Auftragsverarbeitungsvertrag

app.taktera.de (Version 2026-07-12)

Zuletzt aktualisiert: 12.07.2026

Dieser Vertrag über die Verarbeitung von Daten im Auftrag (nachfolgend „AVV“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Nutzung der Praxissoftware taktera ergeben.

Zwischen dem Kunden der Plattform app.taktera.de (nachfolgend „Auftraggeber“) und der Taktera UG (haftungsbeschränkt), Hauptstraße 62a, 67472 Esthal, vertreten durch den Geschäftsführer Leon Leidner (nachfolgend „Auftragnehmer“).

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Der Auftragnehmer stellt dem Auftraggeber eine mandantenfähige Software zur Verfügung. Leistungsgegenstand ist die Bereitstellung und der Betrieb einer mandantenfähigen Software zur Mitarbeiterverwaltung, Dienst- und Raumplanung, Abwesenheitsverwaltung, Zeiterfassung, internen Kommunikation, Benachrichtigung und Benutzerverwaltung für Praxen (Hauptvertrag). Bei der Nutzung dieser Plattform verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO.

(2) Die Laufzeit dieses AVV entspricht der Laufzeit des Nutzungsvertrags über die Plattform taktera (Hauptvertrag).

(3) Die primäre Datenverarbeitung erfolgt in Rechenzentren in Deutschland bzw. innerhalb der Europäischen Union. Soweit Unterauftragsverarbeiter in Drittländern eingesetzt werden (insbesondere für E-Mail- und Push-Dienste), erfolgt die Übermittlung nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage von Standardvertragsklauseln und ergänzender Risikobewertung. Der Auftragnehmer informiert den Auftraggeber über die in § 5 genannten Unterauftragsverarbeiter und Drittlandübermittlungen.

§ 2 Art und Zweck der Verarbeitung, Datenkategorien und Betroffene

(1) **Verarbeitungszwecke:** Der Auftragnehmer verarbeitet die Daten ausschließlich zu folgenden Zwecken im Auftrag des Auftraggebers:

- Authentifizierung und Zugangsverwaltung
- Mitarbeiter- und Rollenverwaltung
- Dienst-, Raum- und Personaleinsatzplanung
- Urlaubs- und Abwesenheitsverwaltung
- Zeiterfassung und Nachweisführung
- Praxisinterne Kommunikation

- E-Mail- und Push-Benachrichtigungen
- Datei-, Avatar- und Logo-Speicherung
- Support, Wartung, Datensicherung und Fehlerbehebung
- Nachweis rechtlicher Zustimmungen
- Automatisierte Workflows innerhalb der Anwendung

(2) **Kategorien betroffener Personen:**

- Mitarbeiter und Auszubildende der Praxis
- Praxisinhaber und Administratoren
- Nutzer mit App-Zugang
- Empfänger von Einladungs-, Reset- und Benachrichtigungs-E-Mails

Im bestimmungsgemäßen Betrieb der Plattform werden **keine Patientendaten** verarbeitet. Der Auftraggeber ist verpflichtet, Freitextfelder (z. B. Kommentare zu Abwesenheiten oder Chat-Nachrichten) nicht für Diagnosen, medizinische Details oder sonstige Patientendaten zu verwenden.

(3) **Arten personenbezogener Daten:**

- Name, E-Mail-Adresse, Benutzer-ID
- Profilbild / Avatar
- Rolle, Team, Qualifikationen und Beschäftigungsstatus
- Arbeitszeitmodelle und Verfügbarkeiten
- Dienstpläne, Raum- und Mitarbeiterzuweisungen
- Urlaubsansprüche und Urlaubstage
- Abwesenheitsart, Zeitraum, Status und Kommentar
- Krankmeldungen als Gesundheitsdaten nach Art. 9 DSGVO
- Zeiterfassungsdaten, Pausen, Plan-/Ist-Zeiten und Freigaben
- Chat-Nachrichten und Chat-Bilder
- In-App-Benachrichtigungen
- Geräte- und Push-Token
- IP-Adresse, User-Agent, Login- und Sitzungsdaten
- Zustimmungen zu AGB, Datenschutz und AVV
- Praxisname, Standort und Logo
- Abo- und Abrechnungsmetadaten

Es werden keine Diagnosen oder medizinischen Details verarbeitet. Freitextfelder dürfen vom Auftraggeber und den Nutzern nicht für Diagnosen oder Patientendaten verwendet werden.

(4) **Besondere Datenkategorien (Art. 9 DSGVO):** Taktera verarbeitet Gesundheitsdaten ausschließlich in Form der Information, dass eine Arbeitsunfähigkeit bzw. Krankmeldung vorliegt, einschließlich Zeitraum und Status. Diagnosen oder Angaben zur Ursache einer Erkrankung sind nicht Bestandteil der vorgesehenen Verarbeitung.

(5) **Hinweis zu Push-Benachrichtigungen:** Der Auftragnehmer weist ausdrücklich darauf hin, dass Push-Benachrichtigungen derzeit teilweise personenbezogene Inhalte (z. B. Namen, Begriffe wie „Krankmeldung“ oder Abwesenheitsarten) im Payload an die Push-Dienste von Google (Firebase Cloud Messaging) und Apple (APNs) übermitteln. Diese Inhalte können von den genannten Anbietern als Unterauftragsverarbeiter verarbeitet werden. Datenschutzfreundlicher wäre der Versand ausschließlich stiller Push-Nachrichten ohne Namen, Abwesenheitsart oder Nachrichteninhalt; eine entsprechende Anpassung ist geplant.

§ 3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist der Verantwortliche (Controller) im Sinne des Art. 4 Nr. 7 DSGVO für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der Daten sowie für die Wahrung der Rechte der Betroffenen.

(2) Der Auftraggeber ist berechtigt, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen müssen schriftlich oder in Textform erfolgen. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber stellt sicher, dass Freitextfelder in der Plattform nicht für Patientendaten, Diagnosen oder medizinische Details genutzt werden, und weist seine Mitarbeiter entsprechend an.

§ 4 Pflichten des Auftragnehmers

(1) **Weisungsbindung:** Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Ist der Auftragnehmer gesetzlich zur Verarbeitung verpflichtet (z. B. Unionsrecht oder Recht der Mitgliedstaaten), teilt er dies dem Auftraggeber vor der Verarbeitung mit, sofern das Gesetz eine solche Mitteilung nicht verbietet.

(2) **Vertraulichkeit:** Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) **Sicherheitsmaßnahmen:** Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkreten Maßnahmen sind in Anlage 1 aufgeführt. Der Auftragnehmer behält sich vor, die Sicherheitsmaßnahmen anzupassen, sofern das Schutzniveau nicht unterschritten wird.

(4) **Unterstützungspflichten:** Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten zur Beantwortung von Anträgen auf Wahrung der in Kapitel III der DSGVO genannten Betroffenenrechte. Er unterstützt den Auftraggeber zudem bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Datensicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung).

(5) **Sicherheitsvorfälle:** Taktera informiert den Verantwortlichen unverzüglich, möglichst innerhalb von 24 Stunden, über bekannt gewordene Verletzungen des Schutzes personenbezogener Daten und stellt alle für Art. 33 und 34 DSGVO erforderlichen Informationen bereit.

(6) **Löschung, Rückgabe und Datenexport:**

- **Datenexport vor Vertragsende:** Der Auftraggeber kann bis zum Ende des Nutzungsvertrags einen Export der in der Plattform gespeicherten Daten über die verfügbaren Exportfunktionen oder auf schriftliche Anfrage anfordern.
- **Löschung nach Vertragsende:** Nach Beendigung des Nutzungsvertrags werden die personenbezogenen Daten des Auftraggebers auf dessen Anfrage oder – sofern keine gesetzliche Aufbewahrungspflicht entgegensteht – innerhalb von 90 Tagen nach Vertragsende aus den Produktivsystemen gelöscht.
- **Produktivsysteme:** Die Löschung aus der PostgreSQL-Datenbank und dem selbst gehosteten Redis erfolgt im Rahmen der Vertragsbeendigung. Eine vollständig automatisierte Löschung sämtlicher Praxisdaten einschließlich Object Storage ist derzeit noch nicht vollständig implementiert; der Auftragnehmer führt die Löschung in diesem Fall manuell oder teilautomatisiert durch.
- **Backups:** Daten in Backups werden nicht aktiv gelöscht, sondern im Rahmen der Backup-Rotation überschrieben. Eine endgültige Entfernung aus Backups erfolgt spätestens nach Ablauf der Backup-Aufbewahrungsfrist von derzeit bis zu 30 Tagen.
- **Avatare, Praxislogos und Chat-Dateien:** Dateien im Hetzner Object Storage werden bei Löschung des zugehörigen Datensatzes oder auf Anfrage des Auftraggebers innerhalb von 90 Tagen nach Vertragsende entfernt.
- **Zeiterfassungsdaten:** Zeiterfassungsdaten werden bis zum Ablauf der gesetzlichen Aufbewahrungsfristen (derzeit bis zu zwei Jahre nach Ende des jeweiligen Kalenderjahres, soweit der Auftraggeber dies veranlasst) aufbewahrt und anschließend gelöscht.
- **Audit- und Zustimmungsnachweise:** Protokolle zu Zeiterfassungsänderungen, Ops-Zugriffen und elektronischen Zustimmungen (AGB, Datenschutz, AVV) werden bis zu drei Jahre nach Erstellung aufbewahrt und anschließend gelöscht.

- **Geräte- und Push-Token:** Push-Token werden bei Abmeldung, Token-Erneuerung oder spätestens 180 Tage nach letzter Nutzung des Geräts gelöscht.

(7) Es sei denn, nach dem Unionsrecht oder dem Recht der Mitgliedstaaten besteht eine Verpflichtung zur weiteren Speicherung der Daten, werden nach Ablauf der genannten Fristen alle verbleibenden personenbezogenen Daten im Auftrag des Auftraggebers gelöscht oder zurückgegeben.

§ 5 Unterauftragsverhältnisse (Sub-Auftragsverarbeiter)

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen.

(2) Derzeit sind die in der folgenden Tabelle aufgeführten Unterauftragsverarbeiter mit der Verarbeitung von Daten in dem dort genannten Umfang beauftragt:

Anbieter	Leistung	Daten	Ort
Hetzner Online GmbH	Cloud-Server, Netzwerk, Datenbankbetrieb und Backups	sämtliche Plattformdaten	Deutschland
Hetzner Object Storage	Avatare, Praxislogos und Chat-Dateien	Bilder und Dateien	Deutschland / EU
Porkbun LLC	SMTP- und Transaktions-E-Mails	Name, E-Mail, Praxisname, Einladungs- und Reset-Inhalte	USA
Google Ireland Limited	Firebase Cloud Messaging für Android-Push	Gerätetoken und aktuell auch Push-Inhalte	EU / USA
Apple Distribution International Ltd.	APNs für iOS-Push	Gerätetoken und aktuell auch Push-Inhalte	EU / USA

(3) Für die Unterauftragsverarbeiter Porkbun LLC, Google Ireland Limited und Apple Distribution International Ltd. liegen Auftragsverarbeitungsverträge bzw. Datenverarbeitungsvereinbarungen, Standardvertragsklauseln und – soweit erforderlich – Transfer Impact Assessments vor und werden auf Anfrage des Auftraggebers zur Verfügung gestellt.

(4) Folgende Dienste werden **nicht** als Unterauftragsverarbeiter im Sinne dieses AVV eingesetzt: OpenAI, Azure OpenAI, Anthropic oder andere KI-Anbieter; Supabase Cloud; Firebase Auth, Firestore oder Firebase Analytics. Die Authentifizierung (GoTrue), PostgreSQL, Redis, Caddy, Socket.IO und BullMQ werden vom Auftragnehmer selbst gehostet. Die Zahlungsabwicklung über Stripe ist Gegenstand der Datenschutzerklärung des Auftragnehmers und nicht Bestandteil der Unterauftragsverarbeiterliste dieses AVV.

(5) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung bezüglich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern per E-Mail oder über die Plattform. Dem Auftraggeber steht das Recht zu, gegen solche Änderungen Widerspruch einzulegen. Widerspricht der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Information, gilt die Änderung als genehmigt. Bei berechtigtem Widerspruch kann der Auftragnehmer den Nutzungsvertrag mit einer Frist von 30 Tagen kündigen.

(6) Dem Unterauftragsverarbeiter müssen vertraglich dieselben Datenschutzpflichten auferlegt werden, die in diesem AVV festgelegt sind.

§ 6 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, in Absprache mit dem Auftragnehmer Überprüfungen durchzuführen oder durch einen von ihm beauftragten, unabhängigen Prüfer durchführen zu lassen.

(2) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag und in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

§ 7 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

(2) Es gilt das Recht der Bundesrepublik Deutschland.

(3) Dieser AVV wird elektronisch geschlossen und ist ab dem Zeitpunkt der Bestätigung in der App oder des Vertragsschlusses des Hauptvertrages für beide Parteien rechtlich bindend.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Gemäß Art. 32 Abs. 1 DSGVO werden folgende Maßnahmen zur Sicherung der Datenverarbeitung implementiert:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Hosting:** Betrieb in deutschen Hetzner-Rechenzentren.

- **Transportverschlüsselung:** HTTPS/TLS über Caddy für sämtliche Client-Server-Kommunikation.
- **Netzwerkisolierung:** PostgreSQL-Datenbank und Redis im privaten Netzwerk; Firewall und Beschränkung des Datenbankzugriffs auf das private Netzwerk.
- **Authentifizierung:** JWT-basierte Authentifizierung über selbst gehostetes GoTrue; Rollen- und Administrationsberechtigungen auf Applikationsebene.
- **Zwei-Faktor-Authentifizierung:** TOTP-Zwei-Faktor-Authentifizierung für die interne Ops-Konsole.
- **Session-Management:** Vierstündiger Inaktivitäts-Logout; zeitlich begrenzte und gehashte Einladungstoken.
- **Dateizugriff:** Signierte Avatar-URLs; Zugriffskontrolle für Chat-Dateien; Upload-Limit von 5 MB.
- **API-Schutz:** Rate-Limiting für sensible öffentliche Endpunkte; Stripe-Webhook-Signaturprüfung.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Trennungskontrolle:** Mandantentrennung über Praxis-IDs und PostgreSQL Row-Level Security (RLS).
- **Audit-Protokolle:** Protokollierung von Zeiterfassungsänderungen und Ops-Zugriffen zur Nachvollziehbarkeit.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- **Backup und Wiederherstellung:** Regelmäßige Backups der Datenbank mit dokumentierten Backup- und Wiederherstellungsverfahren.

4. Verfahren zur regelmäßigen Überprüfung und Sicherheitsvorfälle

- Regelmäßige Software-Updates und Abhängigkeitsprüfungen.
- Verfahren zur Behandlung von Sicherheitsvorfällen gemäß § 4 Abs. 5 dieses AVV.