Auftragsverarbeitungsvertrag

Version 2026-10-11 · gültig ab 11.10.2026

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

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus der Nutzung der Plattform Taktera nach den Allgemeinen Geschäftsbedingungen und der gebuchten Leistungsbeschreibung (zusammen „Hauptvertrag“). In Fragen des Datenschutzes geht dieser AVV dem Hauptvertrag vor.

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Plattform Taktera (Web-App unter app.taktera.de sowie Apps für iOS und Android) für die Personal-, Dienst- und Raumplanung, die Abwesenheitsverwaltung, die Zeiterfassung, die interne Kommunikation, Auswertungen, Automatisierungen und – nach Freischaltung – KI-Funktionen bereit. Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO.

(2) Art und Zweck der Verarbeitung, die Arten personenbezogener Daten, die Kategorien betroffener Personen und die Löschfristen beschreibt Anlage 1.

(3) Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags. Die Pflichten aus § 11 und zur Vertraulichkeit gelten bis zur vollständigen Löschung der Daten fort.

§ 2 Ort der Verarbeitung

(1) Die Daten werden in Rechenzentren der Hetzner Online GmbH in Deutschland gespeichert und verarbeitet.

(2) Eine Verarbeitung in einem Drittland erfolgt nur durch die in Anlage 3 genannten Unterauftragsverarbeiter und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (z. B. EU-U.S. Data Privacy Framework) oder von Standardvertragsklauseln der EU-Kommission.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist durch das Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Auftraggeber diese Verpflichtung vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen sind dieser AVV, der Hauptvertrag sowie die Einstellungen und Handlungen des Auftraggebers und seiner Administratoren in der Plattform, etwa das Anlegen, Ändern und Löschen von Daten, das Aktivieren von Funktionen wie KI-Funktionen oder Automatisierungen, das Festlegen von Löschfristen, Exporte sowie der Versand von E-Mails an vom Auftraggeber festgelegte Empfänger. Weitere Weisungen erteilt der Auftraggeber in Textform an datenschutz@taktera.de.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

(4) Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Änderungswunsch.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Personen (Art. 13, 14 DSGVO), die Wahrung ihrer Rechte sowie – soweit erforderlich – für eine Datenschutz-Folgenabschätzung und die Beteiligung einer Arbeitnehmervertretung verantwortlich.

(2) Der Auftraggeber stellt sicher, dass in Freitextfeldern, Notizen, Chat-Nachrichten und Eingaben in KI-Funktionen keine Patientendaten, Diagnosen oder sonstigen medizinischen Angaben erfasst werden, und weist seine Nutzer entsprechend an.

(3) Der Auftraggeber entscheidet, wem er Zugang und Administratorrechte einräumt, welche Funktionen er nutzt und an welche Empfänger Exporte und E-Mails aus Automatisierungen gehen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 5 Pflichten des Auftragnehmers

(1) **Zweckbindung:** Der Auftragnehmer verarbeitet die Daten nur im Rahmen dieses AVV. Er verwendet die Daten des Auftraggebers nicht für eigene Zwecke, soweit § 10 nichts anderes bestimmt, nicht zum Training von KI-Modellen und gibt sie nicht zu Werbezwecken weiter.

(2) **Vertraulichkeit:** Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht über das Ende der Tätigkeit hinaus fort.

(3) **Sicherheit:** Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind. Er darf sie an den technischen Fortschritt anpassen, sofern das Schutzniveau nicht unterschritten wird, und dokumentiert wesentliche Änderungen.

(4) **Unterstützung:** Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Kapitel III DSGVO) sowie bei den Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation), insbesondere durch die Bereitstellung der dafür erforderlichen Informationen.

(5) Der Auftragnehmer berichtigt, löscht oder schränkt Daten nur auf Weisung des Auftraggebers ein, soweit dies nicht durch Funktionen der Plattform geschieht.

(6) Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und arbeitet auf Anfrage mit der Aufsichtsbehörde zusammen. Über Kontrollen und Maßnahmen einer Aufsichtsbehörde, die diesen Auftrag betreffen, informiert er den Auftraggeber unverzüglich.

(7) Mitarbeitende des Auftragnehmers greifen auf Daten des Auftraggebers nur zu, soweit dies für Support, Wartung, Fehlerbehebung oder Sicherheit erforderlich ist. Zugriffe über die interne Verwaltungskonsole werden protokolliert.

(8) Ansprechpartner für den Datenschutz ist der Geschäftsführer, zu erreichen unter datenschutz@taktera.de. Ändert sich der Ansprechpartner, teilt der Auftragnehmer dies mit.

§ 6 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, in der Regel innerhalb von 24 Stunden, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt geworden ist.

(2) Die Meldung enthält, soweit bekannt, die Informationen nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen. Informationen, die noch nicht vorliegen, reicht er unverzüglich nach.

(3) Der Auftragnehmer ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und stimmt sich dazu mit dem Auftraggeber ab. Meldungen an Aufsichtsbehörden oder betroffene Personen nimmt er nur nach Weisung des Auftraggebers vor.

§ 7 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO). Die in Anlage 3 genannten Unterauftragsverarbeiter gelten als genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vorher per E-Mail an die Administratoren oder in der Plattform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Widerspricht er nicht, gilt die Änderung als genehmigt. Widerspricht er, suchen die Parteien eine einvernehmliche Lösung; gelingt dies nicht, kann jede Partei den Hauptvertrag zum Zeitpunkt der Änderung kündigen. Muss ein Unterauftragsverarbeiter aus dringenden Gründen (z. B. Sicherheit, Ausfall des Anbieters) kurzfristig ersetzt werden, informiert der Auftragnehmer unverzüglich; das Widerspruchsrecht bleibt unberührt.

(3) Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig aus, die hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bieten, und erlegt ihnen vertraglich dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Einhaltung.

(4) Keine Unterauftragsverhältnisse im Sinne dieses AVV sind Nebenleistungen wie Telekommunikations- und Postdienste sowie Leistungen, für die der Auftragnehmer oder ein Dritter selbst verantwortlich ist, etwa die Zahlungsabwicklung über Stripe.

§ 8 Rechte betroffener Personen

(1) Die Plattform bietet Funktionen, mit denen der Auftraggeber Daten einsehen, berichtigen, löschen und exportieren kann. Darüber hinaus unterstützt der Auftragnehmer auf Anfrage.

(2) Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nur nach dessen Weisung.

§ 9 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung, insbesondere diesen AVV mit Anlagen, aktuelle Angaben zu den Maßnahmen nach Anlage 2 und Nachweise der Unterauftragsverarbeiter (z. B. Zertifizierungen der

Rechenzentren).

(2) Der Auftraggeber kann Überprüfungen einschließlich Inspektionen selbst oder durch einen zur Verschwiegenheit verpflichteten, unabhängigen Prüfer durchführen. Prüfungen sind mit angemessener Frist, in der Regel 14 Tage, anzukündigen, finden während der üblichen Geschäftszeiten statt und dürfen den Betrieb nicht unverhältnismäßig stören. Daten anderer Kunden sind zu schützen. Ohne besonderen Anlass sind Prüfungen einmal im Jahr möglich.

(3) Jede Partei trägt ihre eigenen Kosten. Für Vor-Ort-Prüfungen kann der Auftragnehmer eine angemessene Vergütung seines Aufwands verlangen, es sei denn, die Prüfung wurde durch einen Verstoß des Auftragnehmers veranlasst.

§ 10 Verarbeitung für eigene Zwecke des Auftragnehmers

(1) Beim Betrieb der Plattform verarbeitet der Auftragnehmer als eigener Verantwortlicher ausschließlich:

- eine Nutzungsstatistik mit pseudonymen Zählern ohne Inhalte (nutzerbezogen 90 Tage, danach nur Summen je Praxis),
- Fehlerberichte mit pseudonymen Kennungen ohne Inhalte (30 Tage),
- die Erfassung von KI-Anfragen nach Umfang und Kosten ohne Inhalte (für Kontingent und Abrechnung),
- Sicherheitsprotokolle zum Schutz der Plattform sowie
- Vertrags-, Abrechnungs- und Kontaktdaten des Auftraggebers und Nachweise der Zustimmung zu AGB und AVV.

Einzelheiten beschreibt die Datenschutzerklärung. Der Auftraggeber erhält aus diesen Daten keine Auswertungen über einzelne Nutzer.

(2) Der Auftragnehmer darf anonymisierte, zusammengefasste Statistiken ohne Bezug zu Personen oder zum Auftraggeber erstellen, um die Plattform zu betreiben und zu verbessern.

§ 11 Beendigung, Rückgabe und Löschung

(1) **Export:** Während der Laufzeit kann der Auftraggeber Daten über die Exportfunktionen der Plattform abrufen. Auf Anfrage stellt der Auftragnehmer einen vollständigen Export der Daten des Auftraggebers in einem gängigen maschinenlesbaren Format (CSV oder JSON, Dateien im Originalformat) bereit.

(2) **Nach Vertragsende:** Die Daten bleiben nach dem Ende des Hauptvertrags 30 Tage für einen Export verfügbar. Danach löscht der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers einschließlich der Dateien in der Dateiablage, spätestens 90 Tage nach Vertragsende. Sicherungskopien werden im Rahmen der regulären Rotation überschrieben, spätestens 90 Tage nach der Löschung. Die Löschung bestätigt der Auftragnehmer auf Anfrage in Textform.

(3) **Aufbewahrungspflichten des Auftraggebers:** Gesetzliche Aufbewahrungspflichten des Auftraggebers, etwa für Arbeitszeitnachweise oder Lohnunterlagen, erfüllt der Auftraggeber selbst. Er exportiert die betroffenen Daten rechtzeitig vor der Löschung. Der Auftragnehmer bewahrt Daten über das Vertragsende hinaus nur auf, wenn dies gesondert vereinbart ist oder er gesetzlich dazu verpflichtet ist.

(4) **Löschfristen während der Laufzeit:** Die in Anlage 1 genannten automatischen Löschfristen gelten als Weisung des Auftraggebers. Abweichende Fristen können vereinbart oder, soweit die Plattform dies vorsieht, in den Einstellungen festgelegt werden.

§ 12 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregelungen des Hauptvertrags, soweit Art. 82 DSGVO nicht entgegensteht.

§ 13 Schlussbestimmungen

(1) Dieser AVV wird elektronisch geschlossen (Art. 28 Abs. 9 DSGVO), mit der Buchung oder der Bestätigung in der Plattform. Änderungen bedürfen der Textform. Für Änderungen dieses AVV gilt das Verfahren für Änderungen der AGB entsprechend; für Unterauftragsverarbeiter gilt § 7.

(2) Werden Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich und weist die Beteiligten darauf hin, dass die Verantwortung beim Auftraggeber liegt.

(3) Sollte eine Bestimmung unwirksam sein, bleibt der übrige Vertrag wirksam.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Der Gerichtsstand richtet sich nach dem Hauptvertrag.

Anlage 1: Beschreibung der Verarbeitung

1. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers einschließlich Auszubildender, Aushilfen und Praktikanten
- ehemalige Beschäftigte, solange ihre Zeiterfassung aufbewahrt wird
- Praxisinhaber und Administratoren
- sonstige Personen, denen der Auftraggeber Zugang gewährt
- Empfänger von E-Mails, die der Auftraggeber über Automatisierungen festlegt

2. Arten personenbezogener Daten

- **Team und Konten:** Name, Titel, E-Mail-Adresse, Profilbild, Rolle bzw. Berufsgruppe, Team, Administratorrechte, Zugangsstatus, Qualifikationen mit Ablaufdatum, Personalnummer, Beschäftigungsart, Arbeitszeitmodell, Sollzeit mit Verlauf, Urlaubsanspruch und Resturlaub
- **Planung:** Dienst- und Raumpläne, Einteilungen, Vor- und Nachbereitungszeiten, Notizen zu Planungstagen, Verfügbarkeiten, Einsatzregeln
- **Abwesenheiten:** Art, Zeitraum, Status, Genehmigung, optionale Notiz
- **Zeiterfassung:** Kommen, Gehen und Pausen mit Zeitpunkt und Quelle, nachgetragene Buchungen, Korrekturen mit bearbeitender Person, Hinweise (z. B. Ruhezeit), Freigaben, Überstundenkonto, Prüfprotokoll
- **Kommunikation:** Chat-Nachrichten mit Bildern, Dokumenten und Sprachnachrichten, Reaktionen, Lesebestätigungen, Ankündigungen, In-App-Benachrichtigungen
- **Auswertungen:** aus Planungsdaten berechnete Auslastung, Einsatz- und Abwesenheitszeiten und Umsatzpotenzial je Gruppe und Person
- **Automatisierungen:** Abläufe des Auftraggebers und deren Ausführungsprotokolle
- **KI-Funktionen:** Gespräche mit dem Assistenten (pseudonymisiert), Bewertungen von Antworten, Planungsregeln der Praxis
- **Technische Daten:** Anmeldedaten (Passwort-Hash), Anmeldezeitpunkte, IP-Adresse und User-Agent, Push-Token, Gerätename, App-Version
- **Praxis:** Praxisname, Praxis-ID, Standort, Logo, Räume, Einstellungen

3. Besondere Kategorien (Art. 9 DSGVO)

Verarbeitet wird die Tatsache einer Krankmeldung mit Zeitraum, Status und optionaler Notiz. Diagnosen, Ursachen und Arbeitsunfähigkeitsbescheinigungen sind nicht Gegenstand der Verarbeitung. Patientendaten werden nicht verarbeitet.

4. Art und Zweck der Verarbeitung

Speichern, Anzeigen und Berechnen der Daten (z. B. Überstundenkonto, Resturlaub, Hinweise nach dem Arbeitszeitgesetz), Benachrichtigungen per Push und E-Mail, Exporte, Automatisierungen, Auswertungen, KI-Funktionen, Datensicherung, Support, Wartung und Fehlerbehebung sowie Löschung.

5. KI-Funktionen

- Der KI-Assistent und „Plan reparieren“ sind nur aktiv, wenn sie für den Auftraggeber freigeschaltet sind. Den Assistenten können nur Administratoren nutzen.

- Vor jeder Anfrage ersetzt der Auftragnehmer Namen von Beschäftigten und Räumen durch Platzhalter, auch in Freitexten. Abwesenheitsgründe, Zeiterfassungsdaten, E-Mail-Adressen und Personalnummern werden nicht übermittelt.
- Anfragen gehen über die in Anlage 3 genannten Anbieter nur an Modellanbieter, die sie nicht speichern und nicht zum Training verwenden (Zero Data Retention).
- Ergebnisse sind Entwürfe. Sie werden erst wirksam, wenn ein Nutzer sie prüft und speichert.

6. Löschfristen

Daten	Löschung
Zeiterfassung	automatisch sechs Jahre nach Ende des Kalenderjahres (Praxen in Österreich: sieben Jahre)
Chat-Nachrichten	nach der Frist des Auftraggebers, Standard 90 Tage
Gespräche mit dem KI-Assistenten	durch den Nutzer oder 90 Tage nach der letzten Nachricht
Inhalte von Push-Benachrichtigungen	7 Tage
Push-Token	bei Abmeldung, bei Meldung als ungültig durch den Push-Dienst oder mit dem Konto
übrige Daten	durch den Auftraggeber, spätestens nach § 11

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- **Zutrittskontrolle:** Betrieb ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal; die Rechenzentren sind nach ISO/IEC 27001 zertifiziert. Der Auftragnehmer betreibt keine eigenen Serverräume.
- **Zugangskontrolle:** Serverzugang nur per SSH-Schlüssel; Firewall mit Freigabe nur der benötigten Ports; automatische Sperre bei wiederholten Fehlversuchen; Datenbank und Cache nur im privaten Netzwerk erreichbar. Nutzer melden sich mit E-Mail-Adresse und Passwort an; Passwörter werden nur als Hash gespeichert; Anfragebegrenzung für empfindliche Endpunkte; automatische Abmeldung in der Web-App nach vier Stunden Inaktivität. Die interne Verwaltungskonsole ist zusätzlich vorgeschaltet geschützt und erfordert persönliche Konten mit Zwei-Faktor-Authentifizierung.
- **Zugriffskontrolle:** Rollen für Administratoren und Mitarbeitende nach dem Need-to-know-Prinzip; abgestufte Rollen für Mitarbeitende des Auftragnehmers; Dateien nur über angemeldete oder signierte Abrufe; Gespräche mit dem KI-Assistenten nur für den jeweiligen Nutzer sichtbar.
- **Trennungskontrolle:** Mandantentrennung in der Datenbank über Row-Level Security; die Anwendung nutzt eine Datenbankrolle ohne Eigentümerrechte; getrennte Entwicklungs- und Testumgebungen ohne Echtdaten.
- **Pseudonymisierung:** Pseudonymisierung vor KI-Anfragen; Fehlerberichte und Nutzungsstatistik nur mit pseudonymen Kennungen.

2. Integrität

- **Weitergabekontrolle:** TLS-Verschlüsselung aller Verbindungen zwischen Browser bzw. App und Plattform sowie zu Unterauftragsverarbeitern; Push-Benachrichtigungen ohne Inhalte; Exporte nur für Administratoren.
- **Eingabekontrolle:** Zeiterfassung als fortlaufendes Protokoll mit Zeitpunkt, bearbeitender Person und Quelle; Korrekturen bleiben nachvollziehbar; Protokollierung der Handlungen in der internen Verwaltungskonsole; Dokumentation der Zustimmung zu AGB und AVV.

3. Verfügbarkeit und Belastbarkeit

- Rechenzentren mit redundanter Strom-, Klima- und Netzversorgung.
- Regelmäßige Sicherung der Datenbank mit Verfahren zur Wiederherstellung.
- Fehler- und Verfügbarkeitsüberwachung mit Alarmierung auf einem vom Anwendungsserver getrennten Server.

4. Verfahren zur regelmäßigen Überprüfung

- Überprüfung dieser Maßnahmen und der Unterauftragsverarbeiter mindestens einmal jährlich sowie bei wesentlichen Änderungen.
- Verfahren zur Behandlung von Sicherheitsvorfällen nach § 6.
- Datenschutzfreundliche Voreinstellungen: KI-Funktionen standardmäßig aus, Push-Benachrichtigungen ohne Inhalte, automatische Löschfristen.
- Entwicklung mit Code-Review, automatisierten Tests und regelmäßigen Updates von Abhängigkeiten; Zugangsdaten nicht im Quellcode.

- Mitarbeitende sind auf Vertraulichkeit verpflichtet und im Datenschutz unterwiesen.

Anlage 3: Unterauftragsverarbeiter

Anbieter	Leistung	Daten	Ort, Garantie
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server, Netzwerk, Datenbank, Dateiablage (Object Storage), Fehlerüberwachung, Datensicherung	alle Plattformdaten	Deutschland
Porkbun LLC, Portland, USA	Versand von E-Mails	E-Mail-Adresse, Name, Praxisname, Inhalte der E-Mails, bei Automatisierungen je nach Einstellung auch Abwesenheitsart und Zeiterfassungsdaten	USA, Standardvertragsklauseln
Apple Distribution International Ltd., Cork, Irland	Zustellung von Push-Benachrichtigungen an iOS-Geräte	Push-Token, technische Kennungen, neutraler Text	EU / USA, Data Privacy Framework
Google Ireland Limited, Dublin, Irland	Zustellung von Push-Benachrichtigungen an Android-Geräte	Push-Token, technische Kennungen, neutraler Text	EU / USA, Data Privacy Framework
OpenRouter, Inc., USA	Vermittlung von KI-Anfragen, nur bei freigeschalteten KI-Funktionen	pseudonymisierte Planungsdaten und Eingaben ohne Namen	USA, Standardvertragsklauseln, Zero Data Retention
Modellanbieter über OpenRouter	Ausführung der Sprachmodelle	wie OpenRouter	USA / EU, nur Anbieter mit Zero Data Retention; aktuelle Liste auf Anfrage
650 Industries, Inc. (Expo), USA	Bereitstellung von Updates der Android-App	IP-Adresse, Plattform, App-Version	USA, Standardvertragsklauseln

Nicht im Auftrag des Auftraggebers tätig sind Stripe (Zahlungsabwicklung) sowie die Dienste der Website taktera.de; sie sind in der Datenschutzerklärung beschrieben.

Taktera UG (haftungsbeschränkt) · Hauptstraße 62a · 67472 Esthal · www.taktera.de/avv