

# AUFTRAGSVERARBEITUNGSVERTRAG

gemaess Art. 28 DSGVO  
(Datenschutz-Grundverordnung)

## Paragraph 1 - Vertragsparteien

### Zwischen

dem Auftraggeber (Verantwortlicher im Sinne der DSGVO):

Name/Firma: \_\_\_\_\_

Anschrift: \_\_\_\_\_

Vertreten durch: \_\_\_\_\_

- nachfolgend 'Auftraggeber' genannt -

### und

dem Auftragnehmer (Auftragsverarbeiter im Sinne der DSGVO):

#### **Dieter Horst**

Einzelunternehmer, handelnd unter SYSTEMHAUS HORST

Kleibrink 42, 59229 Ahlen

E-Mail: [E-MAIL EINFUEGEN]

- nachfolgend 'Auftragnehmer' genannt -

## Paragraph 2 - Gegenstand und Dauer der Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung der Software 'EVY' / 'MIRA' (KI-Assistenzsystem mit Brain-Funktion).

(2) Die Verarbeitung umfasst folgende Taetigkeiten:

- Speicherung von Benutzerdaten (Zugangsdaten, Profildaten)
- Speicherung von Brain-Inhalten (vom Nutzer eingegebenes Wissen)
- Speicherung von Chat-Verlaeufen
- Verarbeitung von Dokumenten (sofern hochgeladen)
- Technischer Betrieb und Datensicherung

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages (Nutzungsvertrag). Nach Vertragsende werden die Daten genaess Paragraph 10 dieses AVV geloesch.

## Paragraph 3 - Art der personenbezogenen Daten

Folgende Datenkategorien werden verarbeitet:

Kategorie	Beispiele
Stammdaten	Name, E-Mail, Benutzername, Firma
Nutzungsdaten	Login-Zeiten, IP-Adressen, Geraeteinformationen
Inhaltsdaten	Brain-Eintraege, Chat-Nachrichten, hochgeladene Dokumente

Ggf. besondere Kategorien	Falls vom Nutzer selbst eingegeben (z.B. Gesundheitsdaten im Brain)
---------------------------	---

*Hinweis: Der Auftraggeber ist dafür verantwortlich, welche Daten seine Nutzer in das System eingeben. Der Auftragnehmer hat hierauf keinen Einfluss.*

## Paragraph 4 - Kreis der Betroffenen

Die Verarbeitung betrifft folgende Personengruppen:

- Mitarbeiter/Nutzer des Auftraggebers
- Kunden des Auftraggebers (falls deren Daten im System gespeichert werden)
- Geschäftspartner (falls deren Daten im System gespeichert werden)
- Sonstige Personen, deren Daten der Auftraggeber in das System eingibt

## Paragraph 5 - Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach EU- oder nationalem Recht zur Verarbeitung verpflichtet.

(2) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben.

(3) Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Massnahmen gemäss Art. 32 DSGVO (siehe Paragraph 7).

(4) Der Auftragnehmer beachtet die Bedingungen für die Inanspruchnahme von Unterauftragnehmern (siehe Paragraph 6).

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Betroffenenrechten (Auskunft, Löschung, Berichtigung etc.).

(6) Der Auftragnehmer unterstützt den Auftraggeber bei Datenschutz-Folgenabschätzungen, sofern erforderlich.

(7) Der Auftragnehmer löscht oder gibt nach Beendigung der Verarbeitung alle Daten zurück (siehe Paragraph 10).

(8) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung zur Verfügung und ermöglicht Überprüfungen.

## Paragraph 6 - Unterauftragnehmer

(1) Der Auftraggeber erteilt hiermit eine allgemeine Genehmigung zur Beauftragung von Unterauftragnehmern.

(2) Derzeit werden folgende Unterauftragnehmer eingesetzt:

Unterauftragnehmer	Sitz	Leistung
Anthropic PBC	USA (San Francisco)	KI-API (Claude)
[Hoster, falls extern]	[Land]	Server-Hosting

(3) Bei Wechsel oder Hinzunahme von Unterauftragnehmern informiert der Auftragnehmer den Auftraggeber vorab. Der Auftraggeber kann innerhalb von 14 Tagen Einspruch erheben.

**(4) Hinweis zur KI-Verarbeitung: Bei Nutzung der KI-Chat-Funktion werden die Eingaben an den KI-Anbieter (z.B. Anthropic) übermittelt. Dies ist technisch notwendig. Der Auftraggeber stimmt dem mit Abschluss dieses Vertrages zu.**

(5) Der Auftragnehmer stellt sicher, dass Unterauftragnehmer vertraglich zu gleichwertigen Datenschutzpflichten verpflichtet werden.

## **Paragraph 7 - Technische und organisatorische Massnahmen (TOM)**

Der Auftragnehmer hat folgende Massnahmen nach Art. 32 DSGVO getroffen:

### **7.1 Vertraulichkeit**

- Zutrittskontrolle: Server in gesicherten Räumlichkeiten/Rechenzentren
- Zugangskontrolle: Passwortschutz, SSH-Keys für Serveradministration
- Zugriffskontrolle: Berechtigungskonzept, rollenbasierter Zugriff
- Trennungskontrolle: Mandantentrennung in der Software (Multi-Tenant)

### **7.2 Integrität**

- Weitergabekontrolle: Verschlüsselte Übertragung (HTTPS/TLS)
- Eingabekontrolle: Protokollierung von Änderungen

### **7.3 Verfügbarkeit und Belastbarkeit**

- Verfügbarkeitskontrolle: Regelmässige Backups
- Rasche Wiederherstellbarkeit: Dokumentierte Wiederherstellungsprozesse
- Belastbarkeit: Überwachung der Systemressourcen

### **7.4 Verfahren zur regelmässigen Überprüfung**

- Regelmässige Sicherheitsupdates
- Überprüfung der Zugriffsrechte
- Dokumentation von Sicherheitsvorfällen

## **Paragraph 8 - Meldepflichten bei Datenschutzverletzungen**

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich (innerhalb von 24 Stunden) über jede Verletzung des Schutzes personenbezogener Daten.

(2) Die Meldung enthält mindestens:

- Art der Verletzung
- Betroffene Datenkategorien und Personengruppen
- Wahrscheinliche Folgen
- Ergriffene Abhilfemassnahmen

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gegenüber Aufsichtsbehörden und Betroffenen.

## **Paragraph 9 - Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Anforderungen zu überprüfen.

(2) Kontrollen können erfolgen durch:

- Einholung von Auskünften
- Einsichtnahme in Dokumentation und Nachweise
- Vor-Ort-Prüfungen (nach vorheriger Anmeldung)

- (3) Der Auftragnehmer stellt alle erforderlichen Informationen zur Verfügung.

### **Paragraph 10 - Löschung und Rückgabe von Daten**

- (1) Nach Beendigung des Hauptvertrages löscht der Auftragnehmer alle personenbezogenen Daten, sofern keine gesetzliche Aufbewahrungspflicht besteht.
- (2) Auf Wunsch des Auftraggebers erfolgt vorher eine Rückgabe der Daten in einem gängigen Format (z.B. JSON, CSV).
- (3) Die Löschung erfolgt innerhalb von 30 Tagen nach Vertragsende, sofern der Auftraggeber keinen Export anfordert.
- (4) Der Auftragnehmer bestätigt die vollständige Löschung schriftlich auf Anfrage.

### **Paragraph 11 - Weisungsrecht**

- (1) Der Auftraggeber kann Weisungen zur Datenverarbeitung erteilen. Weisungen sind in Textform zu erteilen (E-Mail genügt).
- (2) Weisungsberechtigte Person beim Auftraggeber: \_\_\_\_\_
- (3) Weisungsempfänger beim Auftragnehmer: Dieter Horst (oder benannte Vertretung)
- (4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung gegen Datenschutzrecht verstößt.

### **Paragraph 12 - Haftung**

- (1) Die Parteien haften gegeneinander Betroffenen gemäß Art. 82 DSGVO.
- (2) Im Innenverhältnis haftet jede Partei für Schäden, die durch von ihr zu vertretende Verstöße verursacht wurden.
- (3) Die Haftung richtet sich im Übrigen nach den Regelungen des Hauptvertrages.

### **Paragraph 13 - Laufzeit**

- (1) Dieser AVV ist Bestandteil des Hauptvertrages (Nutzungsvertrag/Lizenzvertrag) und tritt mit dessen Unterzeichnung in Kraft.
- (2) Die Laufzeit entspricht der Laufzeit des Hauptvertrages.
- (3) Nachwirkende Pflichten (insbesondere Vertraulichkeit, Löschung) bleiben auch nach Vertragsende bestehen.

### **Paragraph 14 - Schlussbestimmungen**

- (1) Änderungen dieses Vertrages bedürfen der Textform.
- (2) Es gilt deutsches Recht. Gerichtsstand ist Ahlen.
- (3) Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam.
- (4) Dieser AVV ersetzt alle vorherigen Vereinbarungen zur Auftragsverarbeitung zwischen den Parteien.

## **UNTERSCHRIFTEN**

---

Ort, Datum

---

Ort, Datum

---

**Auftraggeber**  
(Verantwortlicher)

---

**Dieter Horst**  
SYSTEMHAUS HORST (Auftragsverarbeiter)

*HINWEIS: Dieser AVV ist ein Muster und sollte vor Verwendung rechtlich geprüft werden. Die TOM (Paragraph 7) sind ggf. an die tatsächlichen Gegebenheiten anzupassen.*