Vertrag zur Auftragsverarbeitung

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Entwurf, Stand 21.11.2026

Dieser Vertrag zur Auftragsverarbeitung ist ein Entwurf. Er wurde von der Coding Brothers UG (haftungsbeschränkt) erstellt und noch nicht juristisch geprüft; Formulierungen können sich bis zur endgültigen Fassung ändern. Der Abschluss erfolgt durch Annahme der Allgemeinen Geschäftsbedingungen bei der Registrierung. Auf Anforderung stellen wir den Vertrag zusätzlich zur Gegenzeichnung in Textform bereit.

Auftragsverarbeiter

Coding Brothers UG (haftungsbeschränkt), Ottstr. 9, 76744 Wörth am Rhein, vertreten durch die Geschäftsführer Carsten Hater und Jürgen Ertel — nachfolgend „Auftragsverarbeiter“.

Verantwortlicher

Die Praxis, die HeilpraxisOS nutzt (Praxisinhaberin bzw. Praxisinhaber laut Registrierung) — nachfolgend „Verantwortlicher“.

§ 1 Gegenstand und Dauer

Gegenstand dieses Vertrags ist die Bereitstellung der Praxissoftware HeilpraxisOS als Onlinedienst (Software as a Service) durch den Auftragsverarbeiter für den Verantwortlichen. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

Die Dauer der Verarbeitung entspricht der Laufzeit des Nutzungsvertrags über HeilpraxisOS. Endet der Nutzungsvertrag, endet auch dieser Vertrag; die Pflichten zur Löschung und Rückgabe nach Abschnitt 11 bleiben davon unberührt.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung dient ausschließlich dem Betrieb der Praxisverwaltung des Verantwortlichen: Verwaltung von Patientenstammdaten, Terminplanung, Behandlungsdokumentation, Anamnese, Rechnungsstellung, Aufgaben, Kommunikation mit Patientinnen und Patienten, Patientenportal sowie den optionalen Zusatzfunktionen (zum Beispiel Videosprechstunde, KI-gestützte Entwürfe, Online-Zahlung).

Die Verarbeitung umfasst das Erheben, Speichern, Ordnen, Verändern, Abfragen, Übermitteln an vom Verantwortlichen bestimmte Empfänger, Sichern, Exportieren und Löschen dieser Daten. Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Zwecke, insbesondere nicht zu Werbe- oder Analysezwecken und nicht zum Training von KI-Modellen.

§ 3 Art der Daten

Verarbeitet werden Stammdaten (Name, Anschrift, Geburtsdatum, Kontaktdaten, Versicherungsart), Termin- und Abrechnungsdaten, Kommunikationsdaten sowie Zugangs- und Protokolldaten der Nutzerinnen und Nutzer der Praxis.

Verarbeitet werden ferner Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO, insbesondere Anamnesen, Behandlungsnotizen, Diagnosen, Befunde, Laborwerte, Therapiepläne, Fotos und hochgeladene Dokumente. Der Verantwortliche stellt sicher, dass für die Verarbeitung dieser besonderen Kategorien eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vorliegt, in der Regel Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 lit. b BDSG oder eine ausdrückliche Einwilligung.

§ 4 Kategorien betroffener Personen

Betroffen sind Patientinnen und Patienten des Verantwortlichen einschließlich deren Kontakt- und Notfallpersonen, die Mitglieder des Praxisteams (Inhaber, Behandler, Assistenz, Abrechnung) sowie sonstige Personen, deren Daten der Verantwortliche in HeilpraxisOS erfasst, etwa Ansprechpartner von Versicherern oder Überweisern.

§ 5 Weisungsrecht und Dokumentation

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen. Die Nutzung der Funktionen von HeilpraxisOS durch den Verantwortlichen und seine Nutzerinnen und Nutzer gilt als Weisung; darüber hinausgehende Weisungen sind in Textform (zum Beispiel per E-Mail) zu erteilen.

Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Verantwortlichen unverzüglich mit und darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen. Weisungen, die den Funktionsumfang von HeilpraxisOS überschreiten, können als kostenpflichtige Zusatzleistung vereinbart werden.

Der Auftragsverarbeiter ist zur Verarbeitung ohne Weisung verpflichtet, wenn er durch das Recht der Europäischen Union oder eines Mitgliedstaats dazu verpflichtet ist. In diesem Fall informiert er den Verantwortlichen vor der Verarbeitung, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 6 Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich alle mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

Soweit der Verantwortliche einer beruflichen Schweigepflicht unterliegt, wird der Auftragsverarbeiter als mitwirkende Person im Sinne des § 203 Abs. 3 und 4 StGB tätig. Er verpflichtet sich, über fremde Geheimnisse, die ihm bei der Leistungserbringung bekannt werden, Stillschweigen zu bewahren, sich nur insoweit Kenntnis von ihnen zu verschaffen, als dies zur Erfüllung des Auftrags erforderlich ist, und alle mitwirkenden Personen sowie Unterauftragsverarbeiter, die Kenntnis erlangen können, in Textform zur Geheimhaltung zu verpflichten und auf die strafrechtlichen Folgen einer Pflichtverletzung hinzuweisen. Diese Regelung gilt vorsorglich auch dann, wenn offen ist, ob der Verantwortliche zu den in § 203 Abs. 1 StGB genannten Berufsgruppen gehört.

Der Zugriff von Mitarbeitenden des Auftragsverarbeiters auf Daten des Verantwortlichen (Support-Zugriff) erfolgt nur, soweit dies zur Fehlerbehebung oder auf ausdrückliche Bitte des Verantwortlichen erforderlich ist, und wird protokolliert. Ein Zugriff auf Behandlungsinhalte findet ohne ausdrückliche Freigabe des Verantwortlichen nicht statt.

§ 7 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die Maßnahmen nach Art. 32 DSGVO, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie des Risikos für die Rechte und Freiheiten der betroffenen Personen ein dem Risiko angemessenes Schutzniveau gewährleisten.

Die zum Vertragsschluss geltenden Maßnahmen sind in der Anlage „Technische und organisatorische Maßnahmen“ beschrieben, die unter heilpraxisos.de/sicherheit veröffentlicht ist. Dazu gehören insbesondere: Betrieb von Anwendung, Datenbank und Dateispeicher in Frankfurt am Main, Verschlüsselung der Übertragung (TLS) und der Speicherung, Mandantentrennung auf Datenbankebene, rollenbasierte Zugriffsrechte, Zwei-Faktor-Authentifizierung, Protokollierung sicherheitsrelevanter Vorgänge, Ratenbegrenzung an sensiblen Schnittstellen sowie regelmäßige Sicherungen.

Der Auftragsverarbeiter darf die Maßnahmen weiterentwickeln, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden auf der genannten Seite dokumentiert.

§ 8 Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, die in der Anlage „Unterauftragsverarbeiter“ aufgeführten weiteren Auftragsverarbeiter einzusetzen. Die Anlage ist Bestandteil dieses Vertrags und unter heilpraxisos.de/avv sowie heilpraxisos.de/sicherheit jeweils in ihrer aktuellen Fassung abrufbar.

Beabsichtigt der Auftragsverarbeiter, einen neuen Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Verantwortlichen mindestens 30 Tage vor der Änderung in Textform (per E-Mail an die hinterlegte Adresse des Praxisinhabers). Der Verantwortliche kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine einvernehmliche Lösung zustande, kann jede Partei den Nutzungsvertrag mit Wirkung zum Zeitpunkt der Änderung kündigen.

Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diesem Vertrag. Bei Unterauftragsverarbeitern in Drittländern stellt der Auftragsverarbeiter geeignete Garantien nach Kapitel V DSGVO sicher, insbesondere über einen Angemessenheitsbeschluss (etwa das EU-US Data Privacy Framework) oder EU-Standardvertragsklauseln.

Optionale Dienste (SMS, Videosprechstunde, KI-Funktionen, Transkription, Online-Zahlung) werden nur eingesetzt, wenn der Verantwortliche die jeweilige Funktion in HeilpraxisOS aktiviert. Ohne Aktivierung werden keine Daten an den betreffenden Unterauftragsverarbeiter übermittelt.

§ 9 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO nachzukommen. HeilpraxisOS stellt dafür insbesondere den vollständigen Export der Daten einer Patientin oder eines Patienten (Art. 15 und 20 DSGVO), die Berichtigung von Stammdaten und die Löschung einzelner Patientenakten als Funktionen bereit.

Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst, es sei denn, der Verantwortliche hat ihn dazu angewiesen.

§ 10 Unterstützung bei Sicherheit und Meldungen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, die Daten des Verantwortlichen betrifft, meldet er dies dem Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden, damit der Verantwortliche seine Meldepflicht gegenüber der Aufsichtsbehörde innerhalb von 72 Stunden (Art. 33 DSGVO) erfüllen kann. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, die betroffenen Datenkategorien und Personen, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen.

§ 11 Löschung und Rückgabe

Der Verantwortliche kann seine Daten jederzeit während der Vertragslaufzeit selbst exportieren, Patientenakten einzeln in einem maschinenlesbaren Format (Art. 20 DSGVO) und Rechnungs- sowie Kassenbuchdaten als CSV- oder DATEV-Export.

Nach Beendigung des Nutzungsvertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen einschließlich hochgeladener Dateien unwiderruflich, 30 Tage nachdem der Verantwortliche die Löschung des Praxiskontos in HeilpraxisOS beantragt hat (bis dahin kann er den Antrag zurücknehmen und exportieren), spätestens jedoch 90 Tage nach Vertragsende. Die Löschung über die Kontofunktion erfasst sämtliche Datenbanktabellen, den Dateispeicher und das Nutzerkonto beim Anmeldedienst.

Gesetzliche Aufbewahrungspflichten, denen der Auftragsverarbeiter selbst unterliegt (zum Beispiel für Rechnungsdaten des Abonnements), bleiben unberührt. Daten in Sicherungskopien werden mit dem regulären Sicherungszyklus, spätestens nach 30 Tagen, überschrieben. Der Verantwortliche ist selbst dafür verantwortlich, seinen berufsrechtlichen Aufbewahrungspflichten durch rechtzeitigen Export nachzukommen.

§ 12 Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind. Dazu gehören insbesondere die Beschreibung der technischen und organisatorischen Maßnahmen, die Liste der Unterauftragsverarbeiter und auf Anfrage vorliegende Zertifizierungen oder Prüfberichte der eingesetzten Infrastrukturanbieter.

Der Verantwortliche kann Überprüfungen einschließlich Inspektionen durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Überprüfungen sind mit angemessener Frist, in der Regel vier Wochen, anzukündigen, auf das Erforderliche zu beschränken und so durchzuführen, dass der Geschäftsbetrieb des Auftragsverarbeiters und die Daten anderer Praxen nicht beeinträchtigt werden. Der Auftragsverarbeiter kann für den Aufwand, der über die Bereitstellung vorhandener Unterlagen hinausgeht, eine angemessene Vergütung verlangen.

§ 13 Haftung und Schlussbestimmungen

Für die Haftung der Parteien gelten Art. 82 DSGVO und die Haftungsregelungen des Nutzungsvertrags (Allgemeine Geschäftsbedingungen). Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen nur für Schäden, die durch eine Verarbeitung entstanden sind, bei der er seinen speziell den Auftragsverarbeitern auferlegten Pflichten nicht nachgekommen ist oder entgegen rechtmäßig erteilten Weisungen gehandelt hat.

Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

ANLAGE

Unterauftragsverarbeiter

Mit „optional“ gekennzeichnete Anbieter werden nur beteiligt, wenn der Verantwortliche die jeweilige Funktion in HeilpraxisOS aktiviert. Die jeweils aktuelle Fassung dieser Anlage ist unter heilpraxisos.de/avv abrufbar.

Anbieter	Zweck	Verarbeitungsort	Übermittlungsgrundlage
Vercel Inc.	Hosting und Ausführung der Anwendung, Dateispeicher (Blob)	Frankfurt am Main (fra1); US-Unternehmen	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Neon Inc.	PostgreSQL-Datenbank	Frankfurt am Main (AWS eu-central-1)	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Clerk Inc.	Authentifizierung und Nutzerverwaltung des Praxisteams	USA	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Resend Inc.	Versand transaktionaler E-Mails	USA (Speicherort); Versand aus der EU-Region Irland	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Brevo (Sendinblue SAS) (optional)	Informations- und Kampagnen-E-Mails an Praxisinhaber (nur mit Einwilligung; keine Patientendaten) — geplant, noch nicht in Betrieb	Frankreich; Server in Frankreich, Belgien und Deutschland	Verarbeitung in der EU
seven communications GmbH & Co. KG (seven.io) (optional)	SMS-Versand (Terminerinnerungen), je nach Einrichtung anstelle von Twilio	Kiel, Deutschland	Verarbeitung in der EU
Twilio Inc. (optional)	SMS-Versand (Terminerinnerungen), je nach Einrichtung anstelle von seven.io	USA	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Stripe Payments Europe Ltd.	Zahlungsabwicklung des Abonnements; optional Patientenzahlungen (Connect)	Irland; Konzern mit Sitz in den USA	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Daily.co (Daily, Inc.) (optional)	Videosprechstunde	EU-Region; US-Unternehmen	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Anthropic PBC (optional)	KI-gestützte Entwürfe (nur mit Opt-in der Praxis)	USA	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
OpenAI, L.L.C. (optional)	KI-gestützte Entwürfe, Ausweichanbieter (nur mit Opt-in der Praxis)	USA	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
Microsoft Ireland Operations Ltd. (Azure AI Speech) (optional)	Transkription von Behandlungsgesprächen (nur mit Einwilligung je Aufnahme)	EU-Region (Westeuropa oder Deutschland)	Verarbeitung in der EU
Upstash Inc.	Zähler für die Ratenbegrenzung (keine Personendaten, nur gekürzte Schlüssel)	Frankfurt am Main (AWS eu-central-1)	Verarbeitung in der EU

Anbieter	Zweck	Verarbeitungsort	Übermittlungsgrundlage
Functional Software Inc. (Sentry)	Fehlerüberwachung mit Redaktion personenbezogener Inhalte	EU-Region (Frankfurt); US-Unternehmen	Angemessenheitsbeschluss (EU-US Data Privacy Framework)
PostHog Inc.	Nutzungsanalyse ohne Cookies und ohne Patientendaten	EU-Cluster (Frankfurt)	Verarbeitung in der EU

Die technischen und organisatorischen Maßnahmen (Anlage zu § 7) sind unter heilpraxisos.de/sicherheit veröffentlicht und Bestandteil dieses Vertrags.

Für den Verantwortlichen (Praxis)

Ort, Datum, Unterschrift

Name der Praxis und der unterzeichnenden Person in Druckbuchstaben

Für den Auftragsverarbeiter

Ort, Datum, Unterschrift

Coding Brothers UG (haftungsbeschränkt), Geschäftsführung