

Vertrag zur Auftragsverarbeitung

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

Fassung 1.0 vom 21. Oktober 2026

Zwischen

der Praxis (nachfolgend „Verantwortlicher“), die Praxometer nutzt und deren Angaben in Anhang I stehen,

und

Justin Michl, Mühlenplatz 1, 23879 Mölln, Deutschland — Anbieter der App Praxometer (nachfolgend „Auftragsverarbeiter“).

1. Gegenstand und Dauer

1.1 Der Auftragsverarbeiter stellt dem Verantwortlichen die App Praxometer zur Verfügung. Praxometer speichert und verarbeitet im Auftrag des Verantwortlichen Daten über dessen Patientinnen und Patienten, Termine, Leistungen und Behandlungsakten sowie Daten über Mitarbeiterinnen und Mitarbeiter der Praxis. Gegenstand, Art und Zweck der Verarbeitung sowie die Art der Daten und die Kategorien betroffener Personen sind in Anhang II beschrieben.

1.2 Dieser Vertrag gilt, solange der Verantwortliche Praxometer nutzt. Er endet, wenn der Verantwortliche seinen Praxis-Account löscht, der Auftragsverarbeiter den Dienst einstellt oder eine Partei den Vertrag kündigt. Ziffer 9 bleibt davon unberührt.

1.3 Der Vertrag wird elektronisch geschlossen: Der Verantwortliche stimmt ihm beim Einrichten der Praxis in der App zu. Der Auftragsverarbeiter speichert Zeitpunkt und Vertragsfassung der Zustimmung als Nachweis. Beide Parteien können den Vertrag zusätzlich ausgedruckt unterzeichnen.

2. Weisungen

2.1 Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Die Nutzung der App durch den Verantwortlichen — das Anlegen, Ändern, Abrufen und Löschen von Daten in Praxometer — gilt als Weisung. Darüber hinausgehende Weisungen erteilt der Verantwortliche in Textform an support.praxometer@gmail.com.

2.2 Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Zwecke, insbesondere nicht zu Werbe-, Analyse- oder Profilbildungszwecken, und gibt sie nicht an Dritte weiter, soweit nicht dieser Vertrag oder das Recht der Union oder eines Mitgliedstaats es verlangen. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen die rechtliche Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.3 Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Verantwortlichen unverzüglich mit und darf die Weisung bis zur Klärung aussetzen.

3. Vertraulichkeit

Der Auftragsverarbeiter verarbeitet die Daten persönlich und allein. Sollte er künftig Personen mit der Verarbeitung betrauen, verpflichtet er sie vorher schriftlich zur Vertraulichkeit und stellt sicher, dass sie die Daten nur auf seine Weisung verarbeiten. Die Vertraulichkeitspflicht besteht nach Ende der Tätigkeit fort.

4. Sicherheit der Verarbeitung

4.1 Der Auftragsverarbeiter trifft die in Anhang III beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Sie berücksichtigen, dass es sich bei Behandlungsakten um Gesundheitsdaten im Sinne von Art. 9 DSGVO handelt.

4.2 Der Auftragsverarbeiter darf die Maßnahmen an den Stand der Technik anpassen, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er dem Verantwortlichen mit.

5. Unterauftragsverarbeiter

5.1 Der Verantwortliche genehmigt die in Anhang IV genannten Unterauftragsverarbeiter.

5.2 Beabsichtigt der Auftragsverarbeiter, einen weiteren Unterauftragsverarbeiter einzusetzen oder einen zu ersetzen, informiert er den Verantwortlichen mindestens 30 Tage vorher per E-Mail an die in der App hinterlegte Adresse oder durch einen Hinweis in der App. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem Grund widersprechen; in diesem Fall kann jede Partei den Vertrag kündigen. Der Verantwortliche erhält dann seine Daten nach Ziffer 9.

5.3 Der Auftragsverarbeiter legt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die ihm selbst nach diesem Vertrag obliegen. Er haftet gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters.

6. Verarbeitung in der EU

Die Daten werden in Rechenzentren innerhalb der Europäischen Union verarbeitet und gespeichert (Anhang IV). Eine Übermittlung in ein Drittland findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, und wird dem Verantwortlichen vorher mitgeteilt.

7. Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anfragen betroffener Personen (Art. 12 bis 22 DSGVO) zu beantworten — insbesondere durch die Export- und Löschfunktionen der App. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst.

7.2 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde), soweit es die ihm zur Verfügung stehenden Informationen betrifft.

8. Meldung von Verletzungen des Schutzes personenbezogener Daten

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, die die Daten des Verantwortlichen betrifft, meldet er sie dem Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden, per E-Mail. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien und ungefähre Zahl der Betroffenen, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen, Kontakt für Rückfragen. Informationen, die noch nicht vorliegen, werden nachgereicht.

9. Löschung und Rückgabe

9.1 Der Verantwortliche kann seine Daten jederzeit selbst aus der App exportieren (Funktion „Praxisdaten exportieren“: alle Patienten, Termine, Leistungen und Behandlungsakten in einem offenen, maschinenlesbaren Format sowie als lesbare Akten) und seinen Praxis-Account samt aller Daten selbst löschen (Funktion „Account löschen“).

9.2 Endet der Vertrag, gibt der Auftragsverarbeiter dem Verantwortlichen auf Wunsch die Daten heraus und löscht anschließend alle beim Auftragsverarbeiter und seinen Unterauftragsverarbeitern vorhandenen Kopien, es sei denn, das Recht der Union oder eines Mitgliedstaats verpflichtet zur weiteren Speicherung. Sicherungskopien werden spätestens nach Ablauf ihres regulären Aufbewahrungszeitraums (Anhang III) überschrieben.

9.3 Stellt der Auftragsverarbeiter den Dienst Praxometer ein, kündigt er dies dem Verantwortlichen mindestens drei Monate vorher an, damit der Verantwortliche seine Daten exportieren kann. Nach Ablauf der Frist werden alle Daten gelöscht; der Auftragsverarbeiter bestätigt die Löschung auf Anfrage.

10. Nachweis und Kontrolle

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlich sind — insbesondere diesen Vertrag, die Beschreibung der Maßnahmen in Anhang III und die Nachweise seiner Unterauftragsverarbeiter (z. B. Berichte nach SOC 2).

10.2 Der Verantwortliche kann die Einhaltung dieses Vertrags überprüfen. Überprüfungen erfolgen vorrangig durch Einsicht in Dokumente und schriftliche Auskünfte; eine Prüfung vor Ort kann mit angemessener Ankündigung während der üblichen Geschäftszeiten verlangt werden, soweit die Prüfung von Dokumenten nicht ausreicht.

11. Verantwortlichkeit

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage der Verarbeitung von Gesundheitsdaten (Art. 9 Abs. 2 DSGVO) und

für die Information seiner Patientinnen und Patienten (Art. 13 DSGVO). Der Auftragsverarbeiter stellt ihm dafür auf Wunsch einen Textbaustein zur Verfügung.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags bedürfen der Textform. Der Auftragsverarbeiter kann eine neue Fassung in der App zur Zustimmung vorlegen; die bisherige Fassung gilt, bis der Verantwortliche der neuen zugestimmt hat.

12.2 Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Es gilt das Recht der Bundesrepublik Deutschland. Dieser Vertrag geht bei Widersprüchen den sonstigen Vereinbarungen über die Nutzung von Praxometer vor, soweit es den Datenschutz betrifft.

Anhang I — Parteien

Verantwortlicher: die Praxis, deren Inhaber oder Inhaberin diesem Vertrag in der App zugestimmt hat. Name der Praxis, Inhaber, Anschrift und Kontakt sind die in den Praxisdaten der App hinterlegten Angaben zum Zeitpunkt der Zustimmung; der Auftragsverarbeiter speichert Praxisname und Inhaber mit dem Zustimmungsnachweis.

Auftragsverarbeiter: Justin Michl, Mühlenplatz 1, 23879 Mölln, Deutschland. E-Mail: support.praxometer@gmail.com.

Anhang II — Beschreibung der Verarbeitung

Gegenstand: Bereitstellung der App Praxometer zur Verwaltung einer Praxis — Patientenverwaltung, Terminplanung, Behandlungsdokumentation, Teamverwaltung.

Art und Zweck: Speichern, Abrufen, Ändern, Löschen der vom Verantwortlichen eingegebenen Daten auf einem Server, damit sie dem Verantwortlichen und den von ihm berechtigten Mitarbeiterinnen und Mitarbeitern auf allen ihren Geräten zur Verfügung stehen. Keine Auswertung durch den Auftragsverarbeiter, keine Weitergabe, keine Werbung.

Kategorien betroffener Personen: Patientinnen und Patienten des Verantwortlichen; Mitarbeiterinnen und Mitarbeiter der Praxis; der Verantwortliche selbst.

Art der Daten:

- Patienten: Anrede, Name, Anschrift, Telefon, E-Mail, Kundennummer, Notizen, Wiedervorlagen, Behandlungsserien.
- Behandlungsakte: Datum, Behandlung, Notizen, Verlauf, nächste Schritte — Gesundheitsdaten nach Art. 9 DSGVO.
- Termine: Datum, Uhrzeit, Dauer, Leistung, Betrag, Status, Notiz, behandelnde Person.
- Leistungen (Behandlungsarten) der Praxis.
- Mitarbeiter: Name, Aufgabenbereich, Einladungscode, Berechtigungen, anonyme Apple-Anmeldekennung.
- Praxis: Name, Inhaber, Anschrift, Kontakt, Steuernummer, Bankverbindung, Logo (zur Anzeige auf allen Geräten der Praxis).
- Anmeldung: anonyme Nutzerkennung von „Mit Apple anmelden“. Keine Passwörter, keine Apple-ID-E-Mail-Adresse beim Auftragsverarbeiter.

Nicht beim Auftragsverarbeiter: Rechnungen und ihre Positionen bleiben ausschließlich auf dem Gerät des Verantwortlichen.

Dauer: für die Dauer der Nutzung von Praxometer; danach Löschung nach Ziffer 9.

Anhang III — Technische und organisatorische Maßnahmen

Verschlüsselung: Jede Verbindung zwischen App und Server läuft über TLS; unverschlüsselte Verbindungen sind in der App nicht erlaubt. Die Datenbank liegt auf verschlüsselten Datenträgern (AES-256) des Unterauftragsverarbeiters. Daten auf dem iPhone unterliegen dem Dateischutz von iOS (hardwaregestützte Verschlüsselung, an den Gerätecode gebunden).

Zugriffskontrolle und Trennung: Jede Praxis ist auf Datenbankebene durch Zugriffsregeln (Row Level Security) von allen anderen getrennt; jede Abfrage wird serverseitig gegen die Anmeldekennung geprüft. Mitarbeiter erhalten nur die vom Verantwortlichen vergebenen Berechtigungen. Die Anmeldung erfolgt ausschließlich über „Mit Apple anmelden“; der Auftragsverarbeiter speichert keine Passwörter.

Zugang des Auftragsverarbeiters: Der administrative Zugang zur Datenbank ist auf den Auftragsverarbeiter beschränkt und durch Zwei-Faktor-Authentifizierung geschützt. Er wird nur zur Wartung und zur Fehlersuche genutzt, nicht zur Einsicht in Inhalte.

Verfügbarkeit und Wiederherstellung: Tägliche automatische Sicherung der Datenbank beim Unterauftragsverarbeiter mit sieben Tagen Aufbewahrung; Wiederherstellung auf einen Tagesstand ist jederzeit möglich. Zusätzlich kann der Verantwortliche seine Daten selbst exportieren und wieder importieren.

Datensparsamkeit: Keine Analyse-, Tracking- oder Werbedienste in der App. Es werden nur die Daten erhoben, die der Verantwortliche selbst eingibt.

Löschung: Der Verantwortliche kann einzelne Datensätze und den gesamten Account selbst löschen; die Löschung wirkt sofort in der Datenbank und innerhalb des Sicherheitszeitraums auch in den Sicherungen.

Organisation: Der Auftragsverarbeiter arbeitet allein; Änderungen an App und Server werden versioniert dokumentiert. Sicherheitshinweise der Unterauftragsverarbeiter werden umgesetzt.

Anhang IV — Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung
Supabase Inc., 970 Toa Payoh North #07-04, Singapur 318992	Datenbank, Anmeldung, Sicherungen	EU — Region eu-west-1 (Dublin, Irland), betrieben auf Amazon Web Services; Vertrag zur Auftragsverarbeitung mit Supabase geschlossen
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	Rechenzentrum für Supabase	Dublin, Irland (EU)
Apple Inc.	„Mit Apple anmelden“ (Anmeldekennung), App-Vertrieb	Apple verarbeitet dabei als eigener Verantwortlicher; der Auftragsverarbeiter erhält nur eine anonyme Kennung

Unterzeichnung (optional, zusätzlich zur Zustimmung in der App)

Ort, Datum

Ort, Datum

Für die Praxis (Verantwortlicher)

Justin Michl (Auftragsverarbeiter)

Name, Praxis

Praxometer