Technisch-organisatorische Maßnahmen

A. VERTRAULICHKEIT

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☒ Kennwörter (einschließlich entsprechender Policy)	☒ Verschlüsselung von Datenträgern
☒ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis“	☒ Standardprozess für Berechtigungsvergabe
☒ Protokollierung von Zugriffen	☐ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☒ Nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☒ Ja	☐ Nein

B. DATENINTEGRITÄT

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern	☒ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☒ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☒ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges:	

C. VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☒ Backup-Strategie (online/offline; on-site/off-site)	☐ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
☒ Virenschutz	☒ Firewall
☐ Meldewege und Notfallpläne	☐ Security Checks auf Infrastruktur- und Applikationsebene
☐ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☐ Sonstiges:	

Rasche **Wiederherstellbarkeit:**

☒ Ja	☐ Nein