Vereinbarung zur Auftragsverarbeitung (AVV)
gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Zwischen
Dem Auftragnehmer:
Lando Köster – PraxisPilot
Velsener Weg 4, 48231 Warendorf
E-Mail: lando@praxispilot.eu
(nachfolgend „Auftragnehmer“ genannt)

und

Dem Auftraggeber:
[Name der Praxis / Inhaber]
[Straße, Hausnummer, PLZ, Ort]
(nachfolgend „Auftraggeber“ genannt)

§ 1 Gegenstand, Dauer und Zweck der Verarbeitung
(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der KI-gestützten Telefonassistenz („PraxisPilot“).
(2) Gegenstand dieser Vereinbarung ist die Verarbeitung von personenbezogenen Daten, insbesondere Patientendaten wie Name, Geburtsdatum, Telefonnummer und Anrufgrund.
(3) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages über die Nutzung des Dienstes PraxisPilot.

§ 2 Besondere Geheimhaltungspflicht (§ 203 StGB)
(1) Der Auftragnehmer ist sich bewusst, dass der Auftraggeber der ärztlichen Schweigepflicht unterliegt.
(2) Der Auftragnehmer verpflichtet sich, alle ihm im Rahmen der Tätigkeit bekannt gewordenen Patientendaten strikt geheim zu halten.
(3) Alle eingesetzten Mitarbeiter und Unterauftragnehmer sind schriftlich auf das Datengeheimnis und die Wahrung der Berufsgeheimnisse gemäß § 203 StGB verpflichtet worden.

§ 3 Technische und Organisatorische Maßnahmen (TOM)
(1) Der Auftragnehmer setzt die in Anlage 1 detailliert beschriebenen technischen und organisatorischen Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
(2) Die Maßnahmen umfassen insbesondere die Verschlüsselung (TLS/SSL) der Gesprächsdaten.
(3) Transkripte und Audiodaten werden nach erfolgreicher Übermittlung an die Praxis oder spätestens nach Ablauf von 24 Stunden automatisiert gelöscht.
(4) Eine Nutzung der Daten für eigene Zwecke des Auftragnehmers (z. B. Training von KI-Modellen Dritter) ist explizit ausgeschlossen.
(5) Die Verarbeitung erfolgt ausschließlich auf Servern innerhalb der Europäischen Union (ISO 27001 zertifiziert).

§ 4 Unterauftragsverhältnisse
(1) Der Auftraggeber genehmigt die Beauftragung der in Anlage 2 genannten Unterauftragnehmer.
(2) Der Auftragnehmer stellt sicher, dass diese Partner sorgfältig ausgewählt wurden und die Anforderungen der DSGVO erfüllen.
(3) Beabsichtigt der Auftragnehmer, weitere Unterauftragnehmer hinzuzufügen oder zu ersetzen, wird er den Auftraggeber rechtzeitig informieren. Dem Auftraggeber steht in diesem Fall ein Widerspruchsrecht zu.

§ 5 Rechte und Pflichten des Auftraggebers
(1) Der Auftraggeber ist für die Rechtmäßigkeit der Datenverarbeitung (insbesondere die Information der Patienten über den Einsatz des Systems) allein verantwortlich.
(2) Der Auftraggeber hat das Recht, die Einhaltung der vereinbarten Maßnahmen vor Beginn der Verarbeitung und sodann regelmäßig zu kontrollieren.

§ 6 Löschung und Rückgabe von Daten
(1) Nach Beendigung der vertraglichen Arbeiten hat der Auftragnehmer alle in seinen Besitz gelangten Daten sowie Kopien nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben.
(2) Die Löschung ist auf Verlangen des Auftraggebers schriftlich zu bestätigen.
Anlage 1: Technische und Organisatorische Maßnahmen (TOM)
Gemäß Art. 32 DSGVO garantiert der Auftragnehmer folgende Schutzmaßnahmen:
* Vertraulichkeit:
  * Zutrittskontrolle: Nutzung von zertifizierten Rechenzentren (ISO 27001) innerhalb der EU.
  * Zugriffskontrolle: Strenges Berechtigungskonzept; Zugriff auf Patientendaten nur für autorisiertes Personal des Auftragnehmers.
  * Verschlüsselung: Ende-zu-Ende Verschlüsselung via TLS 1.2+ für alle Datenübertragungen.
* Integrität:
  * Schutz vor unbefugter Datenänderung durch modernste API-Authentifizierungsverfahren.
* Verfügbarkeit & Belastbarkeit:
  * Nutzung redundanter Serverinfrastrukturen zur Vermeidung von Ausfällen.
  * Regelmäßige Backups der Systemkonfigurationen (keine dauerhaften Backups von Patientendaten aufgrund der 24h-Löschfrist).
* Verfahren zur regelmäßigen Überprüfung:
  * Turnusmäßige Audits der Schnittstellen-Sicherheit und Überprüfung der Sub-Dienstleister.
Anlage 2: Liste der Unterauftragnehmer
Folgende Dienstleister werden für den Betrieb des PraxisPilot eingesetzt:
* Unterauftragnehmer: Twilio Ireland Ltd.
  * Funktion: Bereitstellung der Telefonie-Infrastruktur und des Anruf-Routings.
  * Standort: EU (Irland).
* Unterauftragnehmer: Vapi, Inc.
  * Funktion: KI-basierte Sprachverarbeitung und technische Orchestrierung der Anrufe.
  * Standort: Verarbeitung erfolgt flüchtig auf EU-basierten Servern.
* Unterauftragnehmer: Hostinger International Ltd.
  * Funktion: Webhosting der Plattform sowie Speicherung notwendiger Metadaten.
  * Standort: EU (Zypern/Niederlande).

Ort, Datum: _____
Unterschrift Auftragnehmer: _____
(Lando Köster – PraxisPilot)
Unterschrift Auftraggeber: _____
([Name der Praxis / Inhaber])