Dieses Dokument als PDF speichern: Browser-Druckdialog → “Als PDF speichern”

Drucken / Als PDF speichern

MedklarAI

KI-GESTÜTZTE PATIENTENAUFKLÄRUNG

Dokument: AVV-2025-v1.0
Stand: Januar 2025
Vertraulich

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 der Verordnung (EU) 2016/679 (DSGVO)

VERTRAGSPARTEIEN

Verantwortlicher (Auftraggeber)

[PRAXISNAME / EINRICHTUNGSNAME]
[STRASSE, HAUSNUMMER]
[PLZ ORT]
vertreten durch: *[NAME, TITEL]*

Auftragsverarbeiter

MedklarAI (Stevan Ursulovic)
[ADRESSE AUFTRAGSVERARBEITER]
E-Mail: datenschutz@medklarai.com

§ 1 Gegenstand und Dauer der Verarbeitung

Dieser Vertrag regelt die Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters im Rahmen der Nutzung der SaaS-Plattform MedklarAI zur KI-gestützten Patientenaufklärung.

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen im Sinne von Art. 28 DSGVO.

Die Laufzeit dieses Vertrages entspricht der Laufzeit des zugrundeliegenden Hauptvertrages (Nutzungsvertrag / SaaS-Abonnement). Der Vertrag endet mit Kündigung des Hauptvertrages, sofern keine gesonderte Vereinbarung getroffen wurde.

§ 2 Art und Zweck der Verarbeitung

Art der Verarbeitung: Erhebung, Speicherung, Verarbeitung und Anzeige personenbezogener Daten im Rahmen der Nutzung der MedklarAI-Plattform.

Zweck der Verarbeitung:

- Bereitstellung von KI-generierten, individualisierten Patienteninformationen und Aufklärungsunterlagen
- Verwaltung von Patientenanfragen innerhalb der Praxissoftware-Integration

Dieses Dokument als PDF speichern: Browser-Druckdialog → “Als PDF speichern”

§ 3 Art der personenbezogenen Daten / Kategorien betroffener Personen

Kategorien personenbezogener Daten:

- Stammdaten (Name, Geburtsdatum, Geschlecht)
- Kontaktdaten (Adresse, Telefon, E-Mail)
- Gesundheitsdaten gemäß Art. 9 DSGVO (Diagnosen, Symptome, Anamnese, Medikation)
- Nutzungsdaten der Plattform (Log-Daten, Session-Informationen)

Kategorien betroffener Personen:

- Patienten der Arztpraxis / medizinischen Einrichtung des Verantwortlichen
- Mitarbeiter des Verantwortlichen (soweit deren Daten verarbeitet werden)

§ 4 Pflichten und Rechte des Verantwortlichen

1. Der Verantwortliche ist allein verantwortlich für die Rechtmäßigkeit der Datenverarbeitung im Verhältnis zu den betroffenen Personen.
2. Der Verantwortliche ist berechtigt, dem Auftragsverarbeiter jederzeit Weisungen zu erteilen. Weisungen sind grundsätzlich schriftlich zu erteilen.
3. Der Verantwortliche stellt sicher, dass die betroffenen Personen über die Verarbeitung ihrer Daten informiert wurden.
4. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, sofern er Fehler in den Ergebnissen der Verarbeitung feststellt.
5. Vor Beginn der Verarbeitung und danach regelmäßig hat der Verantwortliche die beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren und zu dokumentieren.

§ 5 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist durch das Unionsrecht oder das Recht der Mitgliedstaaten zur Verarbeitung verpflichtet.
2. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten gemäß Art. 32–36 DSGVO.
5. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.
6. Der Auftragsverarbeiter benennt einen Ansprechpartner für Datenschutzangelegenheiten: datenschutz@medklarai.com
7. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass eine erteilte Weisung gegen die DSGVO oder sonstige Datenschutzvorschriften verstößt.

§ 6 Unterauftragnehmer

Der Auftragsverarbeiter ist berechtigt, Unterauftragnehmer einzusetzen. Die Einschaltung von Unterauftragnehmern ist dem Verantwortlichen vorab mitzuteilen. Der Verantwortliche kann gegen den Einsatz eines neuen Unterauftragnehmers Einspruch erheben.

Derzeit eingesetzte Unterauftragnehmer:

- **Vercel Inc.** (USA) — Hosting und Bereitstellung der Webanwendung; Grundlage: Standardvertragsklauseln (SCC) gem. Art. 46 Abs. 2 lit. c DSGVO
- **OpenAI OpCo LLC** (USA) — KI-Sprachmodell-Dienste; Grundlage: Standardvertragsklauseln (SCC) gem. Art. 46 Abs. 2 lit. c DSGVO

Der Auftragsverarbeiter verpflichtet Unterauftragnehmer vertraglich zu gleichwertigen Datenschutzpflichten wie in diesem Vertrag festgelegt.

§ 7 Betroffenenrechte

Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflicht, Anträge auf Wahrnehmung der Betroffenenrechte zu beantworten (Art. 12–22 DSGVO):

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Dieses Dokument als PDF speichern: Browser-Druckdialog → “Als PDF speichern”

Wenden sich betroffene Personen direkt an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter.

§ 8 Löschung und Rückgabe

Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter alle personenbezogenen Daten, die im Auftrag des Verantwortlichen verarbeitet wurden, oder gibt diese an den Verantwortlichen zurück — nach dessen Wahl — und löscht vorhandene Kopien, sofern nicht eine Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten die Speicherung vorschreibt.

Der Auftragsverarbeiter bestätigt die vollständige Löschung auf Verlangen schriftlich.

Die Löschfrist beträgt maximal **30 Tage** nach Vertragsbeendigung.

§ 9 Kontrollrechte

Der Verantwortliche hat das Recht, die Einhaltung der Datenschutzvorschriften und der vertraglichen Vereinbarungen beim Auftragsverarbeiter zu überprüfen.

1. Audits sind mit einer Vorankündigungsfrist von mindestens 14 Tagen anzukündigen und während üblicher Geschäftszeiten durchzuführen.
2. Der Auftragsverarbeiter kann als gleichwertigen Nachweis aktuelle Zertifizierungen (z. B. ISO 27001) oder Auditberichte vorlegen.
3. Dem Verantwortlichen entstehen durch ein Audit keine Kosten beim Auftragsverarbeiter, sofern der Aufwand einen halben Arbeitstag nicht überschreitet.

§ 10 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter hat folgende technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO getroffen:

Maßnahme	Umsetzung
Zutrittskontrolle	Ausschließlich cloudbasierter Betrieb; kein physischer Serverzugang. Rechenzentrumssicherheit durch Infrastrukturanbieter (Vercel / AWS).
Zugangskontrolle	Multi-Faktor-Authentifizierung (MFA) für alle Systemzugänge; automatische Sitzungsabmeldung nach Inaktivität.

Dieses Dokument als PDF speichern: Browser-Druckdialog → “Als PDF speichern”

	minimalen Berechtigung; regelmäßige Überprüfung der Zugriffsrechte.
Trennungskontrolle	Strikte logische Mandantentrennung; Praxisdaten werden isoliert verarbeitet und gespeichert.
Verschlüsselung	Transportverschlüsselung: TLS 1.2 / 1.3. Speicherverschlüsselung: AES-256 at rest.
Pseudonymisierung	Patientenbezogene Daten werden, soweit technisch möglich, pseudonymisiert verarbeitet.
Verfügbarkeitskontrolle	Redundante Infrastruktur, automatische Backups, Monitoring mit Alarmierung bei Ausfällen.
Belastbarkeit	Skalierbare Cloud-Architektur; regelmäßige Penetrationstests und Sicherheitsüberprüfungen.
Incident Response	Dokumentiertes Verfahren zur Erkennung, Meldung und Behebung von Datenschutzverletzungen; Meldung an Verantwortlichen innerhalb von 24 Stunden.
Mitarbeiterschulung	Regelmäßige Datenschutzschulungen für alle Mitarbeiter mit Datenzugang.

Dieses Dokument als PDF speichern: Browser-Druckdialog → “Als PDF speichern”

UNTERSCHRIFTEN

Durch ihre Unterschrift bestätigen die Vertragsparteien, diesen Auftragsverarbeitungsvertrag gelesen, verstanden und akzeptiert zu haben.

Ort, Datum *[ORT], [DATUM]*	Ort, Datum *Auftragsverarbeiter*
Unterschrift Verantwortlicher *[NAME, FUNKTION]* *[PRAXISNAME]*	Unterschrift Auftragsverarbeiter *Stevan Ursulovic* *MedklarAI*