

TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

gemäß Art. 32 DSGVO

TOM 1.2 – Anlage zur 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:	Governance 1.1 / DSFA 1.1 / AVV 1.2
Nächste Prüfung:	12 Monate nach Erstfassung

1 Grundarchitektur und Datenschutzprinzip

Ellie Worx ist als temporäres, sessionbasiertes KI-Assistenzsystem konzipiert. Die gesamte Architektur folgt dem Grundsatz: Verarbeiten. Unterstützen. Löschen.

Die nachfolgenden Maßnahmen orientieren sich an Art. 32 DSGVO und sind risikoorientiert auf die Null-Speicher-Architektur zugeschnitten.

Prinzip	Umsetzung
Keine dauerhafte Speicherung	Keine Fallhistorie, keine Textdatenbank, keine textbasierten Backups
Keine Trainingsnutzung	Eingaben werden nicht für KI-Training oder Modelloptimierung verwendet
Keine Profilbildung	Keine Nutzerprofile auf Basis von Sitzungsinhalten
Keine Archivierung	Keine Wiederherstellungsfunktion für Sitzungsinhalte
Datenminimierung	Art. 5 Abs. 1 lit. c DSGVO – systemisch umgesetzt
Privacy by Design	Art. 25 DSGVO – tragendes Architekturprinzip, kein nachträgliches Feature

2 Vertraulichkeit

2.1 Zutrittskontrolle (Infrastruktur)

Maßnahme	Beschreibung
Rechenzentrumsschutz	Hosting in zertifizierten Azure-Rechenzentren (ISO 27001, SOC 2)
Physischer Zutritt	Ausschließlich für autorisiertes Personal von Microsoft; Videoüberwachung, Zutrittsprotokollierung
Standort	EU-Rechenzentren (Deutschland, Schweden, EU)

2.2 Zugangskontrolle (Systemebene)

Maßnahme	Beschreibung
Authentifizierung	Multi-Faktor-Authentifizierung (MFA) für alle Admin-Zugänge
Berechtigungskonzept	Rollenbasierte Zugriffskontrolle (RBAC); Zugriff auf Administrationssysteme ausschließlich für autorisierte Personen
Session-Management d	Automatisches Logout nach Inaktivität (Timeout)
Passwortrichtlinie	Min. 12 Zeichen, Komplexität erforderlich für alle Admin-Zugänge
Brute-Force-Schutz	Rate-Limiting und Account-Sperrung bei wiederholten Fehlversuchen
Zugriffsprüfung	Regelmäßige Überprüfung der Zugriffsrechte

2.3 Zugriffskontrolle (Datenebene)

Maßnahme	Beschreibung
Datenverschlüsselung (at rest)	AES-256 für gespeicherte Account- und Abrechnungsdaten
Keine Klartext-Zugriffe	Kein Zugriff durch Mitarbeiter auf Sitzungsinhalte – diese existieren nicht persistent
Zugriffsprotokollierung	Logging aller administrativen Systemzugriffe (ohne Inhaltsdaten)

2.4 Transportverschlüsselung

Maßnahme	Beschreibung
TLS	TLS 1.2 oder höher für alle Datenübertragungen

HTTPS	HTTPS-only; kein unverschlüsselter HTTP-Verkehr
HSTS	HTTP Strict Transport Security aktiviert
Zertifikate	Zertifikatsüberwachung und automatische Erneuerung

2.5 Vertraulichkeitsverpflichtung

Alle Mitarbeitenden und ggf. beauftragte Dritte werden auf Vertraulichkeit verpflichtet. Die Verpflichtung umfasst das Datengeheimnis und besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

3 Integrität

3.1 Eingabekontrolle

Maßnahme	Beschreibung
Account-Änderungen	Logging aller Änderungen an Account-Daten (wer, wann, was)
Keine Inhaltslogs	Keine textbasierten Debug- oder Systemlogs mit Sitzungsinhalten
Trennung	Strikte Trennung zwischen Systemlogs und Inhaltsverarbeitung

3.2 Systemintegrität

Maßnahme	Beschreibung
Deployment	Versionierte Deployments mit dokumentiertem Release-Prozess
Pre-Submit-Check	Validierung der Systemkonfiguration vor Produktivsetzung
Konfigurationsprüfung	Dokumentierte Prüfung von Logging- und Persistenzeinstellungen
Netzwerksicherheit	Netzwerksegmentierung, Firewall-Regelwerke, Härtung der Serverumgebung

4 Speicherbegrenzung und Löschkonzept

4.1 Verarbeitungsmodell

Die Verarbeitung der vom Auftraggeber eingegebenen Inhalte erfolgt ausschließlich während der aktiven Nutzungssitzung. Es existiert keine Datenbank mit Textinhalten, keine Archivierung und keine temporäre Sicherung zur Wiederherstellung.

4.2 Löschmechanismus

Ereignis	Maßnahme
Session-Ende	Automatische Löschung aller Sitzungsinhalte
Inaktivitäts-Timeout	Automatischer Session-Timeout mit Löschung (technisch noch nicht umgesetzt)
Verbindungsabbruch	Keine serverseitige Zwischenspeicherung; nicht lokal gesicherte Inhalte werden verworfen. Eine technisch unvermeidbare kurzzeitige Verarbeitung im Arbeitsspeicher (RAM) während der aktiven Anfrage stellt keine dauerhafte Speicherung dar.
Kein Auto-Save	Keine automatische serverseitige Sicherung von Eingaben

4.3 Löschfristen nach Datenkategorie

Datenkategorie	Speicherdauer	Löschung
Sitzungsinhalte (Text/Sprache)	Nur während aktiver Sitzung	Automatisch bei Session-Ende
Account-Daten (E-Mail, Login)	Vertragsdauer	Nach Vertragsende oder 180 Tage bei Inaktivität
Zahlungsdaten	Vertragsdauer	Via Stripe; nach Vertragsende + steuerl. Aufbewahrung
Systemlogs (ohne Inhalte)	Max. 90 Tage	Automatische Rotation

5 Verfügbarkeit und Belastbarkeit

Maßnahme	Beschreibung
Redundanz	Betrieb auf redundanter Cloud-Infrastruktur (Azure)
SLA	Azure SLA: 99,9 % Verfügbarkeit
Monitoring	24/7-Monitoring der Systemverfügbarkeit mit Alerting
DDoS-Schutz	DDoS-Schutz durch Azure-Infrastruktur
Updates	Regelmäßige Sicherheitsupdates und Patching
Umgebungstrennung	Getrennte Test- und Produktionsumgebung
Wiederherstellung	Disaster Recovery Plan mit RTO < 24h für Systeminfrastruktur. Hinweis: Da keine Inhaltsdaten dauerhaft gespeichert werden, besteht keine Verpflichtung zur Wiederherstellung von Nutzdaten.

6 Trennungskontrolle

Maßnahme	Beschreibung
Mandantentrennung	Getrennte Session-Instanzen pro Nutzer:in
Keine Zusammenführung	Keine mandantenübergreifende Zusammenführung oder Auswertung von Nutzungsinhalten
Keine Profilbildung	Keine Nutzerprofile auf Basis von Sitzungsinhalten
Keine Verknüpfung	Keine systematische Verknüpfung von Sitzungen
Datenisolation	Getrennte Datenbanken oder strikte Isolation auf Datenebene; keine gemeinsame Nutzung von Verschlüsselungsschlüsseln

7 Weitergabekontrolle

Maßnahme	Beschreibung
Verschlüsselte Übertragung	Alle Datenübertragungen über TLS 1.2/1.3
Keine Weitergabe an Dritte	Außer an genehmigte Unterauftragsverarbeiter (Microsoft Azure)
Subunternehmer-Bindung	Microsoft Azure vertraglich als Auftragsverarbeiter gebunden (Microsoft Data Processing Agreement)
Kein Datenexport	Es erfolgt keine planmäßige Übermittlung in Drittländer außerhalb der EU/des EWR. Eine Verarbeitung erfolgt ausschließlich über EU-basierte Azure-Regionen gemäß vertraglicher Zusicherung.

8 Auftragskontrolle

Maßnahme	Beschreibung
AVV	Abschluss eines AVV mit allen Nutzer:innen gemäß Art. 28 DSGVO
Datenminimierung	Hinweis zur Datenminimierung und Aufklärung im Onboarding
Berufsgruppenbeschränkung	Nutzung ausschließlich für approbierte Psychotherapeut:innen und PiA
Weisungsdokumentation	Dokumentation aller datenschutzrelevanten Weisungen
Subunternehmer-Kontrolle	Dokumentierte Auswahl und Kontrolle von Unterauftragsverarbeitern; ausschließlich mit EU-Datenverarbeitung

9 Incident-Response und Meldeprozess

Schritt	Beschreibung
1. Identifikation	Dokumentierter Prozess zur Identifikation von Sicherheitsvorfällen
2. Bewertung	Bewertung von Vorfällen binnen 24 Stunden
3. Meldung	Betroffene Praxen werden unverzüglich nach Bekanntwerden einer Datenschutzverletzung informiert
4. Dokumentation	Interne Dokumentation aller Sicherheitsereignisse (ohne Inhaltsdaten)
5. Nachbereitung	Analyse der Ursachen und Ableitung von Maßnahmen zur Verhinderung künftiger Vorfälle

Besonderheit der Null-Speicher-Architektur: Da keine Inhaltsdaten dauerhaft gespeichert werden, ist das Schadenpotenzial bei einem hypothetischen Sicherheitsvorfall zeitlich und inhaltlich eng begrenzt. Es existiert kein Angriffsziel in Form gespeicherter Gesundheitsdaten.

10 Datenschutz-Managementsystem

Maßnahme	Beschreibung
Datenschutzverantwortlicher	Benannter Datenschutzverantwortlicher (Peter Wolfgang Rieger-Stemmer, Geschäftsführer)
Mitarbeiterschulung	- keine Mitarbeiter -
DSFA	Datenschutz-Folgenabschätzung 1.1 dokumentiert und jährlich überprüft
TOM-Überprüfung	Regelmäßige Überprüfung und Aktualisierung der TOM, insbesondere bei Systemänderungen
Release-Prüfung	Technischer Pre-Submit-Check vor größeren Releases
Konfigurationsprüfung	Überprüfung von Logging- und Persistenzeinstellungen

11 Skalierungsfähigkeit

Die vorstehenden Maßnahmen sind unabhängig von der Nutzeranzahl wirksam, nicht speicherbasiert und architekturgebunden. Die Architekturprinzipien bleiben bei steigender

Nutzerzahl bestehen. Risiken und Schutzmaßnahmen werden bei wesentlichen Änderungen überprüft.

Organisatorische Anpassungen bei Skalierung umfassen:

- a) Formalisierung interner Rollen und Verantwortlichkeiten
- b) Dokumentierte Security-Reviews
- c) Erweiterte Monitoring-Prozesse
- d) Ggf. Bestellung eines externen Datenschutzbeauftragten bei Erreichen der gesetzlichen Schwellenwerte

12 Reaktion auf Vorfälle (Incident Response)

Im Falle einer Sicherheitsverletzung (Incident) greift ein strukturierter Notfallprozess unter direkter Leitung der Geschäftsführung.

1. **Eindämmung:** Bei Verdacht auf unbefugten Zugriff wird der Dienst unmittelbar in den Wartungsmodus versetzt und betroffene API-Schnittstellen isoliert.
2. **Analyse:** Aufgrund der Null-Speicher-Architektur (keine Inhaltsdatenbank) beschränkt sich die Analyse primär auf den Schutz von Nutzer-Accounts (Login-Daten). Eine dauerhafte Inhaltsdatenbank besteht nicht. Bei der Vorfallanalyse wird dennoch geprüft, ob Fallinhalte während der laufenden Verarbeitung betroffen waren.
3. **Behebung:** Identifizierte Sicherheitslücken werden umgehend geschlossen (z. B. durch Rotation von API-Keys oder Patching).
4. **Meldung:** Eine Information der Nutzer (Auftraggeber) sowie ggf. der Aufsichtsbehörde erfolgt innerhalb von 72 Stunden, sofern ein Risiko für die Rechte und Freiheiten der Nutzer besteht (Art. 33, 34 DSGVO).
5. **Dokumentation:** Jeder Vorfall wird intern protokolliert, um die Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO zu erfüllen.

Versionierung und Prüfzyklus

Version	Datum	Änderung	Verantwortlich
1.0	31.07.2026	Erstfassung, konsolidiert auf Governance 1.0, DSFA 1.0 und AVV 1.0	Peter Wolfgang Rieger-Stemmer
1.1	08.09.2026	Anpassung Governance 1.1; Löschung Gatekeeper, Empfehlung Prinzip der Datenminimierung	Peter Wolfgang Rieger-Stemmer
1.2	02.11.2026	Anpassung an AGB 1.2	Peter Wolfgang Rieger-Stemmer

Die TOM werden jährlich überprüft und bei wesentlichen Änderungen der Systemarchitektur oder Verarbeitung aktualisiert

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)