Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

nach Artikel 28 der Datenschutz-Grundverordnung (DSGVO)

Fassung 2026-10 · gilt für **beide Betriebsarten** — Einzelplatz und BetreuerSuite-Cloud

---

Zwischen

dem Auftraggeber

Name / Firma: ..... Anschrift: ..... vertreten durch: .....

– nachfolgend **„Auftraggeber"** oder **„Verantwortlicher"** –

und

dem Auftragnehmer

Mario Schütte Calle Galeón 16A 03182 Torrevieja (Alicante) Spanien

NIE / NIF: Z1894288-J E-Mail: info@betreuersuite.com Website: www.betreuersuite.com

– nachfolgend **„Auftragnehmer"** oder **„Auftragsverarbeiter"** –

---

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand. Der Auftragnehmer stellt dem Auftraggeber die Software **BetreuerSuite** zur Verfügung. Die Software kann in zwei Betriebsarten genutzt werden:

Betriebsart	Wo die Daten liegen
Einzelplatz	Ausschließlich auf den eigenen Geräten des Auftraggebers.
Mehrplatz (nachfolgend **„BetreuerSuite-Cloud"**)	Auf einer vom Auftragnehmer betriebenen Serverumgebung, damit mehrere Arbeitsplätze auf denselben Datenbestand zugreifen können.

Der Wechsel zwischen den Betriebsarten erfolgt durch den Auftraggeber selbst in den Einstellungen der Software. **Dieser Vertrag gilt für beide Betriebsarten**, mit dem in Absatz 2 beschriebenen unterschiedlichen Umfang.

(2) Umfang der Auftragsverarbeitung je Betriebsart. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers in unterschiedlichem Umfang:

Betriebsart	Auftragsverarbeitung
Einzelplatz	Hinsichtlich der lokal gespeicherten Daten findet keine Auftragsverarbeitung durch den Auftragnehmer statt. Für die optionalen KI-Funktionen gilt § 2 Abs. 6; der dort angebundene KI-Dienst wird vom Auftraggeber unmittelbar eingesetzt.

Betriebs-art	Auftragsverarbeitung
Betreuer-Suite-Cloud	**Vollumfängliche Auftragsverarbeitung** der in § 2 genannten Daten durch den Auftragnehmer. Für die optionalen KI-Funktionen gilt daneben § 2 Abs. 6.

Soweit dieser Vertrag Regelungen enthält, die ihrer Natur nach nur eine Betriebsart betreffen, gelten sie auch nur für diese. Die Zuordnung ergibt sich aus dem jeweiligen Wortlaut; **Anlage 1 ist ausdrücklich nach Betriebsarten gegliedert**.

(3) Dauer und Zustandekommen. Der Vertrag läuft auf unbestimmte Zeit.

Für die BetreuerSuite-Cloud beginnt er mit der Unterzeichnung durch beide Parteien und ist vor der ersten Übertragung personenbezogener Daten in die Cloud zu schließen. Der Auftragnehmer richtet die Serverumgebung des Auftraggebers erst nach Vertragsschluss ein; ohne die dabei übergebenen Zugangsdaten ist eine Nutzung der Cloud technisch nicht möglich.

Für die Betriebsart Einzelplatz kommt dieser Vertrag durch elektronische Bestätigung des Auftraggebers in der Software zustande. Dem Auftraggeber wird vor der Bestätigung die zum Zeitpunkt des Vertragsschlusses geltende Vertragsfassung zur Verfügung gestellt. Die Bestätigung wird unter Angabe des Zeitpunkts, der Vertragsfassung und des zugehörigen Lizenzschlüssels protokolliert. Der Auftraggeber kann die Vertragsfassung speichern bzw. herunterladen.

Der Vertrag endet mit der Beendigung des zugrunde liegenden Nutzungsverhältnisses. Beide Parteien können ihn mit einer Frist von **einem Monat zum Monatsende** kündigen; das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Rangverhältnis. Dieser Vertrag geht den allgemeinen Vertragsbedingungen vor, soweit es um die Verarbeitung personenbezogener Daten geht.

---

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen

(1) Zweck. Der Auftragnehmer verarbeitet die Daten **ausschließlich** zu dem Zweck, dem Auftraggeber die Nutzung der BetreuerSuite-Cloud zu ermöglichen — also zur Speicherung, Bereitstellung und Sicherung der vom Auftraggeber erfassten Daten. **Eine eigene inhaltliche Auswertung findet nicht statt.**

Für die optionalen KI-Funktionen gilt **Absatz 6**; die dort beschriebene Übermittlung veranlasst der Auftraggeber selbst und ist keine Verarbeitung durch den Auftragnehmer.

(2) Art der Verarbeitung. In der **BetreuerSuite-Cloud**: Speichern, Aufbewahren, Bereitstellen zum Abruf durch die Arbeitsplätze des Auftraggebers, Sichern (Backup) und — nach Weisung oder bei Vertragsende — Löschen. **Die KI-Funktionen (Absatz 6) gehören nicht zu den Verarbeitungstätigkeiten des Auftragnehmers**; er stellt dafür lediglich die technische Schnittstelle bereit.

(3) Besondere Kategorien personenbezogener Daten. Den Parteien ist bewusst, dass im Rahmen der rechtlichen Betreuung regelmäßig **besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO** verarbeitet werden, insbesondere **Gesundheitsda-**

ten. Der Auftragnehmer trifft hierfür die in **Anlage 1** beschriebenen erhöhten Schutzmaßnahmen.

(4) Art der Daten. Verarbeitet werden insbesondere:

Kategorie	Beispiele
Stammdaten der Betreuten	Name, Geburtsdatum, Anschrift, Kontaktdaten, Familienstand
Amtliche Kennzeichen	Aktenzeichen, Steuer-ID, Sozialversicherungs- und Rentenversicherungsnummer, Ausweisnummern
Gesundheitsdaten (Art. 9)	Diagnosen, Pflegegrad, Grad der Behinderung, Merkzeichen, Krankenversicherung, Klinikaufenthalte
Verfahrensdaten	Betreuungsgericht, Aufgabenkreise, Beschlüsse, Fristen, Berichte
Vermögensdaten	Konten, IBAN, Kontostände, Buchungen, Belege, Rechnungslegungen
Sozialleistungsdaten	Einnahmen, Ausgaben, Bescheide
Schriftverkehr	Briefe, Anlagen, Empfänger, Versandnachweise
Daten der Beschäftigten des Auftraggebers	Name, Anzeigename des Arbeitsplatzes, Zugriffszeitpunkte

(5) Kreis der Betroffenen. Betroffene sind insbesondere:

- die vom Auftraggeber rechtlich betreuten Personen,
- deren Angehörige, Bevollmächtigte und Kontaktpersonen,
- Verfahrensbeteiligte und Ansprechpartner bei Behörden, Gerichten und Einrichtungen,
- die Beschäftigten des Auftraggebers, soweit sie die Software nutzen.

(6) KI-Funktionen — gilt in BEIDEN Betriebsarten. Die Software bietet Funktionen an, bei denen der Inhalt eines einzelnen Dokuments zur Auswertung an einen KI-Dienst übermittelt wird (etwa zum Auslesen eines Betreuungsbeschlusses oder zum Entwurf eines Berichts).

Wann	Ausschließlich, wenn der Auftraggeber die Funktion im Einzelfall auslöst. Es gibt keine automatische Übermittlung.
Was	Nur der Inhalt des jeweils verarbeiteten Dokuments. **Keine Übertragung des Gesamtdatenbestands.**
Aktivierung	Die KI-Funktionen sind standardmäßig deaktiviert. Sie können erst genutzt werden, nachdem der Auftraggeber sie gesondert aktiviert und bestätigt hat, dass er für die datenschutzrechtliche Zulässigkeit der über die KI-Funktion verarbeiteten Daten verantwortlich ist. Die Aktivierung wird in der Software gespeichert und kann jederzeit widerrufen werden.
Übertragungsweg	Verschlüsselt über HTTPS/TLS (Version 1.2 oder höher).
Zugangsschlüssel	Der Auftraggeber hinterlegt einen **eigenen** Zugangsschlüssel des KI-Anbieters. Dieser wird ausschließlich lokal gespeichert und **nicht an den Auftragnehmer übertragen**.

Der Empfänger dieser Übermittlung ist in Anlage 2 benannt. Nutzt der Auftraggeber die KI-Funktionen nicht, findet diese Verarbeitung nicht statt.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten **ausschließlich auf dokumentierte Weisung** des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO). Dieser Vertrag und die Nutzung der Software stellen die Grunddokumentation der Weisungen dar.

(2) Weisungen erfolgen in Textform (auch per E-Mail). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer informiert den Auftraggeber **unverzüglich**, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt. Er ist berechtigt, die Ausführung einer solchen Weisung auszusetzen, bis sie bestätigt oder geändert wird.

(4) Der Auftragnehmer übermittelt im Rahmen der von ihm durchgeführten Auftragsverarbeitung über die hierfür eingesetzten Server- und Sicherungssysteme keine personenbezogenen Daten in ein Drittland. Für den E-Mail-Verkehr setzt der Auftragnehmer den Dienst Google Workspace ein (Anlage 2); soweit dabei personenbezogene Daten — etwa in Nachrichten, die der Auftraggeber an den Auftragnehmer richtet — außerhalb der Europäischen Union verarbeitet werden, geschieht dies auf Grundlage von Kapitel V DSGVO, nämlich des mit dem Anbieter geschlossenen Datenverarbeitungszusatzes einschließlich der Standardvertragsklauseln der Europäischen Kommission. Hiervon zu unterscheiden sind die in § 2 Abs. 6 beschriebenen KI-Funktionen. Bei deren Nutzung veranlasst der Auftraggeber unmittelbar von seinem Gerät eine Übermittlung einzelner Dokumentinhalte an den von ihm eingesetzten KI-Dienst; § 6 Abs. 5 und Anlage 2 gelten entsprechend.

Sollte der Auftragnehmer darüber hinaus durch Unionsrecht oder mitgliedstaatliches Recht zu einer Übermittlung verpflichtet werden, teilt er dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

---

§ 4 Vertraulichkeit

(1) Der Auftragnehmer wahrt über alle ihm bekannt werdenden Daten Verschwiegenheit. Diese Pflicht besteht auch nach Beendigung des Vertrags fort.

(2) Der Auftragnehmer setzt zur Verarbeitung ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(3) Der Auftragnehmer ist derzeit **Alleinunternehmer ohne Beschäftigte**. Werden künftig Beschäftigte oder freie Mitarbeiter eingesetzt, verpflichtet er sie **vor** Aufnahme der Tätigkeit schriftlich auf das Datengeheimnis und dokumentiert dies.

(4) Schweigepflicht. Soweit der Auftraggeber einer besonderen Geheimhaltungspflicht unterliegt, wird der Auftragnehmer als mitwirkende Person im Sinne des **§ 203 Abs. 4 StGB** tätig. Er verpflichtet sich, die daraus folgenden Pflichten einzuhalten, und verpflichtet auch etwaige weitere mitwirkende Personen entsprechend.

---

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen nach **Art. 32 DSGVO**. **Anlage 1 ist nach Betriebsarten gegliedert** — Teil A gilt für den Einzelplatz, Teil B für die BetreuerSuite-Cloud, Teil C für beide.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie anpassen, **darf das Schutzniveau dabei aber nicht unterschreiten**. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber auf Anfrage mitzuteilen.

---

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt dem Einsatz der in **Anlage 2** genannten Unterauftragsverarbeiter zu.

(2) Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem **mindestens dieselben Pflichten** auferlegt, die ihn selbst aus diesem Vertrag treffen (Art. 28 Abs. 4 DSGVO).

(3) Der Auftragnehmer informiert den Auftraggeber **mindestens vier Wochen im Voraus** über beabsichtigte Änderungen bei den Unterauftragsverarbeitern. Der Auftraggeber kann einer Änderung binnen zwei Wochen aus wichtigem Grund widersprechen. Widerspricht er, kann der Auftragnehmer den Vertrag mit einer Frist von einem Monat kündigen.

(4) Nicht als Unterauftragsverhältnis gelten Nebenleistungen wie Telekommunikation, Post oder Wartung, bei denen kein Zugriff auf die Daten des Auftraggebers besteht oder ein solcher Zugriff nur zufällig und geringfügig sein kann.

(5) KI-Dienst. Die in § 2 Abs. 6 beschriebenen KI-Funktionen begründen **kein Unterauftragsverhältnis**. Der dort angebundene Dienst wird vom **Auftraggeber unmittelbar eingesetzt**; der Auftragnehmer stellt lediglich die technische Schnittstelle bereit. Einzelheiten und die Verantwortlichkeit des Auftraggebers ergeben sich aus **Anlage 2**.

---

§ 7 Unterstützung des Auftraggebers

(1) Betroffenenrechte. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu erfüllen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen **unverzüglich** an den Auftraggeber weiter und beantwortet es **nicht selbst**.

(3) Weitere Unterstützung. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten aus **Art. 32 bis 36 DSGVO** — Datensicherheit, Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation — soweit dies nach Art der Verarbeitung und den ihm vorliegenden Informationen möglich ist.

(4) Meldung von Datenschutzverletzungen. Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens inner-**

halb von 24 Stunden nach Kenntniserlangung (Art. 33 Abs. 2 DSGVO). Die Meldung enthält, soweit bekannt: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen und die ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

(4a) Wer an die Aufsichtsbehörde meldet. Die Meldung nach **Art. 33 Abs. 1 DSGVO** gegenüber der zuständigen Aufsichtsbehörde obliegt dem **Auftraggeber**; sie ist von ihm binnen **72 Stunden** nach eigener Kenntniserlangung zu erstatten. Der Auftragnehmer meldet einen Vorfall aus der Auftragsverarbeitung **nicht selbst an eine Aufsichtsbehörde**, sondern unterrichtet ausschließlich den Auftraggeber nach Absatz 4 und unterstützt ihn nach Absatz 3.

Die 24-Stunden-Frist des Absatzes 4 ist so bemessen, dass dem Auftraggeber innerhalb seiner eigenen 72-Stunden-Frist ausreichend Zeit für Prüfung und Meldung verbleibt.

---

§ 8 Löschung und Rückgabe

(1) Nach Beendigung des Vertrags löscht der Auftragnehmer sämtliche Daten des Auftraggebers oder gibt sie nach dessen Wahl zurück.

Diese Vorschrift betrifft die BetreuerSuite-Cloud. Im **Einzelplatz** verbleiben sämtliche Daten auf den Geräten des Auftraggebers; der Auftragnehmer hat zu keinem Zeitpunkt Kopien und kann daher nichts zurückgeben oder löschen. Der Auftraggeber kann seine Daten dort über die Sicherungsfunktion selbst exportieren und die Anwendungsdaten anschließend selbst entfernen. Für die über die optionalen KI-Funktionen unmittelbar an den KI-Dienst übermittelten Inhalte gelten die zwischen Auftraggeber und KI-Anbieter vereinbarten Lösch- und Aufbewahrungsbedingungen.

(2) Rückgabe. Auf Verlangen stellt der Auftragnehmer die Daten in einem gängigen, maschinenlesbaren Format zur Verfügung. Der Auftraggeber teilt seine Wahl **innerhalb von 30 Tagen** nach Vertragsende mit.

(2a) Eigener Export durch den Auftraggeber. Unabhängig davon kann der Auftraggeber seine Daten **jederzeit selbst aus der Software heraus exportieren** — er ist dafür nicht auf die Mitwirkung des Auftragnehmers angewiesen. Die Software stellt dafür eine Sicherungs- und eine Aktenexport-Funktion bereit.

Umfang je nach Betriebsart: Im **Einzelplatz** umfasst die Sicherung sowohl den Datenbestand als auch die abgelegten Dateien (Belege, Beschlüsse, Anhänge). In der **BetreuerSuite-Cloud** umfasst der Export derzeit **den Datenbestand; die abgelegten Dateien stellt der Auftragnehmer auf Anforderung gesondert bereit**. Der Auftragnehmer wird die Software so erweitern, dass auch dort beides in einem Schritt exportiert werden kann.

(3) Fristen der Löschung.

Ort	Frist
Laufende Serverumgebung (Datenbank, Dateien, Container)	**binnen 30 Tagen** nach Vertragsende bzw. nach erfolgter Rückgabe
Sicherungen (Backups)	**spätestens nach 12 Monaten**, entsprechend der längsten Aufbewahrungsstufe (Anlage 1)

(4) Hinweis zu Sicherungen. Sicherungen werden aus technischen Gründen **nicht einzeln gelöscht**, sondern laufen nach dem in Anlage 1 beschriebenen Aufbewahrungsplan aus. Bis dahin bleiben sie verschlüsselt und ausschließlich für den Auftragnehmer zugänglich. Der Auftraggeber wird hierüber ausdrücklich informiert.

(5) Der Auftragnehmer bestätigt die vollständige Löschung auf Verlangen in Textform.

(6) Gesetzliche Aufbewahrungspflichten bleiben unberührt. Betroffene Daten werden in diesem Fall gesperrt und nicht weiter verarbeitet.

---

§ 9 Nachweise und Kontrollrechte

(1) Der Auftragnehmer weist die Einhaltung der Pflichten aus diesem Vertrag auf Anfrage nach — insbesondere durch Vorlage der aktuellen Fassung von Anlage 1, der Verträge mit Unterauftragsverarbeitern und einer Beschreibung des Sicherungskonzepts.

(2) Der Auftraggeber ist berechtigt, die Einhaltung zu überprüfen. Die Überprüfung erfolgt **nach vorheriger Ankündigung mit angemessener Frist — mindestens zwei Wochen — zu den üblichen Geschäftszeiten** und ohne Störung des Betriebsablaufs.

(3) Der Auftraggeber kann die Überprüfung selbst vornehmen oder einen Prüfenden beauftragen. Der Prüfende darf **kein Wettbewerber** des Auftragnehmers sein und ist zur Verschwiegenheit zu verpflichten.

(4) Der Auftragnehmer kann Nachweise durch aktuelle Zertifikate, Berichte oder Berichtsauszüge unabhängiger Stellen erbringen, soweit diese für den Auftraggeber eine gleichwertige Prüfmöglichkeit eröffnen.

(5) Für den Aufwand einer Vor-Ort-Prüfung, die über die Vorlage von Nachweisen hinausgeht, kann der Auftragnehmer eine angemessene Vergütung verlangen; dies gilt nicht, wenn die Prüfung durch einen begründeten Verdacht auf einen Verstoß veranlasst ist.

---

§ 10 Haftung

(1) Der Auftragnehmer haftet unbeschränkt für Schäden, die auf vorsätzlichem oder grob fahrlässigem Verhalten des Auftragnehmers, seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen, sowie für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, soweit der Auftragnehmer, seine gesetzlichen Vertreter oder Erfüllungsgehilfen die Pflichtverletzung zu vertreten haben.

(2) Bei einfach fahrlässiger Verletzung wesentlicher Vertragspflichten haftet der Auftragnehmer nur für den vertragstypischen und bei Vertragsschluss vorhersehbaren Schaden. Die Haftung nach diesem Absatz ist der Höhe nach auf das vom jeweiligen Auftraggeber für einen Zeitraum von zwölf Monaten geschuldete Jahresentgelt für die vertragsgegenständliche Leistung begrenzt.

(3) Wesentliche Vertragspflichten im Sinne des Absatzes 2 sind solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf. Im Übrigen ist die Haftung des Auftrag-

nehmers für einfach fahrlässig verursachte Schäden ausgeschlossen.

(4) Die vorstehenden Haftungsbeschränkungen gelten nicht, soweit eine Haftung aufgrund zwingender gesetzlicher Vorschriften nicht ausgeschlossen oder beschränkt werden kann. Insbesondere bleiben die Ansprüche und Haftungsregelungen nach der Verordnung (EU) 2016/679 (DSGVO), insbesondere Artikel 82 DSGVO, unberührt.

(5) Die vorstehenden Haftungsbeschränkungen gelten ferner nicht, soweit der Auftragnehmer eine Garantie übernommen oder einen Mangel arglistig verschwiegen hat.

---

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

(3) Rechtswahl. Dieser Vertrag unterliegt dem Recht des Königreichs Spanien unter Ausschluss seiner kollisionsrechtlichen Vorschriften. Zwingende Vorschriften des Unionsrechts sowie zwingende Vorschriften des Rechts, die unabhängig von der Rechtswahl Anwendung finden, bleiben unberührt. Die Anwendung der DSGVO, insbesondere der zwingenden Vorschriften über Rechte betroffener Personen, Haftung und Rechtsbehelfe, bleibt unberührt.

(4) Gerichtsstand. Für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer sind, soweit gesetzlich zulässig, die zuständigen Gerichte in Torrevieja, Spanien, zuständig. Zwingende Gerichtsstände, insbesondere nach Art. 79 Abs. 2 DSGVO, bleiben unberührt.

Ort, Datum: .....

Auftraggeber: .....

Auftragnehmer: .....

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: 26.09.2026

Diese Anlage ist nach Betriebsarten gegliedert:

Teil	Gilt für
Teil A	Einzelplatz
Teil B	BetreuerSuite-Cloud
Teil C	beide Betriebsarten

Teil A — Einzelplatz

A1. Ort der Speicherung

Die Daten werden **ausschließlich auf dem Gerät des Auftraggebers** gespeichert, im Anwendungsverzeichnis des jeweiligen Betriebssystems:

Betriebssystem	Speicherort
macOS	`~/Library/Application Support/betreuer-suite`
Windows	`%APPDATA%\betreuer-suite`

Der Zugriffsschutz richtet sich nach dem Benutzerkonto und dem Sicherheitsmodell des jeweiligen Betriebssystems. **Der Auftragnehmer hat auf diese Daten keinen Zugriff** und speichert zu keinem Zeitpunkt Kopien.

A2. Maßnahmen im Einzelplatz

Maßnahme	Umsetzung
Zugriffskontrolle	Der Auftragnehmer hat keinen technischen Zugriff auf den Datenbestand des Auftraggebers.
Löschung	Die Software stellt eine Löschfunktion bereit, die alle zu einer betreuten Person gehörenden Daten einschließlich der abgelegten Dateien entfernt.
Sicherung	Die Software stellt eine Sicherungsfunktion bereit, die Datenbestand **und** abgelegte Dateien in einem Archiv zusammenfasst. Der Auftraggeber wählt den Ablageort selbst.
Export einzelner Akten	Über die Aktenexport-Funktion lassen sich einzelne Betreuungsakten ausgeben — insbesondere zur Erfüllung von Betroffenenrechten nach Art. 15 und 20 DSGVO.
Zugangsschlüssel des KI-Dienstes	Wird ausschließlich lokal gespeichert und **nicht an den Auftragnehmer übertragen**.

Verantwortung des Auftraggebers. Im Einzelplatz liegen Datensicherung, Geräteschutz, Verschlüsselung des Datenträgers und Zugangsschutz zum Gerät in seiner Hand. Der Auftragnehmer stellt die Werkzeuge bereit, kann ihre Nutzung aber nicht überwachen.

Teil B — BetreuerSuite-Cloud

B1. Ort der Verarbeitung

Server-betrieb	**Hetzner Online GmbH, Rechenzentrum Nürnberg** (Standortkennung `nbg1-dc3`), Deutschland
Sicherungen	**Hetzner Storage Box, Standort Falkenstein**, Deutschland
Land	Die im Auftrag verarbeiteten Daten werden auf den hierfür eingesetzten Server- und Sicherungssystemen **ausschließlich in Deutschland** verarbeitet.

B2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle. Die Rechenzentren werden von der Hetzner Online GmbH betrieben. Zutrittsschutz, Videoüberwachung und Besucherverwaltung richten sich nach deren technischen und organisatorischen Maßnahmen (Anlage 2).

Zugangskontrolle.

- Jeder Auftraggeber erhält eine **eigene, isolierte Serverumgebung** (eigener Container, eigene Datenbank, eigenes Datenverzeichnis, eigener Netzwerk-Port). Ein Zugriff über Mandantengrenzen hinweg ist technisch ausgeschlossen.
- Der Zugang erfolgt über einen **individuellen Zugangsschlüssel** von 43 Zeichen Länge aus kryptografisch sicherer Zufallsquelle, der ausschließlich diesem Auftraggeber zugeordnet ist.
- Zusätzlich kann **je Arbeitsplatz ein eigener Zugangsschlüssel** vergeben werden. Scheidet ein Arbeitsplatz aus, lässt sich dessen Zugang **einzeln sperren**, ohne die übrigen Arbeitsplätze zu beeinträchtigen.
- Der Vergleich der Zugangsschlüssel erfolgt **laufzeitunabhängig**, um Rückschlüsse über die Antwortzeit auszuschließen.
- Fehlversuche werden **je Absenderadresse begrenzt** (Sperre nach wiederholten Fehlversuchen).
- Der administrative Zugang zum Server erfolgt ausschließlich über **SSH mit Schlüsselpaar**; eine Anmeldung mit Passwort ist abgeschaltet.

Zugriffskontrolle.

- Die Datenbankschnittstelle nimmt **ausschließlich vordefinierte Arten von Anweisungen** entgegen (Lesen, Einfügen, Ändern, Löschen einzelner Datensätze sowie das Anlegen von Tabellen und das Hinzufügen von Spalten, soweit dies für die Aktualisierung der Software erforderlich ist). Anweisungen, die Tabellen oder Spalten **entfernen** oder umbenennen, sowie dateisystemnahe Anweisungen werden **abgewiesen**.
- Änderungs- und Löschanweisungen ohne Einschränkung auf bestimmte Datensätze werden abgewiesen.
- Dateizugriffe sind auf das Datenverzeichnis des jeweiligen Auftraggebers beschränkt; Pfadangaben werden vor der Ausführung geprüft.

Trennungskontrolle. Ein Container, eine Datenbank und ein Datenverzeichnis **je Auftraggeber**. Auch die Sicherungen liegen in **getrennten, je Auftraggeber eigenen Archiven** — dies

ermöglicht die Löschung eines einzelnen Auftraggebers, ohne die Sicherungen anderer zu berühren.

Pseudonymisierung/Verschlüsselung.

- Die Übertragung zwischen den Arbeitsplätzen des Auftraggebers und dem Server erfolgt **ausschließlich verschlüsselt (TLS)**; unverschlüsselte Verbindungen werden auf die verschlüsselte Adresse umgeleitet. Die Zertifikate werden automatisch erneuert.
- Die **Sicherungen sind verschlüsselt** (Verfahren: Borg, `repokey-blake2`). Der Schlüssel liegt getrennt vom Sicherungsziel.
- Zugangsschlüssel je Arbeitsplatz werden **nicht im Klartext**, sondern als Prüfsumme gespeichert.

B3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Die Server-Ports sind **ausschließlich lokal gebunden** und nicht unmittelbar aus dem Internet erreichbar; der Zugang läuft über einen vorgeschalteten Reverse-Proxy mit TLS.
- Eine Firewall lässt nur die Ports 22, 80 und 443 zu.
- Sicherheitsaktualisierungen des Betriebssystems werden **automatisch eingespielt**.
- Die Datenbank wird bei jeder Sicherung auf **Unversehrtheit geprüft** (`integrity_check`); ein Fehlschlag löst eine Meldung aus.

B4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Sicherungslauf	**stündlich**, automatisiert
Verfahren	verschlüsselte, deduplizierte Archive; Zwischenkopie wird vor dem Sichern auf Unversehrtheit geprüft
Ziel	Hetzner Storage Box, **getrennt vom Produktivsystem**
Schutz vor Löschung	Der Server kann Sicherungen **nur hinzufügen, nicht entfernen** (append-only). Der zum Löschen berechtigte Schlüssel liegt **nicht auf dem Server**.
Aufbewahrung	**48 stündliche · 14 tägliche · 8 wöchentliche · 12 monatliche** Stände
Überwachung	Ein vom Sicherungslauf **unabhängiger** Wächter prüft alle 30 Minuten, ob die letzte erfolgreiche Sicherung nicht älter als drei Stunden ist, und meldet per E-Mail. Zusätzlich ein wöchentlicher Bericht als Lebenszeichen.
Wiederherstellung	**vierteljährlich erprobt**, mit Prüfung von Datenbestand, Dateien und Unversehrtheit

B5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Vierteljährlicher Wiederherstellungstest (siehe oben).
- Änderungen an der Serversoftware werden vor der Übernahme geprüft; vor jeder Übernahme wird der Datenbestand gesichert und der Rückweg auf die Vorgängerfassung offenge-

halten.

- Alle Eingriffe am Server werden dokumentiert.

B6. Protokollierung

Zugriffe auf die Schnittstelle werden protokolliert. Das Protokoll enthält **Zeitpunkt, Art des Zugriffs, Antwortstatus und den Arbeitsplatz**. Es enthält **bewusst keine Inhaltsdaten**, keine Datenbankabfragen, keine Dateinamen und keine vollständigen Absenderadressen — diese werden gekürzt.

B7. Grenzen — ausdrücklich benannt

- **Der Auftragnehmer hat technisch Zugriff auf die Daten**, da er den Server administriert.

Organisatorisch gilt: Ein Zugriff auf Inhaltsdaten erfolgt **ausschließlich anlassbezogen** — zur Beseitigung einer Störung, zur Wiederherstellung nach einem Datenverlust oder auf ausdrückliche Weisung des Auftraggebers — und nur in dem Umfang, der dafür erforderlich ist. Eine Einsichtnahme ohne solchen Anlass findet nicht statt.

Protokollierung administrativer Zugriffe. Administrative Zugriffe des Auftragnehmers auf die Serverumgebung des Auftraggebers werden technisch protokolliert. Ein solcher Zugriff setzt die Angabe eines Anlasses voraus; ohne Anlass wird er nicht ausgeführt. Protokolliert werden Zeitpunkt, betroffene Serverumgebung und Anlass sowie Art, Länge und Prüfsumme des ausgeführten Befehls — der Befehl selbst bewusst nicht im Wortlaut, damit das Protokoll wie nach Nr. 6 keine Inhaltsdaten enthält. Jeder Zugriff wird bei seinem Beginn per E-Mail an den Auftragnehmer gemeldet. Das Protokoll wird **24 Monate** aufbewahrt und zusätzlich in den Sicherungsbestand übernommen, den der Server nur ergänzen, aber nicht verändern oder löschen kann (Nr. 4).

Grenze: Die Protokollierung macht administrative Zugriffe nachvollziehbar und ein Umgehen auffällig. Sie ist **kein technischer Schutz gegen den Administrator selbst**, der den Server verwaltet und die Protokollierung technisch umgehen könnte.

- Eine **Verschlüsselung der Daten auf dem Server in der Weise, dass auch der Auftragnehmer sie nicht lesen könnte** (Ende-zu-Ende-Verschlüsselung), besteht **nicht**. Sie ist mit der Funktionsweise der Software derzeit nicht vereinbar.
- Der Auftragnehmer ist **Alleinunternehmer**. Bei Ausfall kann die Behebung von Störungen länger dauern als bei einem Unternehmen mit mehreren Beschäftigten. Der Sicherungsbestand ist davon nicht betroffen.

Teil C — Beide Betriebsarten

C1. KI-Funktionen (§ 2 Abs. 6)

Maßnahme	Umsetzung
Datensparsamkeit	Übermittelt wird ausschließlich der Inhalt des jeweils verarbeiteten Dokuments. **Keine Übertragung des Gesamtdatenbestands.**
Aktivierung	Die KI-Funktionen sind standardmäßig deaktiviert. Sie können erst genutzt werden, nachdem der Auftraggeber sie gesondert aktiviert und bestätigt hat, dass er für die datenschutzrechtliche Zulässigkeit der über die KI-Funktion verarbeiteten Daten verantwortlich ist. Die Aktivierung wird in der Software gespeichert und kann jederzeit widerrufen werden.
Verschlüsselung	Übertragung ausschließlich über HTTPS/TLS (Version 1.2 oder höher).
Zugangsschlüssel	Wird lokal beim Auftraggeber gespeichert und **nicht an den Auftragnehmer übertragen**.
Kein Zwang	Die Software ist ohne die KI-Funktionen vollständig nutzbar.

C2. Softwarepflege

Maßnahme	Umsetzung
Aktualisierungen	Sicherheitsrelevante Korrekturen werden über den Aktualisierungskanal der Software verteilt.
Signierte Auslieferung	Die Programmdateien sind digital signiert und für macOS zusätzlich von Apple beglaubigt, sodass Veränderungen auf dem Übertragungsweg erkennbar sind.

Anlage 2 — Unterauftragsverarbeiter

Stand: 26.09.2026

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Serverbetrieb (Rechenzentrum), Speicherplatz für Sicherungen	Nürnberg und Falkenstein, **Deutschland**	Auftragsverarbeitungsvertrag vom **29.08.2026**, Fassung 1.2 vom 16.02.2026
Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland	E-Mail-Dienst (Google Workspace): Versand von Betriebsmeldungen und der Kaufbestätigung, Posteingang der Adressen info@betreuersuite.com und support@betreuersuite.com	Europäische Union und USA (keine feste Datenregion)	Cloud Data Processing Addendum (mit EU-Standardvertragsklauseln), akzeptiert am **12.09.2026**

Die im Rahmen der BetreuerSuite-Cloud im Auftrag verarbeiteten Kundendaten werden auf den hierfür eingesetzten Server- und Sicherungssystemen **ausschließlich in Deutschland** verarbeitet. **Hiervon unberührt bleibt die gesondert geregelte Übermittlung einzelner Dokumentinhalte an den KI-Dienst** (§ 2 Abs. 6), die nicht über diese Systeme läuft.

Hinweis zu weiteren Dienstleistern des Auftragnehmers: Für die Lizenzverwaltung und den Zahlungsverkehr werden weitere Dienstleister eingesetzt. Diese haben **keinen Zugriff auf die in der BetreuerSuite-Cloud gespeicherten Daten** und sind daher nicht Unterauftragsverarbeiter im Sinne dieses Vertrags.

KI-Dienst als vom Auftraggeber unmittelbar eingesetzter Auftragsverarbeiter

Für die in § 2 Abs. 6 beschriebenen KI-Funktionen setzt der Auftragnehmer keinen Unterauftragsverarbeiter ein. Die Software stellt lediglich die technische Schnittstelle bereit, über die der Auftraggeber auf eigene Veranlassung unmittelbar von seinem Gerät auf einen KI-Dienst zugreift.

Der Auftraggeber unterhält hierzu ein eigenes Vertragsverhältnis mit dem Anbieter des KI-Dienstes und verwendet einen eigenen Zugangsschlüssel, den er selbst beim Anbieter erhält und ausschließlich lokal verwaltet. Der Auftragnehmer erhält weder diesen Zugangsschlüssel noch die an den KI-Dienst übermittelten Dokumentinhalte; die Übermittlung erfolgt nicht über Systeme des Auftragnehmers.

Der Auftraggeber ist für die datenschutzrechtliche Zulässigkeit dieses Verarbeitungsvorgangs verantwortlich. Er hat insbesondere sicherzustellen, dass mit dem Anbieter die nach Art. 28 DSGVO erforderliche Vereinbarung besteht und die Voraussetzungen für eine etwaige Übermittlung personenbezogener Daten in ein Drittland nach Kapitel V DSGVO erfüllt sind.

Derzeit technisch angebundener KI-Dienst ist Anthropic PBC, 548 Market St PMB 90375, San Francisco, CA 94104, USA. Nach den derzeit veröffentlichten Bedingungen stellt Anthropic für seine kommerziellen Dienste einschließlich der API eine Datenverarbeitungsvereinbarung ein-

schließlich Standardvertragsklauseln bereit.

Aufbewahrung beim KI-Dienst: Die Aufbewahrung richtet sich nach dem unmittelbar zwischen Auftraggeber und KI-Anbieter bestehenden Vertragsverhältnis. Der Auftraggeber ist für die Auswahl und Konfiguration der dort geltenden Aufbewahrungsbedingungen verantwortlich.

Nutzt der Auftraggeber die KI-Funktionen nicht, findet diese Übermittlung nicht statt. Die Software ist ohne sie vollständig nutzbar.

Anlage 3 — Kontakt

Auftragnehmer

Mario Schütte Calle Galeón 16A 03182 Torrevieja (Alicante) Spanien

NIE / NIF: Z1894288-J E-Mail: info@betreuersuite.com Website: www.betreuersuite.com

Datenschutzbeauftragter: Ein Datenschutzbeauftragter ist derzeit nicht bestellt. Nach der gegenwärtigen Art und dem gegenwärtigen Umfang der Verarbeitung besteht keine Pflicht zur Benennung eines Datenschutzbeauftragten. Die Voraussetzungen des Art. 37 Abs. 1 DSGVO, insbesondere eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 37 Abs. 1 lit. c DSGVO, werden regelmäßig erneut geprüft. Eine zusätzliche Bestellpflicht nach Art. 34 LOPDGDD besteht derzeit nicht.

Kontaktweg für Datenschutzvorfälle:

info@betreuersuite.com

Über diese Adresse läuft die Verständigung in **beide Richtungen**: Der Auftragnehmer unterrichtet den Auftraggeber darüber nach § 7 Abs. 4, und der Auftraggeber kann eigene Beobachtungen hierher melden.

Bitte kennzeichnen Sie solche Nachrichten im Betreff mit **„Datenschutzvorfall"**, damit sie vorrangig bearbeitet werden.

Nicht darüber läuft die Meldung an die Aufsichtsbehörde. Diese erstattet nach **Art. 33 Abs. 1 DSGVO** der **Auftraggeber** selbst gegenüber seiner eigenen zuständigen Aufsichtsbehörde — siehe § 7 Abs. 4a.