

Auftragsverarbeitungsvertrag DokuHilfe

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

dem Verantwortlichen {Firma / Einrichtung} {Straße, PLZ Ort}
{Vertreten durch} — nachfolgend **Auftraggeber** —

und

Florian Weise Rosenstrasse 11, 29439 Lüchow E-Mail:
info.doku.hilfe@gmail.com — nachfolgend **Auftragnehmer** —

§ 1 Gegenstand und Dauer

1. Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten zur Erstellung von Dokumentationsentwürfen für soziale Einrichtungen durch das Software-Angebot „DokuHilfe“ (<https://doku-hilfe.de>).
2. Der Auftrag beginnt mit der erstmaligen Nutzung des Dienstes durch den Auftraggeber und endet mit der Kündigung des Nutzungsverhältnisses.
3. Die Verarbeitung erfolgt ausschließlich nach den Weisungen des Auftraggebers.

§ 2 Art und Zweck der Verarbeitung

1. Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers folgende personenbezogene Daten:
 - Texteingaben des Auftraggebers oder dessen Mitarbeitenden (Stichworte, Beobachtungen, Berichte)
 - Optionale Audio-Aufnahmen (Diktate) zur Transkription
 - Optionale Bildaufnahmen (z. B. Wundfotos) zur Analyse, sofern aktiviert
 - Nutzungsmetadaten (Anmeldezeitpunkt, Anzahl Anfragen, Vorlage)
1. Die Verarbeitung dient ausschließlich der KI-gestützten Erstellung von strukturierten Pflege- und Sozialdokumentations-Entwürfen.
2. **Keine** Datenverarbeitung erfolgt zu eigenen Werbe-, Profiling- oder Trainings-Zwecken des Auftragnehmers oder seiner Unterauftragnehmer.
3. **Status der Bildanalyse-Funktion:** Die Funktion zur KI-gestützten Bildanalyse (z. B. von Wundfotos) ist eine **Beta-Funktion**. Sie ist standardmäßig **deaktiviert** und kann ausschließlich durch den Unternehmens-Administrator des Auftraggebers über die Admin-Oberfläche aktiviert oder jederzeit wieder deaktiviert werden. Vor der Aktivierung muss der Auftraggeber den separaten Beta-Hinweis (im Admin-Bereich angezeigt) bestätigen. Der Auftragnehmer kann die Beta-Funktion ohne Vorlauffrist deaktivieren, falls technische oder rechtliche Gründe dies erforderlich machen.

§ 3 Art der personenbezogenen Daten

1. Folgende Daten-Kategorien werden im Rahmen des Auftrags verarbeitet:
 - **Stammdaten:** Vorname, Nachname, Initialen oder Pseudonyme von Bewohnern/Klienten (sofern vom Auftraggeber selbst in die Stichworte eingegeben)
 - **Gesundheits- und Sozialdaten** nach Art. 9 Abs. 1 DSGVO: Beobachtungen zu Wohlbefinden, Verhalten, Förderung, medizinische Notizen, bei aktivierter Bildanalyse auch Wundfotos
 - **Beschäftigtendaten:** Anmeldedaten der Mitarbeitenden des Auftraggebers (E-Mail, Benutzername)

- **Nutzungs-Metadaten:** IP-Adresse beim Login (kurzzeitig), Zeitstempel, Anzahl Anfragen

1. **Datensparsamkeit — ausdrückliche Empfehlung des Auftragnehmers:** Die Eingabe von Klarnamen, vollständigen Geburtsdaten, Anschriften, Kontaktdaten oder anderen direkt identifizierenden personenbezogenen Daten von Bewohnern/ Klienten in die Stichworte oder Diktate **ist ausdrücklich unerwünscht und nicht erforderlich** für die Funktion der DokuHilfe. Der Auftraggeber wird ausdrücklich angehalten, ausschließlich **Initialen, Pseudonyme oder Bewohner-Nummern** zu verwenden. Die generierten Dokumentationsentwürfe werden vom Auftraggeber im Anschluss in dessen eigenes Pflege-/Sozial-Dokumentationssystem übertragen, in dem die Zuordnung zur Person erst nach Bedarf erfolgt. Der Auftragnehmer übernimmt keine Verantwortung für vom Auftraggeber unnötig eingegebene Klardaten — die Verarbeitung erfolgt in jedem Fall ausschließlich für den vereinbarten Zweck und unter den vereinbarten Schutzmaßnahmen (siehe Anhang 1).

§ 4 Kategorien betroffener Personen

- Bewohner, Klienten oder Pflegebedürftige in Einrichtungen des Auftraggebers
- Mitarbeitende des Auftraggebers (Beschäftigtendatenschutz)

§ 5 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten **ausschließlich auf dokumentierte Weisung** des Auftraggebers.
2. Der Auftragnehmer **gewährleistet die Vertraulichkeit** der zur Auftragsdurchführung eingesetzten Personen. Diese sind nach Art. 28 Abs. 3 b) DSGVO zur Vertraulichkeit verpflichtet.
3. Der Auftragnehmer hat **technische und organisatorische Maßnahmen** (TOMs) ergriffen, die im **Anhang 1** dieses Vertrags spezifiziert sind.
4. Der Auftragnehmer unterstützt den Auftraggeber bei:
 - Anfragen Betroffener nach Art. 15-22 DSGVO
 - Datenpannenmeldungen nach Art. 33, 34 DSGVO (Mitteilung innerhalb von 24 h nach Bekanntwerden)
 - Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO

- Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO
1. Der Auftragnehmer stellt dem Auftraggeber **alle erforderlichen Informationen** zum Nachweis der Einhaltung der DSGVO-Pflichten zur Verfügung und ermöglicht Audits (Art. 28 Abs. 3 h DSGVO) im Rahmen angemessener Vorankündigung.
 2. Nach Beendigung der Auftragsverarbeitung **werden alle personenbezogenen Daten gelöscht** oder zurückgegeben (auf Wunsch des Auftraggebers). Gesetzliche Aufbewahrungsfristen bleiben unberührt.

§ 6 Unterauftragsverarbeiter

1. Der Auftragnehmer setzt folgende **Unterauftragsverarbeiter** ein:

Mistral AI SAS

Sitz: 15 rue des Halles, 75001 Paris, Frankreich.

Zweck: Textgenerierung, Bildanalyse und Sprache-zu-Text (Voxtral) im Default-Routing-Modus „eu_cloud“.

Rahmen: Mistral-DPA und aktuelle Unterauftragsverarbeiter-Liste.

Brevo / Sendinblue SAS

Sitz: 17 rue Salneuve, 75017 Paris, Frankreich.

Zweck: SMTP-Registrierungsbenachrichtigung bei Start einer Testphase.

Rahmen: Brevo-DPA und aktuelle Unterauftragsverarbeiter-Liste.

Lokales KI-Modell auf RTX-4070-Hardware

Sitz: Rosenstrasse 11, 29439 Lüchow, Deutschland.

Zweck: Optionale lokale KI-Verarbeitung bei den Routing-Modi „cost_save“ oder „dsgvo_strict“; kein Cloud-Transfer.

Lokaler Whisper-Server auf RTX-4070-Hardware

Sitz: Rosenstrasse 11, 29439 Lüchow, Deutschland.

Zweck: Sprache-zu-Text-Transkription (faster-whisper, Modell large-v3) bei `audio_provider='local'`.

netcup GmbH

Sitz: Emmy-Noether-Str. 10, 76131 Karlsruhe, Deutschland.

Zweck: Hosting der Plattform-Infrastruktur (Root-Server, Datenbank). Eigene Unterauftragsverarbeiter laut netcup-AVV Anhang 2: Anexia Holding GmbH (Klagenfurt, AT), Anexia Cloud Solutions GmbH (Klagenfurt, AT und Karlsruhe, DE). Die Verarbeitung erfolgt EU/EWR-intern; netcup ist nach ISO 9001, ISO 27001 und ISO 27701 zertifiziert.

(1a) Der Auftragnehmer übermittelt Daten nicht bewusst an einen eigenen Dienstleister außerhalb der EU bzw. des EWR. Soweit ein hier genannter Unterauftragsverarbeiter seinerseits weitere Unterauftragnehmer einsetzt oder Daten übermittelt, richten sich deren Verarbeitung und erforderliche Garantien nach dessen jeweils geltendem DPA und Unterauftragsverarbeiter-Liste.

(1b) Für Mistral gilt das Data Processing Addendum. In der verwendeten Mistral-Organisation sind „Data usage for improving our services“ und Labs-Modelle deaktiviert (Stand 19.08.2026). Neue API-Interaktionen werden damit nicht zum Training der Mistral-Modelle verwendet.

(1c) Brevo verarbeitet ausschließlich für den Versand der internen Registrierungsbenachrichtigung Unternehmensname, E-Mail-Adresse und Benutzername des Unternehmens-Administrators sowie das Trial-Enddatum. Dokumentations-, Audio- oder Bildinhalte werden nicht an Brevo übermittelt.

1. **Änderung von Unterauftragsverarbeitern:** Der Auftragnehmer informiert den Auftraggeber **mindestens 30 Tage vor Wirksamwerden** schriftlich (auch per E-Mail) über jede beabsichtigte Änderung. Der Auftraggeber kann der Änderung innerhalb dieser Frist widersprechen. Bei begründetem Widerspruch und fehlender Einigung steht dem Auftraggeber ein Sonderkündigungsrecht zu.
2. Der Auftraggeber stimmt der **Einbindung der unter Abs. 1 genannten Unterauftragsverarbeiter** mit Abschluss dieses Vertrags **ausdrücklich zu**.

§ 7 Weisungsrecht des Auftraggebers

1. Weisungen sind grundsätzlich in **Textform** zu erteilen (E-Mail genügt). Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.
2. Der Auftragnehmer hat den Auftraggeber **unverzüglich zu informieren**, wenn er der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt.
3. Standard-Weisung mit Vertragsabschluss: Verarbeitung im Rahmen des Funktionsumfangs der DokuHilfe-Plattform nach dem jeweils dokumentierten Stand (<https://doku-hilfe.de/datenschutz>).

§ 8 Aufzeichnung und Mitteilung von Datenpannen

1. Bei Datenpannen, die personenbezogene Daten dieses Auftrags betreffen, informiert der Auftragnehmer den Auftraggeber **unverzüglich, spätestens innerhalb von 24 Stunden** nach Bekanntwerden per E-Mail an die hinterlegte Kontaktadresse.
2. Die Mitteilung enthält mindestens:
 - Beschreibung der Art der Verletzung
 - Kategorien und ungefähre Anzahl der betroffenen Personen
 - Wahrscheinliche Folgen
 - Bereits ergriffene oder geplante Maßnahmen

§ 9 Haftung

Die Haftung der Vertragsparteien richtet sich nach Art. 82 DSGVO und den ergänzenden gesetzlichen Bestimmungen.

§ 10 Schlussbestimmungen

1. Dieser Vertrag unterliegt deutschem Recht.
2. Erfüllungs- und Gerichtsstand ist der Geschäftssitz des Auftragnehmers, soweit der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.
3. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Unterschriften

{Ort, Datum}

Auftraggeber

Auftragnehmer (Florian Weise)

Anhang 1 — Technische und organisatorische Maßnahmen (TOMs)

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

- **Zugangskontrolle:** Login mit Benutzername + Passwort, JWT-Token mit 8 h Lebensdauer, Passwort-Hashes nach bcrypt
- **Zugriffskontrolle:** Rollen-basierte Berechtigung (User, Company-Admin, System-Admin); Mitarbeitende eines Auftraggebers sehen ausschließlich Daten ihrer eigenen Company (Multi-Tenancy)
- **Datenträgerkontrolle:** Hosting-Provider (netcup, zertifiziert nach ISO 27001 und ISO 27701) mit physikalischer Trennung von Systemen, Datenbanken und Datenträgern sowie Datenträgervernichtung nach Sicherheitsstufe H-4; lokales Modell auf verschlüsselter SSD
- **Transportkontrolle:** Verbindungen ausschließlich über HTTPS (TLS 1.2+); interne Kommunikation zwischen DokuHilfe und RTX-4070 über [[Tailscale]]-VPN (WireGuard)
- **Verfügbarkeitskontrolle:** Tägliche Datenbank-[[Backups]], separate Aufbewahrung; Service-Uptime-Monitoring

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

- **Eingabekontrolle:** Logging aller administrativen Änderungen (Anlegen/Sperren von Benutzern, Tarif-Änderungen)
- **Übermittlungskontrolle:** HTTPS für alle Datenübertragungen; KI-Verarbeitung ausschließlich innerhalb der EU (Mistral AI SAS, Frankreich) oder lokal in Deutschland — keine Drittlandübermittlung

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

- **Backups:** SQLite-Datenbanken werden **täglich automatisch um 03:00 Uhr** via systemd-Timer (db-backup.timer) in /root/backups/db-daily/ gesichert; Aufbewahrung **30 Tage rollend**. Zusätzlich werden vor strukturellen Änderungen (Schema-Migrationen, Software-Updates) manuelle Sicherungen erstellt.

- **Ausfallsicherheit:** Bei Ausfall des lokalen KI-Modells automatischer Fallback auf die EU-Cloud-Variante (Mistral, Frankreich; mit transparenter Anzeige im Frontend)

4. Verfahren zur Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- **Datenschutzkonzept:** dieser AVV plus Datenschutzerklärung <https://doku-hilfe.de/datenschutz>
- **Auftragskontrolle:** Unterauftragsverarbeiter werden vor Einbindung auf DSGVO-Konformität geprüft (DPA-Existenz, Standardvertragsklauseln, EU-Repräsentant)
- **Datenschutz durch Voreinstellungen (Privacy by Default):** Bildanalyse standardmäßig **deaktiviert**; Cost-Routing-Modus standardmäßig „**eu_cloud**“ (Mistral AI, Frankreich, EU-intern) — keine Drittlandübermittlung
- **Auditierbarkeit:** Logging aller Generate-Aufrufe in `api_usage`-Tabelle und LLM-Hub-Dashboard

5. Datenschutzkonforme Datenverarbeitung (Art. 32 Abs. 1 lit. d DSGVO)

- **Bilddaten** werden vor Übermittlung an Cloud-Sub-Verarbeiter **EXIF-Metadaten-bereinigt** (GPS, Kameramodell, Aufnahmezeitpunkt werden entfernt) und **auf 2048 × 2048 px verkleinert**
 - **Bilddaten werden nicht persistiert** — sie verbleiben ausschließlich im flüchtigen Arbeitsspeicher während der Analyse
 - **Audio-Dateien** werden nach Transkription nicht gespeichert
 - **Texteingaben** werden nach 12 Stunden automatisch aus der Temporär-Speicherung gelöscht; die rechtliche Aufbewahrungspflicht liegt beim Auftraggeber (z. B. in dessen Pflegesoftware)
-