Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO

Version: 2026-09-09 · Stand: 9. September 2026

Dieser Vertrag gilt zwischen der nutzenden Praxis (Verantwortliche:r im Sinne von Art. 4 Nr. 7 DSGVO) und

Felippe M. Wick, handelnd unter der Geschäftsbezeichnung PTV3-Assistent

c/o Windscheidstr. 20, 10637 Berlin

E-Mail: hallo@ptv3-assistent.de

(nachfolgend „Auftragsverarbeiter“)

Er kommt in elektronischer Form zustande (Art. 28 Abs. 9 DSGVO), indem die Verantwortliche bei Registrierung oder Vertragsschluss den Allgemeinen Geschäftsbedingungen einschließlich dieses AVV zustimmt. Eine eigenhändige Unterschrift ist nicht erforderlich. Der jeweils aktuelle Text ist unter https://www.ptv3-assistent.de/avv abrufbar und als PDF speicherbar.

---

1. Gegenstand, Dauer, Art und Zweck

1.1 Gegenstand

Der Auftragsverarbeiter stellt die webbasierte Software PTV3-Assistent bereit. Damit unterstützt er Psychotherapeut:innen bei der Erfassung strukturierter Angaben und bei der Erstellung von Entwurfstexten für den Bericht an den Gutachter (PTV3).

1.2 Dauer

Der Vertrag gilt für die Dauer der Nutzung von PTV3-Assistent und endet mit Beendigung des Nutzungsvertrags, unbeschadet gesetzlicher Aufbewahrungspflichten.

1.3 Art der Verarbeitung

- Speicherung und Anzeige von Angaben aus Therapeut:innen- und optionalen Patient:innen-Fragebögen
- Verarbeitung hochgeladener Dokumente (z. B. Anamnese-PDFs) zur Texterkennung
- KI-gestützte Analyse und Generierung von Berichtsentwürfen
- Kontoverwaltung, Support und Betrieb der Plattform
- Löschung nach Weisung oder nach Vertragsende

1.4 Zweck

Die Verarbeitung erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen von PTV3-Assistent. Eine Nutzung für eigenes KI-Modelltraining findet nicht statt.

1.5 Ort

Die Verarbeitung soll in der Europäischen Union erfolgen. Soweit ein Unterauftragsverarbeiter Daten außerhalb der EU verarbeitet, gelten die Voraussetzungen der Art. 44 ff. DSGVO (angemessene Garantien, insbesondere Standardvertragsklauseln). Die aktuellen Unterauftragsverarbeiter und Verarbeitungsorte stehen in Anlage 2.

---

2. Kategorien betroffener Personen und Daten

2.1 Betroffene Personen

- Patient:innen der Verantwortlichen
- Nutzer:innen der Verantwortlichen (Therapeut:innen, ggf. Praxispersonal)

2.2 Datenkategorien

Patient:innenbezogene Angaben (besondere Kategorien nach Art. 9 DSGVO):

- Pseudonyme Kennzeichnung (Chiffre oder Initialen; Klarnamen sind nicht erforderlich)
- Anamnestische und biografische Angaben
- Symptomatik, Diagnosen, Verlauf, Befund
- Therapieplanung und berichtstypische klinische Einschätzungen
- Inhalte hochgeladener Unterlagen, soweit sie in die Plattform gelangen

Nutzerdaten:

- Name, E-Mail-Adresse, Konto- und Nutzungsdaten
- Technische Protokolle, soweit für Betrieb, Sicherheit und Fehlerbehebung erforderlich

---

3. Weisungen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung der Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er der Verantwortlichen diese rechtliche Verpflichtung vor der Verarbeitung mit, sofern das betreffende Recht dies nicht verbietet.

Weisungen ergeben sich aus diesem Vertrag, den AGB, der Nutzung der Softwarefunktionen und aus gesonderten schriftlichen (einschließlich elektronischen) Weisungen.

Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, teilt er dies der Verantwortlichen unverzüglich mit.

---

4. Pflichten des Auftragsverarbeiters

4.1 Vertraulichkeit und § 203 StGB

Personen, die Zugriff auf die Daten haben, sind zur Vertraulichkeit verpflichtet. Soweit Berufsgeheimnisse im Sinne von § 203 StGB betroffen sind, verpflichtet der Auftragsverarbeiter sich und die eingesetzten Personen auf die Wahrung dieser Geheimnisse (§ 203 Abs. 4 StGB).

4.2 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO (Anlage 1) und hält sie während der Vertragslaufzeit aufrecht. Wesentliche Verschlechterungen sind der Verantwortlichen mitzuteilen.

4.3 Unterstützung

Der Auftragsverarbeiter unterstützt die Verantwortliche nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen

- bei der Erfüllung von Betroffenenrechten (Art. 12–22 DSGVO),
- bei den Pflichten nach Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

Anfragen von Betroffenen leitet er unverzüglich an die Verantwortliche weiter, sofern sie ihn erreichen.

4.4 Löschung und Rückgabe

Nach Abschluss der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl der Verantwortlichen alle in ihrem Auftrag verarbeiteten personenbezogenen Daten oder gibt sie an die Verantwortliche zurück und löscht die vorhandenen Kopien. Die Verantwortliche teilt ihre Wahl in Textform mit. Erfolgt keine Mitteilung, löscht der Auftragsverarbeiter die Daten nach Ablauf einer 30-tägigen Exportfrist.

Die Löschung aus den aktiv genutzten Systemen erfolgt unverzüglich nach der Weisung, spätestens jedoch innerhalb von 30 Tagen. Sicherungskopien werden bis zu ihrer turnusmäßigen Überschreibung gesperrt und nicht erneut produktiv verarbeitet; sie werden spätestens innerhalb von 90 Tagen gelöscht oder überschrieben. Auf Verlangen bestätigt der Auftragsverarbeiter der Verantwortlichen die Löschung in Textform.

Diese Pflichten gelten nicht, soweit Unionsrecht oder das Recht eines Mitgliedstaats den Auftragsverarbeiter zur weiteren Speicherung verpflichtet. In diesem Fall informiert er die Verantwortliche, soweit rechtlich zulässig, über Rechtsgrundlage und Dauer der Speicherung und verarbeitet die Daten ausschließlich zu diesem Zweck weiter.

Während der Vertragslaufzeit und innerhalb der 30-tägigen Exportfrist kann die Verantwortliche ihre Daten über die bereitgestellten Softwarefunktionen exportieren und löschen.

4.5 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt der Verantwortlichen alle erforderlichen Informationen zum Nachweis der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen – durch die Verantwortliche oder einen von ihr beauftragten Prüfer. Vor-Ort-Kontrollen sind mit angemessener Frist anzukündigen, während der üblichen Geschäftszeiten durchzuführen und dürfen den Betrieb nicht unverhältnismäßig stören. Vorhandene Zertifikate und Prüfberichte von Unterauftragsverarbeitern (z. B. C5-/SOC-Berichte von Microsoft Azure) können als Nachweis dienen.

4.6 Verzeichnis und Verzeichnisauskunft

Der Auftragsverarbeiter führt die ihm obliegenden Angaben nach Art. 30 Abs. 2 DSGVO.

---

5. Unterauftragsverarbeiter

Die Verantwortliche erteilt eine allgemeine schriftliche Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO, weitere Auftragsverarbeiter hinzuzuziehen.

Genehmigte Unterauftragsverarbeiter sind in Anlage 2 aufgeführt. Der Auftragsverarbeiter informiert über beabsichtigte Hinzuziehung oder Ersetzung rechtzeitig, in der Regel mindestens 14 Tage vorher, durch Aktualisierung der Liste unter https://www.ptv3-assistent.de/avv und – bei wesentlichen Änderungen – per E-Mail an die hinterlegte Kontoadresse.

Die Verantwortliche kann der Änderung aus datenschutzrechtlichen Gründen widersprechen. Im Widerspruchsfall können die Parteien den Nutzungsvertrag kündigen, soweit die Leistung ohne den Unterauftragsverarbeiter nicht erbracht werden kann.

Mit jedem Unterauftragsverarbeiter wird ein Vertrag geschlossen, der denselben Datenschutzpflichten unterliegt wie dieser Vertrag (Art. 28 Abs. 4 DSGVO). Der Auftragsverarbeiter bleibt gegenüber der Verantwortlichen für die Einhaltung dieser Pflichten verantwortlich.

---

6. Pflichten der Verantwortlichen

Die Verantwortliche ist für die Rechtmäßigkeit der Übermittlung und der Verarbeitung verantwortlich, einschließlich einer geeigneten Rechtsgrundlage (Art. 6, Art. 9 DSGVO) und der Information der Patient:innen.

Sie setzt PTV3-Assistent so ein, dass möglichst keine Klarnamen, sondern Chiffren oder Initialen verwendet werden. Das ersetzt weder diesen Vertrag noch eine Rechtsgrundlage.

Sie erteilt nur rechtmäßige Weisungen und ist erste Anlaufstelle für Betroffenenrechte.

---

7. Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet der Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden sind, möglichst innerhalb von 24 Stunden, an die hinterlegte Konto-E-Mail oder an die von der Verantwortlichen benannte Datenschutzkontaktadresse.

Die Meldung enthält die nach Art. 33 Abs. 3 DSGVO verfügbaren Angaben. Der Auftragsverarbeiter dokumentiert Verletzungen und unterstützt die Verantwortliche bei Meldungen an die Aufsichtsbehörde und – soweit erforderlich – bei der Benachrichtigung Betroffener.

---

8. Haftung

Die Haftung richtet sich nach Art. 82 DSGVO und den gesetzlichen Bestimmungen sowie, soweit zulässig, nach den AGB.

---

9. Schlussbestimmungen

Änderungen dieses Vertrags erfolgen in Textform, einschließlich der Veröffentlichung einer neuen Version unter https://www.ptv3-assistent.de/avv mit Angabe des Geltungsdatums. Für bereits laufende Verträge gilt die neue Fassung, wenn die Verantwortliche ihr zustimmt oder den Dienst nach Hinweis auf die Änderung weiter nutzt, ohne zu widersprechen.

Es gilt deutsches Recht. Gerichtsstand ist Berlin, soweit gesetzlich zulässig.

Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

Anlage 1 — Technische und organisatorische Maßnahmen

Die folgenden Maßnahmen beschreibt der Auftragsverarbeiter für den Betrieb von PTV3-Assistent. Physische Rechenzentrumsmaßnahmen der Cloud-Anbieter (Zutritt, Videoüberwachung, redundante Energieversorgung) gelten zusätzlich über deren eigene TOM und Zertifikate.

- Zugangskontrolle: Individuelle Benutzerkonten, Passwortvorgaben, rollenbasierte Berechtigungen, Zwei-Faktor-Authentifizierung für administrative Zugänge.
- Zugriffskontrolle: Zugriff nur, soweit für Betrieb, Support oder gesetzliche Pflichten erforderlich. Protokollierung administrativer Zugriffe, soweit technisch vorgesehen.
- Trennung: Logische Mandantentrennung der Praxisdaten. Getrennte Entwicklungs- und Produktionsumgebungen. In Entwicklung und Tests keine echten Patientendaten.
- Übertragung: Verschlüsselte Übertragung (TLS).
- Speicherung: Verschlüsselung der gespeicherten Daten bei den eingesetzten Cloud-Diensten. Sitzungsaudio wird auf den Servern des Auftragsverarbeiters nicht gespeichert. Speichert die Praxis-App eine Aufnahme auf dem Gerät, geschieht das verschlüsselt (AES-256-GCM). Der Schlüssel verbleibt im gerätegebundenen Schlüsselspeicher und wird nicht in Cloud-Backups übernommen. Eine Klartextdatei wird nur vorübergehend zum Versand an Azure erzeugt und danach gelöscht.
- Pseudonymisierung: Die Software ist auf Führung von Fällen mit Chiffre oder Initialen ausgelegt. Klarnamen sind nicht erforderlich.
- Integrität und Verfügbarkeit: Regelmäßige Backups über die Infrastruktur der Unterauftragsverarbeiter. Monitoring und Fehlererkennung.
- Kein Modelltraining: Eingaben und Ausgaben werden nicht zum Training eigener oder fremder Basismodelle verwendet, soweit der Auftragsverarbeiter das vertraglich mit den KI-Anbietern ausgeschlossen hat.
- Datenminimierung: Es werden nur die für die Berichtserstellung und den Betrieb erforderlichen Daten verarbeitet.
- Löschung: Löschung über die Produktfunktionen sowie nach Vertragsende gemäß Ziffer 4.4. Daten in aktiven Systemen werden spätestens innerhalb von 30 Tagen, Sicherungskopien spätestens innerhalb von 90

Tagen gelöscht oder überschrieben, soweit keine gesetzliche Aufbewahrungspflicht des Auftragsverarbeiters entgegensteht.

Anlage 2 — Unterauftragsverarbeiter

Stand: 9. September 2026. Änderungen werden unter https://www.ptv3-assistent.de/avv veröffentlicht.

Microsoft Ireland Operations Ltd. (Azure)

Dienste: Azure OpenAI (Textgenerierung), Azure AI Document Intelligence (Texterkennung hochgeladener Dokumente), Azure Speech (Live- und Datei-Transkription, Region Sweden Central).

Zweck: KI (LLM), Dokumenten Analyse, Sprach-Input, Sitzungsdokumentation.

Ort: Rechenzentren in der Europäischen Union (Data Zone Standard EU, Speech in Sweden Central).

Hinweis zu Speech: keine dauerhafte Audio-Speicherung bei Microsoft, keine Stimmbiometrie. Audio-Logging bleibt deaktiviert.

Maßnahmen: AVV unterzeichnet, TLS, Daten verschlüsselt (at rest), SOC 2, ISO 27001, C5 Typ 2, kein Modelltraining, Nachweise archiviert.

Nachweise: https://www.ptv3-assistent.de/avv#nachweise

Hinweis: Für Azure liegt ein C5-Testat (Typ 2) vor; das ist für Cloud-Verarbeitung von Gesundheitsdaten nach § 393 SGB V relevant.

Supabase, Inc.

Dienste: Datenbank, Authentifizierung, Dateispeicher.

Zweck: Speicherung von Konten, Fällen, Fragebogendaten und Dokumenten.

Ort: Frankfurt, DE.

Maßnahmen: AVV unterzeichnet, TLS, Daten verschlüsselt (at rest), SOC 2, ISO 27001, Nachweise archiviert.

Nachweise: https://www.ptv3-assistent.de/avv#nachweise

Vercel Inc.

Dienste: Hosting und Auslieferung der Webanwendung.

Zweck: Betrieb der Plattform, technische Protokolle.

Ort: Frankfurt, DE.

Maßnahmen: AVV unterzeichnet, TLS, SOC 2, ISO 27001, Nachweise archiviert.

Nachweise: https://www.ptv3-assistent.de/avv#nachweise

Der Auftragsverarbeiter setzt diese Stellen nur ein, soweit der jeweilige Dienst für die konkrete Verarbeitung tatsächlich genutzt wird.