Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO · zwischen Praxis/Einrichtung und Medendo GmbH · Stand 13.10.2026

Vertragsparteien

Verantwortlicher (Auftraggeber): _____ (vollständiger Name der Praxis oder Einrichtung), _____ (Anschrift), vertreten durch _____ (Name, Funktion).

Auftragsverarbeiter (Auftragnehmer): Medendo GmbH, c/o Mindspace, Friedrichstraße 68, 10117 Berlin, Amtsgericht Charlottenburg, HRB 291693 B, vertreten durch die Geschäftsführer Marcus Ross und Stijn Verstijnen. Die Medendo GmbH ist eine 100%ige Tochtergesellschaft der Medendo B.V., Utrecht (Niederlande).

Hauptvertrag ist der zwischen den Parteien geschlossene Vertrag über die Nutzung von Medendo.

1. Begriffe und Gegenstand

1.1 Die Begriffe personenbezogene Daten, betroffene Person, Verantwortlicher, Auftragsverarbeiter und Datenschutzverletzung haben die Bedeutung des Art. 4 DSGVO. Mitarbeiter sind alle für den Auftragnehmer tätigen natürlichen Personen. Betroffenenanfragen umfassen Beschwerden und die Ausübung der Rechte nach Kapitel III DSGVO.

1.2 „Vorfall“ umfasst Datenschutzverletzungen sowie behördliche Untersuchungen oder Beschlagnahmen und hinreichende Anzeichen hierfür, soweit sie Auftragsdaten betreffen.

1.3 Der Auftragnehmer verarbeitet Auftragsdaten ausschließlich zur Durchführung des Hauptvertrags. Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Datenarten und die Kategorien betroffener Personen sind in diesem Vertrag und in Anlage 1 beschrieben. Anlage 1 beschreibt Verarbeitung, Fristen und Unterauftragnehmer, Anlage 2 die technischen und organisatorischen Maßnahmen, Anlage 3 die Kontakte. Alle Anlagen sind Vertragsbestandteil.

1.4 Bei Widersprüchen zu datenschutzrechtlichen Regelungen des Hauptvertrags hat dieser Vertrag Vorrang. Dieser Vertrag schafft keine Rechtsgrundlage für die Behandlung oder die Aufnahme von Gesprächen.

2. Dauer

Dieser Vertrag beginnt mit Abschluss und läuft für die Dauer des Hauptvertrags einschließlich Verlängerungen. Die Pflichten bestehen fort, solange der Auftragnehmer Auftragsdaten verarbeitet.

3. Weisungen, Vertraulichkeit und Verarbeitungsorte

3.1 Der Auftragnehmer verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich Übermittlungen in Drittländer, und nur für die Zwecke aus Anlage 1. Eine eigenständige Nutzung der Auftragsdaten, Werbung sowie das Training eigener oder fremder KI-Modelle mit Auftragsdaten sind ausgeschlossen.

3.2 Zulässige Weisungen werden umgesetzt. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich. Verlangt das Recht der Union oder eines Mitgliedstaats eine Verarbeitung, informiert er den Verantwortlichen vorab über Pflicht und Umfang, soweit das Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses untersagt. Er beschränkt die Verarbeitung auf das Erforderliche.

3.3 Alle zur Verarbeitung befugten Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht. Der Zugriff ist auf die für die jeweilige Aufgabe notwendigen Personen beschränkt. Soweit § 203 StGB Anwendung findet, verpflichtet der Auftragnehmer mitwirkende Personen einschließlich Unterauftragnehmer zur Geheimhaltung.

3.4 Die Verarbeitung der Gesprächs- und Patientendaten (Audio, Transkripte, Berichte) erfolgt in der EU bzw. im EWR. Eine Verarbeitung oder ein Zugriff außerhalb des EWR erfordert die vorherige dokumentierte Genehmigung des Verantwortlichen und eine zulässige Grundlage nach Kapitel V DSGVO.

4. Sicherheit und Kontrolle

4.1 Der Auftragnehmer setzt geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO um und berücksichtigt dabei Stand der Technik, Kosten, Art, Umfang, Zwecke und die Risiken für betroffene Personen. Gesundheitsdaten werden besonders berücksichtigt. Die Maßnahmen ergeben sich aus Anlage 2.

4.2 Der Auftragnehmer stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen beauftragten Prüfer. Ablauf und Schutz der Daten Dritter werden vorab abgestimmt. Der Auftragnehmer überprüft seine Maßnahmen regelmäßig und passt sie bei Bedarf an.

5. Vorfälle

5.1 Der Auftragnehmer meldet Datenschutzverletzungen unverzüglich nach Kenntnis an den Kontakt des Verantwortlichen nach Anlage 3, in jedem Fall spätestens innerhalb von 24 Stunden. Weitere erhebliche Sicherheitsvorfälle werden gemeldet, soweit Auftragsdaten betroffen sind.

5.2 Die Meldung enthält Art des Vorfalls, betroffene Daten und Personen einschließlich verfügbarer Zahlen, wahrscheinliche Folgen, ergriffene Maßnahmen und einen erreichbaren Ansprechpartner. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht. Der Auftragnehmer begrenzt die Folgen, untersucht und dokumentiert den Vorfall und stimmt sich mit dem Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden, ab.

5.3 Der Verantwortliche beurteilt und erfüllt seine Pflichten nach Art. 33 und 34 DSGVO; der Auftragnehmer unterstützt ihn dabei. Ohne Weisung oder gesetzliche Pflicht informiert der Auftragnehmer weder Betroffene noch sonstige Dritte.

6. Unterstützung

Betroffenenanfragen leitet der Auftragnehmer unverzüglich, spätestens innerhalb von 24 Stunden, an den Verantwortlichen weiter und beantwortet sie nicht selbst, sofern er nicht angewiesen oder gesetzlich verpflichtet ist. Er unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung der Rechte nach Kapitel III sowie der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Sicherheit, Meldungen, Datenschutz-Folgenabschätzung und vorheriger Konsultation.

7. Unterauftragnehmer

7.1 Der Verantwortliche erteilt eine allgemeine schriftliche Genehmigung für die in Anlage 1 genannten Unterauftragnehmer. Neue oder ersetzte Unterauftragnehmer kündigt der Auftragnehmer mindestens drei Monate vor Einsatz unter Angabe von Funktion, Daten, Verarbeitungsorten und Schutzmaßnahmen an. Der Verantwortliche kann innerhalb dieser Frist aus sachlichem Grund Einwände erheben.

7.2 Der Auftragnehmer bemüht sich, Einwände auszuräumen oder die Leistung ohne den betroffenen Unterauftragnehmer zu erbringen. Gelingt das nicht, kann der Verantwortliche den Vertrag ganz oder teilweise mit einer Frist von sechs Monaten ab Ablauf der Einwendungsfrist kündigen; der betroffene Unterauftragnehmer wird bis dahin nicht für Auftragsdaten des Verantwortlichen eingesetzt. Während der Aussetzung entsteht keine Vergütungs- oder Schadenersatzpflicht des Verantwortlichen.

7.3 Der Auftragnehmer verpflichtet Unterauftragnehmer durch Vertrag oder anderes Rechtsinstrument mindestens zu denselben Datenschutzpflichten, einschließlich ausreichender Garantien für geeignete Maßnahmen, kontrolliert dies und bleibt dem Verantwortlichen gegenüber für deren Erfüllung voll verantwortlich.

8. Kosten

Die Auftragsverarbeitung und die Unterstützung bei Betroffenenrechten sind in der Vergütung des Hauptvertrags enthalten. Die Rückgabe und Löschung von Auftragsdaten nach Ziffer 10 erfolgt ohne zusätzliche Kosten; Sonderwünsche mit erheblichem Mehraufwand werden vorab vereinbart. Kosten dürfen die Ausübung gesetzlicher Rechte nicht vereiteln.

9. Beendigung

9.1 Der Verantwortliche kann den Vertrag aus wichtigem Grund fristlos kündigen, insbesondere bei einer erheblichen, dem Auftragnehmer zurechenbaren Pflichtverletzung, die nicht binnen 30 Tagen nach schriftlicher Aufforderung behoben wird, sowie bei Auflösung oder Insolvenz des Auftragnehmers.

9.2 Übernahmen oder Eigentümerwechsel beim Auftragnehmer teilt dieser frühzeitig mit. Bei schwerwiegenden Einwänden kann der Verantwortliche ohne Schadenersatzpflicht kündigen. Die

Übertragung dieses Vertrags oder einzelner Rechte und Pflichten bedarf der ausdrücklichen schriftlichen Zustimmung des Verantwortlichen.

10. Rückgabe und Löschung

10.1 Der Auftragnehmer bewahrt Auftragsdaten nur für die Zwecke und Fristen aus Anlage 1 auf. Nach Leistungsende, Fristablauf oder zulässiger Weisung gibt er sie nach Wahl des Verantwortlichen zurück oder löscht sie; Kopien werden gelöscht, soweit nicht das Recht der Union oder eines Mitgliedstaats eine Aufbewahrung verlangt. Die Rückgabe erfolgt elektronisch in einem gängigen, strukturierten Format.

10.2 Die Löschung wird auf Anforderung bestätigt. Ist eine sofortige Löschung technisch nicht möglich, werden Grund und Endtermin dokumentiert, die Daten gesperrt und die Vertraulichkeit gewahrt.

11. Schlussbestimmungen

Änderungen und Ergänzungen bedürfen der Schriftform oder Textform. Sind einzelne Regelungen unwirksam, bleibt der Vertrag im Übrigen wirksam. Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Berlin. Zwingendes Datenschutzrecht und Betroffenenrechte bleiben unberührt.

Ort, Datum: _____

Verantwortlicher: _____ (Name, Funktion, Unterschrift)

Auftragsverarbeiter: _____ (Name, Funktion, Unterschrift)

Anlage 1: Verarbeitung, Fristen und Unterauftragnehmer

1. Dienst, Zweck, Daten, Betroffene

Dienst: Erfassung von Gesprächsaudio, Transkription und Erstellung eines Dokumentationsentwurfs in einer gewählten Vorlage, gegebenenfalls unter Einsatz der unten genannten Unterauftragnehmer. Zweck: Unterstützung der Behandlungsdokumentation. Die Behandlerin oder der Behandler prüft jeden Entwurf; klinische Entscheidungen werden nicht auf Medendo übertragen.

Betroffene: Patientinnen und Patienten, Behandler sowie weitere im Gespräch genannte Personen. Daten: Audio, Transkripte, Berichte und Entwürfe, medizinische und sonstige Gesprächsinhalte sowie Nutzername, E-Mail-Adresse, Kennungen, Einstellungen und notwendige technische Nutzungs- und Fehlerdaten.

Verarbeitungsschritte: Erfassen, Zwischenspeichern, Übermitteln, Transkribieren, Strukturieren, Erstellen des Entwurfs, Bereitstellen und Exportieren, Rückgeben und Löschen.

2. Gesundheitsdaten: Rollen und Rechtsgrundlage

Gesundheitsdaten sind besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO. Der Verantwortliche bestimmt vor Beginn der Nutzung eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und eine Ausnahme nach Art. 9 Abs. 2 DSGVO einschließlich nationaler Anforderungen. Dieser Vertrag nach Art. 28 DSGVO ist weder eine solche Ausnahme noch eine Patienteneinwilligung.

Stützt der Verantwortliche die Audio- und KI-Verarbeitung auf Einwilligung, holt und dokumentiert er eine ausdrückliche, informierte, zweckbezogene und freiwillige Einwilligung nach Art. 9 Abs. 2 lit. a in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO ein; sie ist jederzeit mit Wirkung für die Zukunft widerrufbar. Eine Dokumentation ohne Aufnahme bleibt möglich. Stützt er die Verarbeitung auf die Versorgung, ist Art. 9 Abs. 2 lit. h in Verbindung mit Abs. 3 DSGVO und dem anwendbaren Recht zu prüfen.

Der Verantwortliche informiert Patientinnen und Patienten nach Art. 13 und 14 DSGVO, klärt die Befugnis zur Aufnahme aller erfassten Gesprächsteilnehmer (§ 201 StGB), stellt die Verpflichtungen nach § 203 StGB sicher und prüft die Notwendigkeit einer Datenschutz-Folgenabschätzung. Lehnt eine Person die Aufnahme ab, wird ohne Aufnahme dokumentiert.

3. Aufbewahrung und Löschung

- Audio: wird vorübergehend für die Transkription verarbeitet, einschließlich einer temporären Zwischenspeicherung, und nach Erstellung des Transkripts automatisch gelöscht.
- Transkripte und Berichte: standardmäßig 7 Tage. Chat-Daten: 7 Tage.
- Protokolle (Logs): 90 Tage.
- Account-Daten: für die Dauer des Vertrags; Löschung spätestens 90 Tage nach Vertragsende.

4. Unterauftragnehmer

Der Auftragnehmer setzt folgende Unterauftragnehmer ein:

- Google Cloud (Google Cloud EMEA Limited bzw. Google Ireland Limited): Hosting, Speicherung, Datenbank, Spracherkennung und KI-Dienste, temporäre Audio-Zwischenspeicherung. Gesprächs- und Nutzerdaten. Verarbeitung in der EU. Auftragsverarbeitungsvertrag von Google (Cloud Data Processing Addendum).
- ElevenLabs: Sprache-zu-Text. Gesprächsinhalte im Streaming. Verarbeitung in der EU. Auftragsverarbeitungsvertrag (DPA).
- Microsoft Azure: Transkription und Befüllung von Berichtsfeldern. Gesprächs- und Nutzerdaten im Streaming. Verarbeitung in der EU. Microsoft-DPA.
- Sentry: Fehlererkennung und Monitoring. E-Mail-Adresse, Kennungen und technische Daten, 90 Tage. Verarbeitung in der EU. Sentry-DPA.
- Medendo B.V., Utrecht (Niederlande), Muttergesellschaft: technischer Betrieb und Support der Plattform im Konzernverbund.

Account- und Supportdaten können unter Beteiligung der genannten Dienstleister auch außerhalb des EWR verarbeitet werden; hierfür gilt Ziffer 3.4 des Vertrags. Gesundheitsdaten gehören nicht in Supportanfragen und sollten über sichere Wege übermittelt werden.

Anlage 2: Technische und organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich, für die Verarbeitung der Auftragsdaten angemessene Maßnahmen nach Art. 32 DSGVO zu unterhalten und regelmäßig zu überprüfen. Sie umfassen mindestens folgende Bereiche:

- Zugriffskontrolle: rollenbasierte, auf das Notwendige beschränkte Zugriffe, Vergabe nur an verpflichtete Personen.
- Vertraulichkeit: Verpflichtung der Mitarbeiter zur Geheimhaltung, Trennung der Daten verschiedener Kunden.
- Integrität und Weitergabekontrolle: Schutz der Daten bei Übertragung und Speicherung nach dem Stand der Technik.
- Verfügbarkeit und Wiederherstellbarkeit: Sicherung und Wiederherstellung von Daten, Betriebskontinuität.
- Löschung: Löschung von Auftragsdaten nach den Fristen in Anlage 1.
- Protokollierung und Schutz technischer Logs vor Gesundheitsdaten, soweit möglich.
- Sichere Entwicklung und Änderungsmanagement, Umgang mit Schwachstellen und Sicherheitsvorfällen.
- Auswahl und Überprüfung von Unterauftragnehmern.

Eine ausführlichere Beschreibung der Maßnahmen stellt der Auftragnehmer auf Anfrage zur Verfügung.

Anlage 3: Kontakte

Verantwortlicher: _____ (weisungsberechtigte Person, Funktion, E-Mail, Telefon).

Auftragnehmer: Medendo GmbH, kontakt@medendo.com, +49 30 754 367 92. Datenschutzanfragen: dataprotection@medendo.com. Meldungen von Vorfällen und Weisungen richtet der Verantwortliche an kontakt@medendo.com.

Bitte senden Sie über allgemeine Kontakt- oder Marketingformulare keine Patientendaten.