AUFTRAGSVERARBEITUNGSVERTRAG (AVV) nach Art. 28 DSGVO

ratiomedicus GmbH

Stand: 6 November 2025
Version: 2.1 (Aktualisiert mit Abschnitt Kooperationspartner)

Vertragsparteien

Auftragsverarbeiter: ratiomedicus GmbH

Am Flughafen 12 - 60549 Frankfurt am Main - Handelsregister: HRB 138874, AG Frankfurt - Geschäftsführung: Niclas Ryberg, Martin Werner-Böhm - USt-ID: DE366563907 - E-Mail: office@ratiomedicus.de

(im Folgenden „Auftragsverarbeiter" oder „ratiomedicus")

Auftraggeber (Verantwortlicher):

(im Folgenden „Verantwortlicher" oder „Praxis")

§ 1 GEGENSTAND, DAUER UND WEISUNGSRECHT

1.1 Auftrag

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der:

- Abrechnungsberatung und -optimierung
- EBM- und GOÄ-Abrechnungsanalyse
- Plausibilitätsprüfungen nach ICD-10
- Identifikation von Optimierungspotenzialen
- Sonstigen in der Leistungsbeschreibung des Hauptvertrags genannten Dienstleistungen

Eine Verarbeitung für andere Zwecke erfolgt nicht ohne ausdrückliche schriftliche Zustimmung des Verantwortlichen.

1.2 Dauer

Der AV-Vertrag tritt mit Unterzeichnung in Kraft und gilt für die Dauer des Hauptvertrags zwischen ratiomedicus und dem Verantwortlichen. Nach Beendigung des Hauptvertrags endet dieser AV-Vertrag automatisch.

1.3 Weisungsrecht

Der Verantwortliche ist berechtigt, dem Auftragsverarbeiter Weisungen zur Verarbeitung personenbezogener Daten zu erteilen. Der Auftragsverarbeiter führt diese Weisungen unverzüglich durch. Sollten Weisungen gegen die DSGVO verstoßen, teilt der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich mit.

§ 2 VERARBEITETE DATENKATEGORIEN

Der Auftragsverarbeiter verarbeitet folgende Kategorien personenbezogener Daten:

- **Patientenstammdaten:** Name, Vorname, Geburtsdatum, Geschlecht, Versichertennummer, Kontaktdaten
- **Patientenmedizinische Daten:** Diagnosen (ICD-10), Verordnungen, Behandlungsdaten, Symptome

- **Abrechnungsdaten:** Gebührenordnungsziffern (GOÄ), EBM-Ziffern, Leistungsbeschreibungen, Abrechnungsbeträge
- **Finanzielle Daten:** Rechnungen, Zahlungsinformationen, Versicherungsdaten
- **Sonst. Daten:** Kommunikation mit dem Verantwortlichen, Vertragsunterlagen, Anfragen

Eine Verarbeitung zusätzlicher oder anderer Datenkategorien erfolgt nur nach schriftlicher Zustimmung des Verantwortlichen.

---

§ 3 Art DER VERARBEITUNG UND VERARBEITUNGSVORGÄNGE

3.1 Verarbeitungsvorgänge

Der Auftragsverarbeiter führt folgende Verarbeitungsvorgänge durch:

- **Speicherung:** Speicherung der Daten in verschlüsselten Datenbanken
- **Analyse:** Auswertung der Abrechnungsdaten zur Optimierung
- **Bearbeitung:** Bearbeitung der Daten gemäß den Weisungen des Verantwortlichen
- **Einsicht:** Gewährung von Einsicht in die Daten für berechtigte Personen des Verantwortlichen
- **Zugriff:** Remote-Zugriff auf die verarbeiteten Daten durch autorisierte Mitarbeitende
- **Berichte:** Erstellung von Berichten und Analysen

3.2 Häufigkeit und Umfang

Die Verarbeitung erfolgt laufend nach Maßgabe der Anforderungen des Verantwortlichen und der vertraglichen Verpflichtungen.

---

§ 4 SICHERHEITS- UND SCHUTZFORDERUNGEN

4.1 Technische Maßnahmen

Der Auftragsverarbeiter implementiert und unterhält folgende technische Maßnahmen:

- **Verschlüsselung:** Alle Daten werden bei der Übertragung (TLS) und in der Speicherung (AES-256) verschlüsselt

- **Zugriffsschutz:** Authentifizierung und Autorisierung durch Passwörter und Multi-Faktor-Authentifizierung
- **Malware-Schutz:** Einsatz von Antivirus-Software und Firewalls
- **Datensicherung:** Tägliche Backups mit Redundanz
- **Patch-Management:** Regelmäßige Sicherheitsupdates
- **Monitoring:** Kontinuierliche Überwachung der Systeme

4.2 Organisatorische Maßnahmen

Der Auftragsverarbeiter trifft folgende organisatorische Maßnahmen:

- **Zugriffskontrolle:** Nur autorisierte Personen haben Zugriff auf Daten
- **Schulung:** Regelmäßige Schulung der Mitarbeitenden zu Datenschutz
- **Vertraulichkeit:** Vertraulichkeitsverpflichtungen für alle Mitarbeitenden
- **Trennung:** Logische und physische Trennung von Daten verschiedener Verantwortlicher
- **Incident Response:** Dokumentiertes Verfahren für Sicherheitsvorfälle
- **Dokumentation:** Dokumentation aller Verarbeitungsvorgänge

4.3 Detaillierte TOM-Dokumentation

Die detaillierten technischen und organisatorischen Maßnahmen sind im separaten Dokument **„Technische und organisatorische Maßnahmen (TOM)“** dokumentiert, das Bestandteil dieses AV-Vertrags ist.

---

§ 5 UNTERAUFTRAGSVERARBEITER

5.1 Zulässigkeit und Genehmigung

Der Auftragsverarbeiter darf personenbezogene Daten nur an Unterauftragsverarbeiter weitergeben, die:

1. vom Auftragsverarbeiter selbst beauftragt werden
2. das gleiche Maß an Datenschutz gewährleisten
3. vorher schriftlich von dem Verantwortlichen genehmigt werden

5.2 Derzeitige Unterauftragsverarbeiter

Derzeit arbeitet der Auftragsverarbeiter mit folgenden Unterauftragsverarbeitern zusammen:

Unterauftragsverarbeiter	Verarbeitungsgegenstand	Standort	AV-Vertrag
Microsoft Ireland Operations Ltd	Cloud-Speicherung (Office 365, Dynamics 365)	Dublin, Irland	Ja
Hetzner Online GmbH	Server-Hosting	Gunzenhausen, Deutschland	Ja
abcomed GmbH	Analysesoftware	Königstein, Deutschland	Ja
DATEV eG	Buchhaltungsoftware	Nürnberg, Deutschland	Ja

5.3 Änderung von Unterauftragsverarbeitern

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen vor der Beauftragung neuer Unterauftragsverarbeiter schriftlich zu informieren. Der Verantwortlicher kann innerhalb von 14 Tagen Einwände erheben. Im Falle von berechtigten Einwänden wird eine Alternative gesucht.

§ 6 KOOPERATIONSPARTNER UND EXTERNE VERTRIEBSPARTNER

6.1 Rechtliche Einordnung

Die ratiomedicus GmbH arbeitet im Rahmen der Kundenakquisition und Vertriebsunterstützung mit externen Vertriebspartnern und Kooperationspartnern zusammen. Diese Partner sind **keine Unterauftragsverarbeiter im Sinne von Art. 28 DSGVO**, sondern **eigenverantwortliche Verantwortliche** gemäß Art. 4 Nr. 7 DSGVO.

6.2 Datenart und Umfang der Weitergabe

An externe Vertriebspartner werden ausschließlich folgende B2B-Kontaktdaten weitergegeben:

- Name der Arztpraxis/Klinik/MVZ
- Name und Position von Ansprechpartnern
- Geschäftliche E-Mail-Adressen
- Geschäftliche Telefonnummern
- Praxisanschrift

Ausdrücklich werden NICHT weitergegeben: - Patientendaten jeglicher Art - Gesundheitsdaten oder Diagnosen - Abrechnungsdaten - Finanzielle Daten - Zugangsdaten zu Systemen

6.3 Zweck der Datenweitergabe

Die Weitergabe von B2B-Kontaktdaten an externe Vertriebspartner erfolgt ausschließlich zum Zweck der:

- Kundenakquisition
- Vertriebskoordination
- Ermöglichung der Kontaktaufnahme durch den Vertriebspartner
- Durchführung von gemeinsamen Vertriebsprojekten

6.4 Verantwortlichkeit der Vertriebspartner

Die externen Vertriebspartner sind eigenverantwortlich dafür verpflichtet:

- Alle datenschutzrechtlichen Vorgaben (DSGVO, BDSG) einzuhalten
- Technische und organisatorische Maßnahmen zum Schutz der Daten zu implementieren
- Betroffenenrechte (Auskunft, Löschung, Berichtigung) eigenständig zu gewährleisten
- Bei Datenschutzverletzungen eigenständig die erforderlichen Meldungen vorzunehmen
- Nach Vertragsende die übermittelten Daten zu löschen

6.5 Informationspflicht

Der Auftragsverarbeiter teilt dem Verantwortlichen auf Anfrage mit, welche Vertriebspartner aktuell mit B2B-Kontaktdaten beliefert werden. Der Verantwortlicher kann berechtigte Einwände gegen einzelne Vertriebspartner vorbringen.

6.6 Zukünftige Erweiterung

Sollte in Zukunft eine Verarbeitung von Patientendaten oder sensiblen Daten durch Vertriebspartner erforderlich werden, wird vorab die schriftliche Zustimmung des Verantwortlichen eingeholt und dieser AV-Vertrag entsprechend ergänzt oder ein separater AV-Vertrag mit dem Vertriebspartner geschlossen.

§ 7 RECHTE DES VERANTWORTLICHEN

7.1 Auskunftsrecht

Der Verantwortliche hat das Recht, jederzeit Informationen über die Verarbeitung seiner Daten zu erhalten, insbesondere:

- Art und Umfang der Verarbeitung
- Eingesehene oder übermittelte Daten
- Beteiligte Mitarbeitende
- Sicherheitsmaßnahmen

Der Auftragsverarbeiter stellt diese Informationen innerhalb von 5 Arbeitstagen zur Verfügung.

7.2 Inspektions- und Audit-Recht

Der Verantwortlicher (oder ein von ihm beauftragter Dritter) hat das Recht:

- Die Verarbeitungsvorgänge zu inspizieren
- Audits durchzuführen
- Einsicht in Verarbeitungsdokumentationen zu nehmen
- Besichtigungen der Verarbeitungsorte durchzuführen

Der Auftragsverarbeiter gewährleistet diese Rechte nach vorheriger Ankündigung (mindestens 5 Arbeitstage). Die Inspektionen erfolgen während der Geschäftszeiten.

7.3 Weisungsrecht

Der Verantwortliche ist berechtigt, jederzeit Weisungen zur Verarbeitung personenbezogener Daten zu erteilen. Der Auftragsverarbeiter führt diese unverzüglich durch.

7.4 Recht auf Datenherausgabe

Der Verantwortlicher kann jederzeit verlangen, dass der Auftragsverarbeiter die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellt (Portabilität).

---

§ 8 PFLICHTEN DES AUFTRAGSVERARBEITERS

8.1 Geheimhaltungsverpflichtung

Der Auftragsverarbeiter und seine Mitarbeitenden sind verpflichtet:

- Strikte Geheimhaltung aller personenbezogenen Daten
- Verarbeitung der Daten nur nach Weisung des Verantwortlichen
- Keine Offenbarung von Daten an unbefugte Dritte
- Einhaltung dieser Verpflichtung auch nach Beendigung des Vertrags

8.2 Vertraulichkeitsverpflichtung

Der Auftragsverarbeiter gewährleistet, dass:

- Alle Mitarbeitenden schriftlich auf Vertraulichkeit verpflichtet sind
- Nur notwendige Mitarbeitende Zugriff auf Daten haben
- Eine Schulung zu Datenschutz durchgeführt wird
- Vertraulichkeitsverpflichtungen auch für externe Dienstleister gelten

8.3 Datensicherheit

Der Auftragsverarbeiter implementiert und unterhält angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO (siehe auch § 4 und separates TOM-Dokument).

8.4 Löschung und Rückgabe

Nach Beendigung dieses Vertrags stellt der Auftragsverarbeiter sicher, dass:

- Alle Daten gelöscht oder vollständig an den Verantwortlichen zurückgegeben werden
- Keine Kopien mehr vorliegen (außer soweit gesetzlich erforderlich)
- Bis zur Löschung die Geheimhaltung gewährleistet bleibt
- Die Löschung dokumentiert wird

Der Verantwortlicher entscheidet, ob Daten gelöscht oder zurückgegeben werden.

8.5 Unterstützung bei Betroffenenrechten

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Betroffenenrechten:

- Auskunftsersuchen
- Löschansprüche
- Berichtigungsersuchen
- Widerspruchsrechte

Der Auftragsverarbeiter stellt erforderliche Informationen innerhalb von 3 Arbeitstagen bereit.

8.6 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldest dem Verantwortlichen ohne schuldhaftes Zögern, spätestens aber innerhalb von 24 Stunden nach Kenntnisnahme, über:

- Datenschutzverletzungen
- Verdacht auf Datenschutzverletzungen
- Unbefugte Zugriffe oder Änderungen
- Verlust oder Beschädigung von Daten

Die Meldung enthält Informationen zur Art des Vorfalls, den betroffenen Daten und Personen sowie ergriffenen Maßnahmen.

§ 9 REGELMÄSSIGE ÜBERPRÜFUNG UND VERBESSERUNG

9.1 Überprüfungspflicht

Der Auftragsverarbeiter überprüft die Einhaltung dieser Vereinbarung regelmäßig:

- Mindestens einmal pro Jahr eine Selbstbewertung
- Quartalsweise Sicherheitsprüfungen
- Jährliche externe Audits durch unabhängige Dritte

9.2 Dokumentation

Der Auftragsverarbeiter dokumentiert:

- Alle Überprüfungen und Audit-Ergebnisse
- Identifizierte Sicherheitslücken
- Ergriffene Korrekturmaßnahmen
- Verbesserungen der Sicherheitsmaßnahmen

9.3 Berichterstattung

Der Auftragsverarbeiter berichtet dem Verantwortlichen:

- Jährlich über die Überprüfungsergebnisse
- Unverzüglich über wesentliche Sicherheitsmängel
- Unverzüglich über Datenschutzverletzungen

§ 10 HAFTUNG UND VERSICHERUNG

10.1 Haftung

Der Auftragsverarbeiter haftet für:

- Verletzungen seiner Pflichten aus diesem AV-Vertrag

- Verstöße gegen die DSGVO
- Schäden durch Datenschutzverletzungen
- Unbefugte Verarbeitung personenbezogener Daten

Die Haftung ist nicht beschränkt für:

- Verletzungen von Datenschutzrechten
- Verluste von Gesundheitsdaten
- Vorsätzliches oder fahrlässiges Verhalten

10.2 Versicherung

Der Auftragsverarbeiter unterhält eine angemessene Cyber- und Haftpflichtversicherung mit einer Mindestdeckungssumme von 1.000.000 EUR pro Schadensfall.

---

§ 11 SUBUNTERNEHMER UND WEITERE DIENSTLEISTER

11.1 Bekanntgabe

Der Auftragsverarbeiter teilt dem Verantwortlichen regelmäßig mit:

- Eine aktuelle Liste aller Unterauftragsverarbeiter
- Bei Änderungen: Benachrichtigung mindestens 14 Tage vor Beauftragung

11.2 Vertragliche Anforderungen

Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter:

- Die gleichen Datenschutzverpflichtungen erfüllen
- Auftragsverarbeitungsverträge nach Art. 28 DSGVO unterzeichnet haben
- Von der ständigen Aufsicht des Auftragsverarbeiters unterliegen

---

§ 12 DATENSCHUTZ-FOLGENABSCHÄTZUNG

12.1 Unterstützungspflicht

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei:

- Durchführung von Datenschutz-Folgenabschätzungen (DSFA) gemäß Art. 35 DSGVO
- Bereitstellung erforderlicher Informationen
- Bewertung von Sicherheitsmaßnahmen
- Dokumentation des Prozesses

---

§ 13 LAUFZEIT UND BEENDIGUNG

13.1 Laufzeit

Dieser AV-Vertrag gilt für die Dauer des Hauptvertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter.

13.2 Beendigung

Der AV-Vertrag beendet sich automatisch mit Beendigung des Hauptvertrags oder auf schriftliche Kündigung durch eine der Parteien.

13.3 Pflichten nach Beendigung

Nach Beendigung des Vertrags:

- Löschung aller Daten oder Rückgabe an den Verantwortlichen (auf Wunsch)
- Dokumentation der Löschung
- Geheimhaltung auch nach Vertragsende
- Herausgabe aller erforderlichen Dokumente und Berichte

---

§ 14 SCHLUSSBESTIMMUNGEN

14.1 Geltung und Vorrang

Dieser AV-Vertrag gilt ergänzend zu den Regelungen des Hauptvertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter.

Im Falle von Widersprüchen zwischen diesem AV-Vertrag und dem Hauptvertrag gelten die Bestimmungen des AV-Vertrags (da sie speziellere Regelungen zur DSGVO darstellen).

14.2 Salvatorische Klausel

Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleiben die übrigen Bestimmungen gültig. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.

14.3 Schriftformerfordernis

Änderungen dieses Vertrags müssen schriftlich erfolgen. Eine Aufhebung des Schriftformerfordernisses bedarf selbst der Schriftform.

14.4 Rechtliche Grundlagen

Dieser Vertrag beruht auf:

- Datenschutz-Grundverordnung (DSGVO), insbesondere Art. 28
- Bundesdatenschutzgesetz (BDSG)
- Deutsches Recht (BGB, HGB)

Anwendbar ist deutsches Recht. Gerichtsstand ist Frankfurt am Main.

14.5 Anlagen

Bestandteil dieses Vertrags sind folgende Anlagen: (die Dokumente können auf Wunsch eingesehen werden)

- **Anlage 1:** Technische und organisatorische Maßnahmen (TOM)
- **Anlage 2:** Verzeichnis von Verarbeitungstätigkeiten (VVT)
- **Anlage 3:** Datenschutzrichtlinie
- **Anlage 4:** Liste der Unterauftragsverarbeiter

---

§ 15 UNTERSCHRIFTEN

Für den Auftragsverarbeiter (ratiomedicus GmbH):

Für den Verantwortlichen (Praxis/Klinik/MVZ):

---

ratiomedicus GmbH
Am Flughafen 12
60549 Frankfurt/Main
+49 69 509 589 452
office@ratiomedicus.de

HRB 138874 | AG Frankfurt
Geschäftsführung
Niclas Ryberg
Martin Werner-Böhm

USt-ID: DE366563907
Deutsche Bank
IBAN: DE08 7207 0024 0057 993800
BIC: DEUTDEDB720