FLOWMATIX

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

Version 2.0 · Stand: April 2026

VERANTWORTLICHER

[Name der Klinik]
[Straße, Hausnummer]
[PLZ, Ort, Land]
vertreten durch: [Geschäftsführung / Inhaber]
— nachstehend „Verantwortlicher" —

AUFTRAGSVERARBEITER

Flowmatix – Automation
Inhaber: Bastian Barkowski
An der Moorbäke 6, 27798 Hude, Deutschland
E-Mail: legal@flowmatix.io
— nachstehend „Auftragsverarbeiter" —

Präambel

Der Verantwortliche nutzt die Dienstleistungen des Auftragsverarbeiters zur Automatisierung der Patientenkommunikation, Vorqualifizierung, Terminorganisation und KI-gestützten Vorbereitung von medizinischen Beurteilungen. Dabei werden personenbezogene Daten von Patienten und Interessenten des Verantwortlichen verarbeitet. Dieser Vertrag regelt die Pflichten der Parteien zum Datenschutz nach Art. 28 DSGVO und ersetzt alle vorherigen Vereinbarungen zur Auftragsverarbeitung.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung der Flowmatix CRM- und Automatisierungsplattform für den Verantwortlichen.

(2) Dauer

Der Vertrag beginnt mit Vertragsschluss und läuft auf unbestimmte Zeit. Er endet automatisch mit Beendigung des zugrundeliegenden Hauptvertrags oder kann von beiden Parteien mit einer Frist von vier Wochen schriftlich gekündigt werden. Eine außerordentliche Kündigung aus wichtigem Grund bleibt unberührt.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zu folgenden Zwecken:

- Digitale Patientenkommunikation über WhatsApp und vergleichbare Kanäle
- Vorqualifizierung von Patienten anhand von Anamnesedaten
- KI-gestützte Vorbereitung von Patientenakten zur ärztlichen Beurteilung (mittels Anthropic Claude API)
- Organisation von Beratungsterminen, OP-Terminen und Folgekontakten
- Versand von Erinnerungen, Aftercare-Nachrichten und Behandlungsplänen
- Verwaltung von Patientendokumenten, Fotos und medizinischen Angaben
- Bereitstellung von Statistiken und Reportings für den Verantwortlichen
- Technischer Support und Wartung der Plattform

Eine medizinische Diagnose oder Therapieempfehlung erfolgt durch den Auftragsverarbeiter ausdrücklich nicht. Die Letztverantwortung für medizinische Entscheidungen verbleibt beim Verantwortlichen und seinem ärztlichen Personal.

§ 3 Art der personenbezogenen Daten

Im Rahmen dieses Vertrags werden folgende Kategorien personenbezogener Daten verarbeitet:

- **Stammdaten:** Vor- und Nachname, Geschlecht, Alter / Geburtsdatum, Sprache, Land
- **Kontaktdaten:** Telefonnummer (WhatsApp), E-Mail-Adresse
- **Gesundheitsdaten (Art. 9 DSGVO):** Anamnese, Haarstatus, Vorerkrankungen, Medikation, Allergien, Vorbehandlungen, Raucherstatus, Blutverdünner, weitere medizinische Angaben
- **Bilddaten:** Patientenfotos (Front, Seite, Spenderbereich, Nahaufnahmen)
- **Termindaten:** Beratungs- und OP-Termine, Kalenderbuchungen
- **Kommunikationsinhalte:** WhatsApp-Nachrichten, Sprachnachrichten (transkribiert), Dokumente
- **Reisedaten:** Flugdaten (freiwillig vom Patienten übermittelt), Fahrer-/Hotelinfos
- **Einwilligungsnachweise:** DSGVO-Consent-Logs mit Zeitstempel

§ 4 Kategorien betroffener Personen

- Patienten und Interessenten des Verantwortlichen
- Mitarbeiter und ärztliches Personal des Verantwortlichen (in begrenztem Umfang, soweit für die Nutzung der Plattform erforderlich)

§ 5 Pflichten des Auftragsverarbeiters

(1) Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf Übermittlungen in Drittländer, sofern keine gesetzliche Verpflichtung besteht.

(2) Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Mitarbeiter werden regelmäßig zum Datenschutz geschult.

(3) Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft alle erforderlichen Maßnahmen nach Art. 32 DSGVO. Eine detaillierte Beschreibung der technischen und organisatorischen Maßnahmen findet sich in **Anlage 1**.

(4) Unterstützung

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit angemessenen technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen sowie bei der Einhaltung der Pflichten nach Art. 32–36 DSGVO (insbesondere Sicherheit, Meldung von Datenpannen und Datenschutz-Folgenabschätzungen).

§ 6 Sub-Auftragsverarbeiter

(1) Allgemeine Genehmigung

Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter („Sub-Auftragsverarbeiter") für die Erbringung der Dienstleistung einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Sub-Auftragsverarbeiter sind in **Anlage 2** aufgelistet.

(2) Änderungen

Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Sub-Auftragsverarbeitern mindestens 30 Tage im Voraus per

E-Mail an die hinterlegte Kontaktadresse. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichen Grund schriftlich widersprechen. Im Widerspruchsfall sind beide Parteien zur außerordentlichen Kündigung berechtigt.

(3) Pflichten der Sub-Auftragsverarbeiter

Der Auftragsverarbeiter verpflichtet jeden Sub-Auftragsverarbeiter vertraglich zu mindestens den gleichen Datenschutzpflichten, wie sie in diesem AVV festgelegt sind. Erfüllt ein Sub-Auftragsverarbeiter seine Datenschutzpflichten nicht, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Sub-Auftragsverarbeiters.

§ 7 Internationale Datenübermittlungen

Sofern personenbezogene Daten in Drittländer außerhalb des EWR übermittelt werden, stellt der Auftragsverarbeiter sicher, dass eine der folgenden Garantien nach Art. 44 ff. DSGVO vorliegt:

- Angemessenheitsbeschluss der EU-Kommission, oder
- EU-Standardvertragsklauseln (SCC) in der jeweils aktuellen Fassung (Durchführungsbeschluss (EU) 2021/914), ggf. ergänzt um zusätzliche Maßnahmen nach Schrems-II-Rechtsprechung, oder
- Verbindliche interne Datenschutzvorschriften (BCR), oder
- Eine ausdrückliche Einwilligung der betroffenen Person in die konkrete Datenübermittlung nach Art. 49 Abs. 1 lit. a DSGVO.

Eine konkrete Auflistung aller Drittlandtransfers und ihrer rechtlichen Grundlagen findet sich in **Anlage 2**.

§ 8 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Kenntnisnahme, über jede Verletzung des Schutzes personenbezogener Daten (Art. 33 DSGVO). Die Meldung enthält mindestens:

- Beschreibung der Art der Verletzung (Kategorien und ungefähre Anzahl betroffener Personen und Datensätze)
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen oder geplanten Abhilfemaßnahmen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Meldepflichten gegenüber der Aufsichtsbehörde und ggf. den betroffenen Personen.

§ 9 Rechte der betroffenen Personen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Wahrnehmung der Rechte betroffener Personen nach Art. 12–22 DSGVO, insbesondere:

- **Recht auf Auskunft (Art. 15):** Die Plattform stellt eine Export-Funktion bereit (JSON-Format), mit der alle gespeicherten Patientendaten heruntergeladen werden können.
- **Recht auf Berichtigung (Art. 16):** Stammdaten und Patientenakten können vom Verantwortlichen jederzeit aktualisiert werden.
- **Recht auf Löschung (Art. 17):** Die Plattform bietet eine vollständige Löschfunktion („Hard Delete"), die alle personenbezogenen Daten irreversibel entfernt.
- **Recht auf Einschränkung (Art. 18):** Der Verantwortliche kann Patientenakten in einen Read-Only-Status versetzen.
- **Recht auf Datenübertragbarkeit (Art. 20):** Die Export-Funktion liefert Daten in einem strukturierten, gängigen und maschinenlesbaren Format (JSON).
- **Widerspruchsrecht (Art. 21):** Der Verantwortliche kann die automatisierte Verarbeitung jederzeit deaktivieren.

§ 10 Audit-Rechte des Verantwortlichen

Der Verantwortliche hat das Recht, die Einhaltung der Pflichten dieses Vertrags durch den Auftragsverarbeiter zu kontrollieren. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung zur Verfügung.

Audits können nach vorheriger Ankündigung mit einer Frist von vier Wochen vor Ort oder remote durchgeführt werden, höchstens einmal pro Kalenderjahr und maximal an einem Werktag, sofern keine konkreten Anhaltspunkte für eine Datenschutzverletzung vorliegen. Der Auftragsverarbeiter kann anstelle eines Vor-Ort-Audits den aktuellen Bericht eines unabhängigen Prüfers (z.B. ISO 27001, SOC 2, BSI C5) vorlegen.

§ 11 Aufbewahrung und Löschung

Der Auftragsverarbeiter speichert personenbezogene Daten nur so lange, wie es für die Erbringung der vereinbarten Leistungen erforderlich ist oder gesetzliche Aufbewahrungspflichten bestehen. Die Plattform implementiert einen automatisierten Retention-Scanner, der Patientendaten nach Ablauf der konfigurierbaren Aufbewahrungsfrist (Standard: 10 Jahre gemäß § 630f BGB) anonymisiert.

Nach Beendigung des Vertrags löscht oder anonymisiert der Auftragsverarbeiter alle personenbezogenen Daten innerhalb von **30 Tagen**, sofern der Verantwortliche nicht ausdrücklich die Rückgabe in einem strukturierten Format verlangt. Die Löschung wird auf Anfrage schriftlich bestätigt.

§ 12 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Der Auftragsverarbeiter haftet nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Eine Haftung des Auftragsverarbeiters für medizinische Entscheidungen, Behandlungsmaßnahmen oder Therapieempfehlungen ist ausgeschlossen. Diese liegen ausschließlich im Verantwortungsbereich des Verantwortlichen.

§ 13 Datenschutzbeauftragter

Der Datenschutzbeauftragte des Auftragsverarbeiters ist erreichbar unter: **privacy@flowmatix.io**. Der Verantwortliche teilt dem Auftragsverarbeiter Name und Kontaktdaten seines Datenschutzbeauftragten (falls bestellt) unverzüglich mit.

§ 14 Anwendbares Recht und Gerichtsstand

Auf diesen Vertrag findet ausschließlich deutsches Recht unter Ausschluss des UN-Kaufrechts Anwendung. Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Hude (bzw. das nächstgelegene zuständige Gericht in Deutschland), sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

§ 15 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so wird die Wirksamkeit des Vertrags im Übrigen nicht berührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame Bestimmung ersetzen, die dem wirtschaftlichen und rechtlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieser Schriftformklausel.

(3) Im Falle eines Widerspruchs zwischen diesem AVV und Regelungen aus dem Hauptvertrag gehen die Bestimmungen dieses AVV vor.

VERANTWORTLICHER	AUFTRAGSVERARBEITER
[Name]	**Bastian Barkowski · Flowmatix**
Ort, Datum, Unterschrift	Hude, _____, _____

Anlage 1 — Technische und organisatorische Maßnahmen (TOM)

Diese Anlage beschreibt die nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung eines dem Risiko angemessenen Schutzniveaus.

1. Vertraulichkeit

Maßnahme	Umsetzung
Zutrittskontrolle	Server in zertifizierten Rechenzentren (Hetzner Online GmbH, Falkenstein/Nürnberg, Deutschland) — ISO 27001-zertifiziert. Physischer Zugang nur für autorisiertes Personal mit Zwei-Faktor-Authentifizierung.
Zugangskontrolle	Multi-Faktor-Authentifizierung (TOTP) für alle Plattform-Konten. Sitzungs-Cookies mit Refresh-Token-Rotation. Bcrypt-Passwort-Hashing (Cost-Faktor 12).
Zugriffskontrolle	Rollenbasierte Zugriffssteuerung (RBAC) mit 6 Rollen (admin, coordinator, doctor, finance, platform_owner, staff). Row-Level Security (RLS) auf Datenbankebene erzwingt Mandantentrennung. Jeder Mitarbeiter sieht nur Daten seiner Klinik.
Trennungskontrolle	Multi-Tenant-Architektur mit strikter Trennung pro Klinik (organization_id) auf allen Ebenen. PostgreSQL Row-Level Security verhindert Cross-Tenant-Zugriffe auch bei Anwendungsfehlern.
Pseudonymisierung	Sensible Felder (z.B. Anamnese-Daten) werden verschlüsselt gespeichert. Audit-Logs enthalten User-IDs statt Namen.

2. Integrität

Maßnahme	Umsetzung
Weitergabekontrolle	Transportverschlüsselung (TLS 1.3) für alle externen Verbindungen. WhatsApp-Kommunikation Ende-zu-Ende-verschlüsselt durch das WhatsApp-Protokoll.
Eingabekontrolle	Vollständiges Audit-Log aller Datenzugriffe und -änderungen mit Zeitstempel, User-ID, IP-Adresse und User-Agent. Lesezugriffe auf Patientenakten werden gemäß Art. 30 DSGVO protokolliert.
Verschlüsselung at rest	Datenbank-Backups mit AES-256 verschlüsselt. Sensible Felder zusätzlich auf Anwendungsebene verschlüsselt (Application-Layer Encryption).

3. Verfügbarkeit und Belastbarkeit

Maßnahme	Umsetzung
Verfügbarkeitskontrolle	Tägliche, wöchentliche und monatliche automatische Backups mit Off-Site-Replikation. Monitoring 24/7 mit Alerting (Grafana, Prometheus, Loki, Uptime Kuma). Geografisch redundante DNS.
Wiederherstellbarkeit	Recovery Time Objective (RTO): 4 Stunden. Recovery Point Objective (RPO): 24 Stunden. Disaster-Recovery-Plan dokumentiert und jährlich getestet.
Resilienz	Circuit Breaker für externe APIs, automatische Failover für Datenbank-Verbindungen, Redis-Persistierung mit AOF + RDB.

4. Verfahren zur regelmäßigen Überprüfung

Maßnahme	Umsetzung
Datenschutz-Management	Datenschutzbeauftragter benannt (privacy@flowmatix.io). Verfahrensverzeichnis nach Art. 30 DSGVO geführt. Datenschutz-Folgenabschätzung (DPIA) für die Verarbeitung von Gesundheitsdaten dokumentiert.
Incident-Response-Management	Dokumentierter Prozess zur Erkennung, Meldung und Behandlung von Datenschutzvorfällen. Meldepflicht an Verantwortlichen innerhalb von 24 Stunden (siehe § 8).
Datenschutz durch Technikgestaltung	Privacy-by-Design Grundsatz. Daten-Minimierung. Zweckbindung. Standard-Einstellungen sind datenschutzfreundlich (z.B. Google-Drive-Auto-Upload standardmäßig deaktiviert).
Auftragskontrolle	Sub-Auftragsverarbeiter werden vor Einbindung auf DSGVO-Konformität geprüft. Schriftliche Verträge mit allen Sub-Prozessoren (siehe Anlage 2).

Anlage 2 — Sub-Auftragsverarbeiter

Folgende Sub-Auftragsverarbeiter sind zum Zeitpunkt des Vertragsschlusses eingesetzt. Änderungen werden gemäß § 6 Abs. 2 AVV mitgeteilt.

Name & Sitz	Zweck	Verarbeitete Daten	Drittlandtransfer	Garantien
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting, Server-Infrastruktur, Backups	Alle	Nein (EU/DE)	AVV nach Art. 28 DSGVO
Anthropic, PBC 548 Market St, PMB 90375, San Francisco, CA 94104, USA	KI-Sprachmodell (Claude) zur Verarbeitung von Patientennachrichten	Nachrichteninhalte, Anamnese (kein direkter Identifier)	Ja (USA)	EU-Standardvertragsklauseln (SCC) 2021/914 + Zero Data Retention API Mode
360dialog GmbH Torstraße 61, 10119 Berlin, Deutschland	WhatsApp Business Solution Provider (BSP)	Telefonnummern, Nachrichteninhalte	Indirekt über Meta (Irland/USA)	AVV nach Art. 28 DSGVO + SCC für Meta-Komponenten
Meta Platforms Ireland Ltd. 4 Grand Canal Square, Dublin 2, Irland	WhatsApp-Infrastruktur (Cloud API)	Nachrichteninhalte, Telefonnummern	Ja (USA)	EU-Standardvertragsklauseln (SCC) 2021/914
Stripe Payments Europe Ltd. 1 Grand Canal Street Lower, Dublin 2, Irland	Zahlungsabwicklung	Name, E-Mail, Zahlungsdaten	Indirekt (Irland/USA)	EU-Standardvertragsklauseln (SCC) 2021/914
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107, USA	CDN, DDoS-Schutz, Web Application Firewall	IP-Adressen, HTTP-Header	Ja (USA)	EU-Standardvertragsklauseln (SCC) 2021/914
Brevo (ehem. Sendinblue) 106 boulevard Haussmann, 75008 Paris, Frankreich	Transaktions-E-Mails (Verifizierung, Benachrichtigungen)	E-Mail-Adressen, Inhalte	Nein (EU/FR)	AVV nach Art. 28 DSGVO

Google Ireland Ltd. Gordon House, Barrow Street, Dublin 4, Irland	*Optional*: Google Calendar Sync, Google Drive Foto-Backup (nur bei expliziter Aktivierung durch Verantwortlichen)	Termine, Patientenfotos (nur wenn opt-in)	Ja (USA)	EU-Standardvertragsklauseln (SCC) 2021/914 — Google Workspace DPA des Verantwortlichen erforderlich
AviationStack apilayer Data Products GmbH, Wien, Österreich	Flugstatus-Abfrage (nur bei aktiviertem Flug-Tracking)	Flugnummern (nicht patientenbezogen)	Nein (EU/AT)	AVV nach Art. 28 DSGVO

Hinweis zu Drittlandtransfers: Alle Übermittlungen in die USA erfolgen auf Grundlage der EU-Standardvertragsklauseln (SCC) gemäß Durchführungsbeschluss (EU) 2021/914 in der jeweils aktuellen Fassung. Zusätzliche technische und organisatorische Maßnahmen (z.B. Verschlüsselung, Pseudonymisierung) werden geprüft und ggf. ergriffen, um den Anforderungen der „Schrems II"-Rechtsprechung des EuGH zu entsprechen.

Anlage 3 — Weisungen des Verantwortlichen

Der Verantwortliche erteilt dem Auftragsverarbeiter folgende dauerhafte Weisungen für die Verarbeitung personenbezogener Daten:

1. Verarbeitung ausschließlich zu den in § 2 dieses Vertrags genannten Zwecken.
2. Speicherung der Daten ausschließlich auf Servern innerhalb des EWR (Hetzner Deutschland), mit Ausnahme der in Anlage 2 genannten Sub-Auftragsverarbeiter.
3. Verarbeitung von Gesundheitsdaten (Art. 9 DSGVO) nur nach ausdrücklicher Einwilligung der betroffenen Person, dokumentiert im Consent-Log der Plattform.
4. Automatische Anonymisierung von Patientendaten nach Ablauf der konfigurierten Aufbewahrungsfrist (Standard: 10 Jahre).
5. Auf Anfrage des Verantwortlichen vollständige Löschung („Hard Delete") einer Patientenakte innerhalb von 24 Stunden.
6. Bereitstellung von Daten-Exports im JSON-Format auf Anfrage betroffener Personen.
7. Keine Verwendung der Daten zu eigenen Zwecken, insbesondere kein Training von KI-Modellen mit Patientendaten.
8. Sofortige Information bei Anfragen von Behörden oder Aufsichtsbehörden in Bezug auf die verarbeiteten Daten.

Weitere Einzelweisungen kann der Verantwortliche jederzeit per E-Mail an **privacy@flowmatix.io** erteilen. Der Auftragsverarbeiter wird die Weisung unverzüglich umsetzen oder, falls eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt, den Verantwortlichen unverzüglich darauf hinweisen.