Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO · Stand: 9. November 2026

Auftraggeber (Verantwortlicher): der Nutzer von BetreuerWerk (Berufsbetreuerin, Berufsbetreuer oder Betreuungsverein) als Vertragspartner des Nutzungsvertrags.

Auftragnehmer (Auftragsverarbeiter): Florian Hartschwager, BetreuerWerk, Kumbusch 7, 49328 Melle, E-Mail: florian@betreuerwerk.de

Dieser Vertrag ist Bestandteil des Nutzungsvertrags über BetreuerWerk (AGB, § 6). Er gilt ohne gesonderte Unterschrift mit dem Abschluss des Nutzungsvertrags. Auf Wunsch stellen wir eine von beiden Seiten unterzeichnete Fassung bereit.

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Software BetreuerWerk zur Verwaltung seiner Betreuungen bereit. Dabei verarbeitet er personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers.

(2) Der Vertrag gilt für die Dauer des Nutzungsvertrags und endet mit ihm. Pflichten zur Löschung, Rückgabe und Vertraulichkeit gelten darüber hinaus.

§ 2 Art und Zweck der Verarbeitung, Daten, Betroffene

(1) **Zweck:** Speichern, Ordnen, Durchsuchen, Auswerten (auch mit KI), Darstellen, Übermitteln auf Veranlassung des Auftraggebers (z. B. Briefe, E-Mails, eBO-Nachrichten an Gerichte und Behörden), Abrufen von Kontoinformationen, Erstellen von Berichten, Anträgen und Rechnungslegungen sowie Löschen.

(2) **Arten von Daten:**

- Stammdaten der betreuten Personen (Name, Anschrift, Geburtsdatum, Aktenzeichen, Aufgabenkreise)
- Gesundheitsdaten und weitere besondere Kategorien nach Art. 9 DSGVO (z. B. Diagnosen, Pflegegrad, Behandlungen)
- Vermögens-, Konto- und Zahlungsdaten (Kontostände, Umsätze, Verbindlichkeiten, Einnahmen und Ausgaben)
- Dokumente, Schriftverkehr, E-Mails, eBO-Nachrichten, Aktennotizen, Aufgaben und Fristen
- Kontaktdaten von Angehörigen, Ärzten, Einrichtungen, Behörden, Gerichten und weiteren Beteiligten
- Daten der Mitarbeiter des Auftraggebers, die BetreuerWerk nutzen (Name, E-Mail, Zeiterfassung, Protokoll der Aktionen)

(3) **Betroffene:** betreute Personen, deren Angehörige und Bezugspersonen, Kontaktpersonen bei Behörden, Gerichten, Einrichtungen und Dienstleistern sowie Mitarbeiter des Auftraggebers.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers. Weisungen sind die Nutzung der Funktionen von BetreuerWerk sowie Anweisungen in Textform (E-Mail genügt).

(2) Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er dies dem Auftraggeber unverzüglich mit. Er darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

(3) Eine Verarbeitung für eigene Zwecke des Auftragnehmers, insbesondere Werbung oder das Training von KI-Modellen, findet nicht statt.

§ 4 Vertraulichkeit und Berufsgeheimnis

(1) Der Auftragnehmer und alle Personen, die für ihn Zugang zu den Daten haben, sind zur Vertraulichkeit

verpflichtet. Diese Pflicht besteht auch nach Vertragsende.

(2) Soweit der Auftraggeber einer gesetzlichen Schweigepflicht unterliegt (z. B. § 203 StGB), nimmt der Auftragnehmer als mitwirkende Person davon Kenntnis und verpflichtet sich zur Verschwiegenheit. Er verschafft sich Kenntnis von geschützten Inhalten nur, soweit dies für die Leistung erforderlich ist, etwa zur Fehlerbehebung auf Bitte des Auftraggebers. Weitere mitwirkende Personen und Unterauftragsverarbeiter werden entsprechend verpflichtet.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in Anlage 1 beschriebenen Maßnahmen nach Art. 32 DSGVO. Er darf sie an den Stand der Technik anpassen, wenn das Schutzniveau nicht sinkt.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Mit jedem besteht ein Vertrag, der den Pflichten dieses Vertrags entspricht.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor dem Einsatz eines neuen oder dem Wechsel eines Unterauftragsverarbeiters per E-Mail. Der Auftraggeber kann aus wichtigem Datenschutzgrund innerhalb dieser Frist widersprechen. Kommt keine Einigung zustande, kann er den Nutzungsvertrag zum Zeitpunkt der Änderung kündigen.

(3) Keine Unterauftragsverarbeiter sind Stellen, an die der Auftraggeber Daten selbst übermitteln lässt (z. B. Gerichte und Behörden über das eBO, E-Mail-Empfänger, das vom Auftraggeber angebundene eigene E-Mail-Postfach) und Anbieter, die als eigene Verantwortliche handeln (siehe Anlage 2, Teil B).

§ 7 Verarbeitung außerhalb der EU

Die Daten werden in der Europäischen Union verarbeitet. Haben Unterauftragsverarbeiter ihren Sitz außerhalb der EU, sind Übermittlungen durch die EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) abgesichert; Einzelheiten nennt Anlage 2.

§ 8 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei Anfragen betroffener Personen (Art. 15–22 DSGVO), bei der Sicherheit der Verarbeitung, bei Datenschutz-Folgenabschätzungen und bei Anfragen von Aufsichtsbehörden. BetreuerWerk bietet dafür eigene Funktionen, insbesondere den Export einer vollständigen Betreutenakte und das Löschen von Daten.

§ 9 Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 48 Stunden nachdem er davon Kenntnis erlangt hat, per E-Mail. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Daten und Personen, wahrscheinliche Folgen und ergriffene Maßnahmen, damit der Auftraggeber seine Pflichten nach Art. 33 und 34 DSGVO erfüllen kann.

§ 10 Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die zum Nachweis erforderlichen Informationen zur Verfügung, insbesondere diesen Vertrag mit Anlagen und die Verträge mit den Unterauftragsverarbeitern. Kontrollen vor Ort sind nach Anmeldung mit angemessener Frist zu den Geschäftszeiten möglich; Rechenzentren der Unterauftragsverarbeiter werden über deren Nachweise und Zertifikate kontrolliert.

§ 11 Löschung und Rückgabe nach Vertragsende

(1) Bis zum Vertragsende kann der Auftraggeber seine Daten jederzeit selbst exportieren (z. B. „Akte exportieren“ je Betreuten).

(2) Nach Vertragsende löscht der Auftragnehmer alle Daten des Auftraggebers innerhalb von 30 Tagen (AGB § 7.4), soweit keine gesetzliche Aufbewahrungspflicht besteht. Datensicherungen und ältere Dateiversionen werden nach Ablauf der in Anlage 1 genannten Fristen entfernt.

§ 12 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Regelungen der AGB.

(2) Bei Widersprüchen zwischen diesem Vertrag und den AGB geht dieser Vertrag in Fragen des Datenschutzes vor. Änderungen bedürfen der Textform. Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

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

1. Vertraulichkeit

- **Zutritt:** Server und Speicher stehen ausschließlich in Rechenzentren der Unterauftragsverarbeiter (Hetzner Falkenstein, AWS Frankfurt) mit Zutrittskontrolle und ISO-27001-Zertifizierung. Der Auftragnehmer betreibt keine eigenen Serverräume.
- **Zugang:** Anmeldung mit persönlichem Konto; Passwörter werden nur als kryptografischer Hash gespeichert. Die Verwaltung der Server ist nur per SSH-Schlüssel des Betreibers möglich.
- **Zugriff:** Strikte Mandantentrennung: Jedes Büro hat eine eigene Kennung, und jede Datenbankabfrage ist auf das eigene Büro beschränkt; dies wird durch automatisierte Tests geprüft. Dokumente sind nicht öffentlich erreichbar und werden nur über signierte Links mit höchstens 15 Minuten Gültigkeit ausgeliefert. Der Verwaltungsbereich ist auf das Betreiberkonto beschränkt.
- **Trennung:** Entwicklung und Tests laufen mit getrennter Datenbank und erfundenen Beispieldaten; Prüfungen im Echtbetrieb nur im eigenen Büro des Betreibers.
- **Datensparsamkeit:** Server-Protokolle enthalten keine Inhalte (keine Namen, Texte, Dateinamen oder ungekürzten Kontonummern), sondern nur Kennungen und Fehlercodes; dies wird automatisiert geprüft. Suchbegriffe für die Internetsuche werden vor dem Absenden auf Namen, Geburtsdaten, Aktenzeichen und IBANs geprüft und bei Treffern nicht gesendet. Support-Anfragen werden vor dem Speichern automatisch um bekannte Personendaten bereinigt.
- **Verschlüsselung:** Alle Übertragungen sind verschlüsselt (TLS). Die Datenbank ist beim Anbieter verschlüsselt gespeichert. Für den Dokumentenspeicher ist eine zusätzliche Verschlüsselung der gespeicherten Dateien in Vorbereitung; bis dahin schützen Zugriffsbeschränkung und signierte Links.

2. Integrität

- **Weitergabe:** Übermittlungen an Unterauftragsverarbeiter, Banken und das eBO erfolgen ausschließlich verschlüsselt.
- **Eingabe:** Ein Aktivitätsprotokoll hält fest, wer wann welche Änderung vorgenommen hat. KI-Vorschläge werden erst nach Bestätigung durch den Nutzer übernommen.

3. Verfügbarkeit und Belastbarkeit

- Datenbank als verwalteter Dienst mit Wiederherstellung auf jeden Zeitpunkt der letzten 6 Stunden.
- Dokumentenspeicher mit Versionierung: Gelöschte oder überschriebene Dateien bleiben 30 Tage wiederherstellbar.
- Neue Programmversionen werden erst nach bestandenen Prüfungen und in einem Schritt ausgetauscht; die Vorversion bleibt als Rückfall erhalten.
- Stromversorgung, Brandschutz und Netzredundanz durch die Rechenzentren der Unterauftragsverarbeiter.

4. Überprüfung und Datenschutz durch Technik

- Vor jeder Auslieferung laufen automatisierte Tests, darunter Tests zur Mandantentrennung und zum Inhalt der Protokolle.

- Programmänderungen werden zusätzlich durch eine unabhängige technische Prüfung kontrolliert.
- KI-Verarbeitung ausschließlich in der EU; abweichende Regionen sind technisch gesperrt. Der Nutzung von Inhalten zum Training wurde widersprochen.
- Keine Tracking-, Analyse- oder Werbe-Cookies.
- Unterauftragsverarbeiter nur mit Vertrag nach Art. 28 DSGVO (Anlage 2).

Anlage 2: Unterauftragsverarbeiter

Teil A: Genehmigte Unterauftragsverarbeiter

Hetzner

Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland

Betrieb der Anwendungsserver und des Dokumentenspeichers (Object Storage)
Deutschland (Rechenzentrum Falkenstein)
Auftragsverarbeitungsvertrag nach Art. 28 DSGVO (Fassung 1.2, abgeschlossen am 05.10.2026)

Neon

Databricks, Inc. mit Neon, LLC, San Francisco, USA

Betrieb der Datenbank (PostgreSQL)
Deutschland (AWS-Region Frankfurt, eu-central-1); Betriebsmesswerte ohne Inhalte bei Grafana Labs, USA
Data Processing Addendum (Databricks DPA v3) mit EU-Standardvertragsklauseln

AWS

Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg

KI-Auswertungen und Kira-Chat (Amazon Bedrock) sowie Spracheingabe (Amazon Transcribe)
EU (Region Frankfurt, EU-Inferenzprofile nur mit Rechenzentren in der EU)
AWS Data Processing Addendum mit EU-Standardvertragsklauseln; Nutzung von Inhalten zur Verbesserung der KI-Dienste per Organisationsrichtlinie widersprochen

Staan

European Search Perspective SAS, 42 avenue de la Porte de Clichy, 75017 Paris, Frankreich

Internetsuche für Kira (nur Suchbegriffe, vorab automatisch auf Namen, Geburtsdaten, Aktenzeichen und IBANs geprüft)
Frankreich (OVH)
Data Processing Agreement nach Art. 28 DSGVO

Resend

Plus Five Five, Inc. (Resend), San Francisco, USA

Versand von System-E-Mails (z. B. Benachrichtigungen, Einladungen)
EU (Irland)
Data Processing Addendum mit EU-Standardvertragsklauseln

mailbox.org

Heinlein Hosting GmbH, Schwedter Straße 9a, 10119 Berlin, Deutschland

Geschäftspostfach von BetreuerWerk (Support-Kommunikation)
Deutschland
Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Die Unterauftragsverarbeiter setzen ihrerseits weitere Dienstleister ein, die sie in ihren Verträgen benennen.

Teil B: Eigenständig Verantwortliche (keine Auftragsverarbeitung)

BANKSapi (BANKSapi Technology GmbH, Pettenkoferstraße 35, 80336 München, Deutschland): Kontoabruf und Zahlungsauslösung für verknüpfte Bankkonten (BaFin-zugelassener Zahlungsdienst). Eigener Verantwortlicher bis zur Übergabe der Kontodaten an BetreuerWerk (AGB Zahlungsdienste, Nr. 2.6–2.9). Ab der Übergabe der Kontodaten verarbeitet BetreuerWerk sie im Auftrag des Auftraggebers nach diesem Vertrag.