Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)

Verantwortlicher (als Auftragsverarbeiter): Bastian Barkowski · Flowmatix · privacy@flowmatix.io
Version: 1.0 · **Stand:** April 2026 · **Nächste Überprüfung:** April 2027

> Flowmatix tritt gegenüber seinen Klinik-Kunden als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) auf. Die Kliniken sind Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Dieses Verzeichnis dokumentiert die Verarbeitungstätigkeiten von Flowmatix gemäß Art. 30 Abs. 2 DSGVO.

1. Patientenkommunikation via WhatsApp

Merkmal	Details
Zweck	Automatisierte und manuelle Kommunikation mit Patienten und Interessenten der Kliniken über WhatsApp
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragsanbahnung); Art. 9 Abs. 2 lit. a (Einwilligung für Gesundheitsdaten)
Datenkategorien	Name, Telefonnummer, Nachrichteninhalte, Sprache, Land
Betroffene Personen	Patienten und Interessenten der Klinik-Kunden
Empfänger	360dialog GmbH (WhatsApp-Provider), Meta Platforms Ireland Ltd. (WhatsApp-Infrastruktur)
Drittlandtransfer	Meta (USA) — EU-SCC (2021/914)
Speicherfrist	Für Dauer des Vertragsverhältnisses + 90 Tage, danach Löschung

2. KI-gestützte Vorqualifizierung (Anthropic Claude)

Merkmal	Details
Zweck	Automatisierte Beantwortung von Patientennachrichten, Anamnese-Erhebung, Terminvorbereitung mittels KI
Rechtsgrundlage	Art. 9 Abs. 2 lit. a (ausdrückliche Einwilligung mit Anthropic-Disclosure im GDPR-Gate)
Datenkategorien	Nachrichteninhalte, Patientenname, Anamnesedaten (Gesundheitsdaten Art. 9)
Betroffene Personen	Patienten, die mit dem KI-Bot interagieren

Empfänger	Anthropic, PBC (San Francisco, USA) — API-Verarbeitung
Drittlandtransfer	USA — EU-SCC (2021/914); Anthropic verwendet API-Daten nicht für Modell-Training
Speicherfrist	Anthropic: bis zu 30 Tage (Trust & Safety); Flowmatix-Nachrichten: wie Punkt 1

3. Anamnesedaten und Patientenakte

Merkmal	Details
Zweck	Erfassung, Speicherung und Verwaltung von Anamnesedaten zur Vorbereitung ärztlicher Beurteilungen
Rechtsgrundlage	Art. 9 Abs. 2 lit. a (Einwilligung); Art. 9 Abs. 2 lit. h (Gesundheitsversorgung)
Datenkategorien	Gesundheitsdaten (Haarausfall, Vorerkrankungen, Medikamente), Fotos (Kopfbereich), Alter, Geschlecht
Betroffene Personen	Patienten der Klinik-Kunden
Empfänger	Ärztliches Personal der jeweiligen Klinik; Cloudflare R2 (Foto-Speicherung)
Drittlandtransfer	Cloudflare (USA) — EU-SCC; R2-Bucket in EU-Region
Speicherfrist	Standard 10 Jahre (§ 630f BGB); konfigurierbar pro Klinik; automatische Anonymisierung nach Fristablauf
Verschlüsselung	AES-256-GCM Feldverschlüsselung für alle PII-Felder (phone, email, name, intake_data)

4. Reisekoordination und Flugüberwachung

Merkmal	Details
Zweck	Überwachung von Anreise-Flugdaten zur Koordination von Airport-Transfer und Hotelcheck-in für internationale Patienten
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragserfüllung); Daten werden ausschließlich auf freiwilliger Basis vom Patienten übermittelt
Datenkategorien	Flugnummer, Abflug-/Ankunftszeiten, Flugstatus (kein Gesundheitsdaten-Bezug); Name des Patienten zur Zuordnung
Betroffene Personen	Patienten mit aktiviertem Flug-Tracking (opt-in)

Empfänger	AviationStack API (apilayer Data Products GmbH, Wien, Österreich) — nur Flugnummer, kein PII; Fahrer-Personal der Klinik
Drittlandtransfer	Keiner (AviationStack: EU/AT)
Speicherfrist	72 Stunden nach geplantem Ankunftsdatum, dann automatische Löschung

5. Terminorganisation

Merkmal	Details
Zweck	Buchung, Verwaltung und Erinnerung zu Behandlungsterminen
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragserfüllung)
Datenkategorien	Name, Telefon, Termindaten, Behandlungsart, Notizen
Betroffene Personen	Patienten der Klinik-Kunden
Empfänger	Klinik-Mitarbeiter; optional Google Calendar (nur bei aktivierter Integration)
Drittlandtransfer	Google (USA, optional) — EU-SCC
Speicherfrist	Wie Patientenakte (Punkt 3)

6. Einzahlungen und Reservierungsgebühren (Stripe)

Merkmal	Details
Zweck	Abwicklung von Patientenanzahlungen und Reservierungsgebühren
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragserfüllung)
Datenkategorien	Zahlungsdaten (via Stripe), Betrag, Währung — keine vollständigen Zahlungsdaten bei Flowmatix
Betroffene Personen	Zahlende Patienten
Empfänger	Stripe Payments Europe Ltd. (Irland) / Stripe, Inc. (USA)
Drittlandtransfer	USA — EU-SCC; Stripe ist EU-Datenschutzrahmen zertifiziert
Speicherfrist	10 Jahre (§ 147 AO)

7. Mitarbeiterdaten der Klinik

Merkmal	Details
Zweck	Verwaltung von Klinik-Mitarbeiterkonten (Login, Rollen, Benachrichtigungen)
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragserfüllung); Art. 6 Abs. 1 lit. f (berechtigtes Interesse)
Datenkategorien	Name, E-Mail, Telefon (optional), Rolle, Login-Daten (gehasht)
Betroffene Personen	Klinik-Mitarbeiter (Admin, Koordinatoren, Ärzte, Finanz)
Empfänger	Keine externen Empfänger
Drittlandtransfer	Keiner
Speicherfrist	Für Dauer des Beschäftigungsverhältnisses + gesetzliche Aufbewahrungsfristen

8. Technische Logs und Monitoring

Merkmal	Details
Zweck	Systemstabilität, Fehlerbehebung, Sicherheitsmonitoring
Rechtsgrundlage	Art. 6 Abs. 1 lit. f (berechtigtes Interesse: Systemsicherheit)
Datenkategorien	IP-Adressen, Zeitstempel, User-IDs, API-Aufrufe (keine Nachrichteninhalte)
Betroffene Personen	Klinik-Nutzer, Patienten (indirekt via IP)
Empfänger	Grafana/Prometheus/Loki (intern); Telegram (Alerts, nur Metadaten)
Drittlandtransfer	Telegram FZ-LLC (Dubai) für Alerts — nur technische Metadaten, keine PII
Speicherfrist	Anwendungslogs: 30 Tage; Audit-Log: 365 Tage; Queue-Jobs: 48 Stunden

9. Flowmatix-eigene Verarbeitungstätigkeiten (als Verantwortlicher)

Merkmal	Details
Zweck	Verwaltung von Klinik-Kundenkonten, Abrechnung, Newsletter (opt-in)
Rechtsgrundlage	Art. 6 Abs. 1 lit. b (Vertragserfüllung); Art. 6 Abs. 1 lit. a (Einwilligung für Marketing)
Datenkategorien	Firmenname, Ansprechpartner, E-Mail, Telefon, Rechnungsdaten
Betroffene Personen	Klinik-Kunden (Unternehmen + Ansprechpartner)

Empfänger	Stripe (Abrechnung); Resend/Nodemailer (E-Mail-Versand)
Drittlandtransfer	Stripe (USA) — EU-SCC
Speicherfrist	Vertragsdauer + 10 Jahre (§ 147 AO für Rechnungen)
