

AUFTAGSVERARBEITUNGSVERTRAG

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 Tätigkeiten:

- Speicherung von Benutzerdaten (Zugangsdaten, Profildaten)
- Speicherung von Brain-Inhalten (vom Nutzer eingegebenes Wissen)
- Speicherung von Chat-Verläufen
- 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 gemaess Paragraph 10 dieses AVV gelöscht.

Paragraph 3 - Art der personenbezogenen Daten

Folgende Datenkategorien werden verarbeitet:

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

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

Hinweis: Der Auftraggeber ist dafuer 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)
- Geschaeftspartner (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 gewaehrleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben.
- (3) Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Massnahmen gemaess Art. 32 DSGVO (siehe Paragraph 7).
- (4) Der Auftragnehmer beachtet die Bedingungen fuer die Inanspruchnahme von Unterauftragnehmern (siehe Paragraph 6).
- (5) Der Auftragnehmer unterstuetzt den Auftraggeber bei der Erfuellung von Betroffenenrechten (Auskunft, Loeschung, Berichtigung etc.).
- (6) Der Auftragnehmer unterstuetzt den Auftraggeber bei Datenschutz-Folgenabschaetzungen, sofern erforderlich.
- (7) Der Auftragnehmer loescht oder gibt nach Beendigung der Verarbeitung alle Daten zurueck (siehe Paragraph 10).
- (8) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung zur Verfuegung und ermoeglicht Ueberpruefungen.

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 [Hoster, falls extern]	USA (San Francisco) [Land]	KI-API (Claude) 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) uebermittelt. 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 Raeumen/Rechenzentren
- Zugangskontrolle: Passwortschutz, SSH-Keys fuer Serveradministration
- Zugriffskontrolle: Berechtigungskonzept, rollenbasiertes Zugriff
- Trennungskontrolle: Mandantentrennung in der Software (Multi-Tenant)

7.2 Integritaet

- Weitergabekontrolle: Verschluesselte Uebertragung (HTTPS/TLS)
- Eingabekontrolle: Protokollierung von Aenderungen

7.3 Verfuegbarkeit und Belastbarkeit

- Verfuegbarkeitskontrolle: Regelmaessige Backups
- Rasche Wiederherstellbarkeit: Dokumentierte Wiederherstellungsprozesse
- Belastbarkeit: Ueberwachung der Systemressourcen

7.4 Verfahren zur regelmaessigen Ueberpruefung

- Regelmaessige Sicherheitsupdates
- Ueberpruefung der Zugriffsrechte
- Dokumentation von Sicherheitsvorfaellen

Paragraph 8 - Meldepflichten bei Datenschutzverletzungen

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

(2) Die Meldung enthaelt mindestens:

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

(3) Der Auftragnehmer unterstuetzt den Auftraggeber bei der Erfuellung seiner Meldepflichten gegenueber Aufsichtsbehoerden und Betroffenen.

Paragraph 9 - Kontrollrechte des Auftraggebers

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

(2) Kontrollen koennen erfolgen durch:

- Einholung von Auskuenften
- Einsichtnahme in Dokumentation und Nachweise
- Vor-Ort-Pruefungen (nach vorheriger Anmeldung)

(3) Der Auftragnehmer stellt alle erforderlichen Informationen zur Verfuegung.

Paragraph 10 - Loeschung und Rueckgabe von Daten

(1) Nach Beendigung des Hauptvertrages loescht der Auftragnehmer alle personenbezogenen Daten, sofern keine gesetzliche Aufbewahrungspflicht besteht.

(2) Auf Wunsch des Auftraggebers erfolgt vorher eine Rueckgabe der Daten in einem gaengigen Format (z.B. JSON, CSV).

(3) Die Loeschung erfolgt innerhalb von 30 Tagen nach Vertragsende, sofern der Auftraggeber keinen Export anfordert.

(4) Der Auftragnehmer bestaetigt die vollstaendige Loeschung schriftlich auf Anfrage.

Paragraph 11 - Weisungsrecht

(1) Der Auftraggeber kann Weisungen zur Datenverarbeitung erteilen. Weisungen sind in Textform zu erteilen (E-Mail genuegt).

(2) Weisungsberechtigte Person beim Auftraggeber: _____

(3) Weisungsempfaenger beim Auftragnehmer: Dieter Horst (oder benannte Vertretung)

(4) Der Auftragnehmer informiert den Auftraggeber unverzueglich, wenn er der Meinung ist, dass eine Weisung gegen Datenschutzrecht verstoesst.

Paragraph 12 - Haftung

(1) Die Parteien haften gegeneuber Betroffenen gemaess Art. 82 DSGVO.

(2) Im Innenverhaeltnis haftet jede Partei fuer Schaeden, die durch von ihr zu vertretende Verstoesse verursacht wurden.

(3) Die Haftung richtet sich im Uebrigen 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, Loeschung) bleiben auch nach Vertragsende bestehen.

Paragraph 14 - Schlussbestimmungen

(1) Aenderungen dieses Vertrages beduerfen der Textform.

(2) Es gilt deutsches Recht. Gerichtsstand ist Ahlen.

(3) Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Uebrigen 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 geprueft werden. Die TOM (Paragraph 7) sind ggf. an die tatsaechlichen Gegebenheiten anzupassen.