

ZUSATZVEREINBARUNG ZUR WAHRUNG DER BERUFLICHEN SCHWEIGEPFLICHT (§ 203 StGB)

gemäß § 203 Abs. 3 S. 2, Abs. 4 StGB
§203-Anlage 1.2 – Anlage 5 zum AVV 1.2

Ellie Worx UG (haftungsbeschränkt)

KI-Assistenzsystem für Psychotherapeut:innen
Architekturprinzip: Verarbeiten. Unterstützen. Löschen.

Version:	1.2
Stand:	02.11.2026
Verantwortlich:	Peter Wolfgang Rieger-Stemmer, Geschäftsführer
Grundlage:	AVV 1.2 / TOM 1.2/ Governance 1.1
Status:	Anlage 5 zum AVV 1.2

Vertragsparteien

Auftraggeber (Verantwortlicher / Berufsgeheimnisträger)

[Name / Praxis des Auftraggebers]

[Adresse]

[E-Mail]

nachfolgend „Verantwortlicher“ oder „Berufsgeheimnisträger“

Auftragnehmer (Auftragsverarbeiter)

Ellie Worx UG (haftungsbeschränkt)

Heinrich-Weißmann-Str. 18,

88048 Friedrichshafen

Vertreten durch: Peter Wolfgang Rieger-Stemmer, Geschäftsführer

nachfolgend „Auftragsverarbeiter“

§ 1 Präambel und Zweck

(1) Der Verantwortliche ist Berufsgeheimnisträger im Sinne des § 203 StGB und unterliegt der strafrechtlich sanktionierten Schweigepflicht. Er verarbeitet im Rahmen seiner beruflichen Tätigkeit regelmäßig Geheimnisse im Sinne des § 203 StGB, insbesondere Gesundheitsdaten, Behandlungs- und Therapieinhalte.

(2) Diese §203-Anlage ergänzt den zwischen den Parteien geschlossenen Auftragsverarbeitungsvertrag (AVV 1.2) gemäß Art. 28 DSGVO. Sie konkretisiert die berufsgeheimnisrechtlichen Anforderungen an die Einbindung des Auftragsverarbeiters und seiner Mitwirkenden gemäß § 203 Abs. 3 S. 2 und Abs. 4 StGB.

(3) Ziel ist die Sicherstellung, dass eine Kenntnisnahme geschützter Inhalte durch den Auftragsverarbeiter, dessen Mitarbeitende oder Unterauftragnehmer technisch und organisatorisch ausgeschlossen ist (**Zero-Access**) und dass solche Inhalte nicht dauerhaft gespeichert werden (**Zero-Retention**).

(4) Im Fall von Widersprüchen gehen die strengeren Anforderungen dieser §203-Anlage den Regelungen des AVV vor, soweit dies zur Wahrung der Schweigepflicht erforderlich ist.

§ 2 Begriffe

(1) **Geschützte Inhalte** sind sämtliche Informationen, die dem Verantwortlichen im Rahmen seiner beruflichen Tätigkeit anvertraut oder bekannt werden. Dies umfasst insbesondere Gesundheitsdaten im Sinne des Art. 9 DSGVO, Therapie- und Behandlungsinhalte, Befunde, Diagnosen, Anamnesen, Berichte, Dokumente und Kommunikation sowie alle daraus ableitbaren sensiblen Informationen.

(2) **Zero-Access** bezeichnet eine technische und organisatorische Ausgestaltung, bei der der Auftragsverarbeiter und seine eingesetzten Personen keine Möglichkeit haben, geschützte Inhalte in Klartext zur Kenntnis zu nehmen, zu entschlüsseln oder wiederherzustellen.

(3) **Zero-Retention** bezeichnet die als **Null-Speicher-Architektur** (vgl. AVV 1.2 § 5; Governance 1.1, § 3) implementierte Ausgestaltung, bei der geschützte Inhalte nach Ende einer Nutzungssitzung nicht dauerhaft beim Auftragsverarbeiter gespeichert werden, sondern ausschließlich flüchtig und temporär verarbeitet werden, soweit dies zur Bereitstellung der Assistenzleistung erforderlich ist.

(4) **Mitwirkende** sind alle beim Auftragsverarbeiter oder bei von ihm eingesetzten Unterauftragnehmern tätigen Personen, die mit Betrieb, Wartung, Support, Sicherheit oder sonstiger Leistungserbringung befasst sind.

§ 3 Grundsätze: Zero-Access und Zero-Retention

(1) Der Auftragsverarbeiter sichert zu, dass ausschließlich der Verantwortliche bzw. die von ihm autorisierten Endnutzer Zugriff auf geschützte Inhalte haben.

(2) Der Auftragsverarbeiter und seine Mitwirkenden haben keine Möglichkeit, geschützte Inhalte dauerhaft zu speichern, manuell einzusehen oder zu entschlüsseln. Die zur Leistungserbringung erforderliche temporäre maschinelle Verarbeitung durch KI-Sprachmodelle (Azure OpenAI Services) erfolgt ausschließlich flüchtig und begründet keinen menschlichen Zugriff auf geschützte Inhalte. Dies gilt insbesondere für Administrations-, Betriebs-, Wartungs- und Supportzugänge, Zugriff auf Datenbanken oder Storage-Systeme, Einsicht in Logs, Tracing, Monitoring oder Error-Tracking sowie Wiederherstellung aus Backups, Snapshots oder Recovery-Systemen.

(3) Der Auftragsverarbeiter hält keine Schlüssel oder sonstige Zugangsmittel vor, die eine Entschlüsselung geschützter Inhalte ermöglichen.

(4) Der Auftragsverarbeiter speichert geschützte Inhalte nicht dauerhaft. Nach Ende einer Nutzungssitzung werden flüchtige und temporäre Artefakte (Arbeitsspeicher, temporäre Dateien, Caches, Queues) unverzüglich gelöscht. Ergebnisse können ausschließlich lokal durch den Verantwortlichen gespeichert werden.

(5) Der Auftragsverarbeiter stellt sicher, dass geschützte Inhalte nicht in Protokolldaten (Logs), Telemetrie, Monitoring, Error-Tracking, Ticketsystemen oder Backups verarbeitet oder gespeichert werden (vgl. TOM 1.2, Abschnitt 3 und 4).

(6) Die Empfehlung zur Eingabe anonymisierter bzw. pseudonymisierter Inhalte gemäß AVV 1.2, § 4 Abs. 2 bleibt unberührt. Die datenschutz- und berufsrechtliche Verantwortung für die Entscheidung über den Grad der Pseudonymisierung liegt beim Verantwortlichen. Die Zusicherungen nach Absätzen 1 bis 5 gelten unabhängig hiervon.

§ 4 Verpflichtung der Mitwirkenden

(1) Der Auftragsverarbeiter verpflichtet alle Mitwirkenden auf strikte Vertraulichkeit gemäß § 203 Abs. 4 S. 1 StGB. Die Verpflichtung umfasst insbesondere ein Verbot der Kenntnisnahme, Offenlegung oder Nutzung von Informationen, die Rückschlüsse auf geschützte Inhalte zulassen.

(2) Der Auftragsverarbeiter stellt durch organisatorische Maßnahmen sicher, dass Mitwirkende nur insoweit Zugriff auf technische Systeme erhalten, wie dies zur Leistungserbringung zwingend erforderlich ist (Need-to-know, Least Privilege; vgl. TOM 1.2, Abschnitt 2.3).

(3) Der Auftragsverarbeiter schult Mitwirkende – sofern vorhanden – regelmäßig zu Vertraulichkeit, IT-Sicherheit und den besonderen Anforderungen bei Berufsgeheimnistragenden, einschließlich § 203 StGB und Art. 32 DSGVO.

§ 5 Unterauftragnehmer und Lieferkette

(1) Der Auftragsverarbeiter setzt Unterauftragnehmer ausschließlich nach Maßgabe des AVV 1.2, § 9 (Art. 28 Abs. 2–4 DSGVO) ein. Die aktuelle Liste der Unterauftragnehmer ergibt sich aus Anlage 2 zum AVV 1.2 .

(2) Der Auftragsverarbeiter stellt sicher, dass Unterauftragnehmer und deren Mitwirkende **keinen Zugriff** auf geschützte Inhalte in Klartext erhalten. Das Zero-Access- und Zero-Retention-Prinzip wird in der gesamten Lieferkette gewahrt.

(3) Derzeit eingesetzte Unterauftragnehmer:

Microsoft Ireland Operations Limited (Azure / Azure OpenAI Services) – Cloud-Infrastruktur und KI-Modelle. Standort: EU (Deutschland/EU). Grundlage: Microsoft DPA, Zero-Data-Retention-Policy für Azure OpenAI Services, ISO 27001, SOC 2.

(4) Sofern Unterauftragnehmer technisch Zugriffsmöglichkeiten auf Datenverarbeitungssysteme haben (z. B. Hosting, Managed Services), stellt der Auftragsverarbeiter durch technische Gestaltung, organisatorische Kontrollen und vertragliche Verpflichtungen sicher, dass eine Kenntnisnahme geschützter Inhalte ausgeschlossen ist.

(5) Unterauftragnehmer in Drittländern oder mit Drittlandzugriffen werden nur eingesetzt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Auch in solchen Konstellationen muss Zero-Access gewahrt bleiben. Derzeit findet kein Drittlandtransfer von Inhaltsdaten statt (vgl. VVT 1.1, Abschnitt 4).

§ 6 Support, Wartung und Ausnahmefälle

(1) Support und Wartung erfolgen grundsätzlich ohne Zugriff auf geschützte Inhalte. Der Auftragsverarbeiter verwendet hierfür vorrangig Metadaten und technische Diagnosen ohne Inhaltsbezug.

(2) Supportanfragen sind ohne Patienten- oder Fallinhalte zu stellen. Für die Fehleranalyse werden ausschließlich technische Angaben sowie anonymisierte oder synthetische Beispiele verwendet.

(3) Der Auftragsverarbeiter hält keinen „Break-Glass“-Zugriff zur Entschlüsselung oder Einsichtnahme in geschützte Inhalte vor.

§ 7 Protokollierung, Logs und Betriebsdaten

(1) Der Auftragsverarbeiter verarbeitet Betriebs- und Sicherheitsprotokolle ausschließlich in dem Umfang, der für den sicheren Betrieb, die Missbrauchsabwehr und die Fehleranalyse erforderlich ist. Protokolle enthalten **keine geschützten Inhalte** (keine Sitzungstexte, Prompts, Diagnosen oder Befunde).

(2) Sofern IP-Adressen oder vergleichbare technische Kennungen verarbeitet werden, werden diese nach Maßgabe der Datenschutzerklärung Plattform (DSE Plattform/App 1.2) und des Löschkonzepts (TOM 1.2, Abschnitt 4) gelöscht oder anonymisiert.

(3) Sicherheitsereignisprotokolle (Security-Logs) werden getrennt von Zugriffslogs geführt. Der Zugriff ist strikt auf die Geschäftsführung und den technischen Betrieb beschränkt.

§ 8 Sicherheitsvorfälle und behördliche Anfragen

- (1) Bei Verletzungen des Schutzes personenbezogener Daten unterstützt der Auftragsverarbeiter den Verantwortlichen gemäß AVV 1.2, § 11 und Art. 33/34 DSGVO. Der Auftragsverarbeiter achtet dabei darauf, dass keine geschützten Inhalte offenbart werden.
- (2) Aufgrund der Null-Speicher-Architektur ist das Schadenpotenzial bei einem hypothetischen Sicherheitsvorfall zeitlich und inhaltlich eng begrenzt. Es existiert kein Angriffsziel in Form dauerhaft gespeicherter Gesundheitsdaten (vgl. TOM 1.2, Abschnitt 9).
- (3) Erhält der Auftragsverarbeiter behördliche oder gerichtliche Anfragen, die auf die Herausgabe von Informationen gerichtet sind, informiert er den Verantwortlichen unverzüglich, soweit rechtlich zulässig, und unterstützt ihn bei der Wahrung der Berufsgeheimnisse.

§ 9 Nachweise und Audit

- (1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage geeignete Informationen zur Verfügung, um die Einhaltung dieser §203-Anlage nachzuweisen. Dies umfasst insbesondere ein Architektur-Statement zum Zero-Access- und Zero-Retention-Prinzip, die aktuelle Unterauftragsverarbeiterliste (Anlage 2 zum AVV 1.2) , einen Auszug der technisch-organisatorischen Maßnahmen (TOM 1.2) sowie Schulungsnachweise.
- (2) Auditrechte richten sich nach AVV 1.2 § 12. Prüfungen sind so durchzuführen, dass keine geschützten Inhalte offengelegt werden.

§ 10 Schlussbestimmungen

- (1) Diese §203-Anlage gilt für die Dauer des AVV 1.2 Sie tritt mit Abschluss des Nutzungsvertrags in Kraft und endet mit dessen Beendigung. Die Verpflichtungen zur Geheimhaltung und zum Schutz der Berufsgeheimnisse bestehen über das Vertragsende hinaus fort.
- (2) Änderungen und Ergänzungen bedürfen der Textform. Die Zustimmung kann elektronisch erfolgen.
- (3) Sollte eine Bestimmung dieser §203-Anlage unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame ersetzen, die dem Zweck am nächsten kommt.
- (4) Es gilt das Recht der Bundesrepublik Deutschland.

Unterschriften

Die Zustimmung kann auch elektronisch (digitale Bestätigung bei Vertragsschluss) erfolgen.

Ort, Datum: _____

[Verantwortlicher / Berufsgeheimnisträger]

[Auftragsverarbeiter]

Versionierung

Version	Datum	Änderung	Verantwortlich
1.0	31.07.2026	Erstfassung, konsolidiert auf AVV 1.0, TOM 1.0, Governance 1.	Peter Wolfgang Rieger-Stemmer
1.1	08.09.2026	Anpassung an Governance 1.1	Peter Wolfgang Rieger-Stemmer
1.2	02.11.2026	Abgleich mit AVV 1.2 und TOM 1.2; Aktualisierung der Dokumentverweise und Unterauftragnehmerliste; Klarstellung der Fortgeltung der Geheimhaltungspflichten nach Vertragsende	Peter Wolfgang Rieger-Stemmer

Ellie Worx UG (haftungsbeschränkt) · Heinrich-Weißmann-Str.18, 88048 Friedrichshafen · HRB 751433
Registergericht Ulm. Aufsichtsbehörde: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg (LfDI BaWü)