FLOWMATIX

Datenschutz-Folgenabschätzung (DPIA)

gemäß Art. 35 DSGVO

Version 1.0 · Stand: April 2026 · Verantwortlich: Bastian Barkowski

---

1. Zusammenfassung

Diese Datenschutz-Folgenabschätzung dokumentiert die Risiken und Schutzmaßnahmen der durch Flowmatix bereitgestellten Verarbeitung personenbezogener Daten von Patienten und Interessenten von Haartransplantations-Kliniken. Die Verarbeitung umfasst **besondere Kategorien personenbezogener Daten** nach Art. 9 DSGVO (Gesundheitsdaten) sowie den Einsatz **automatisierter Entscheidungsfindung mit KI** (Anthropic Claude), und erfüllt damit zwei der in Art. 35 Abs. 3 DSGVO genannten Kriterien. Eine DPIA ist daher gesetzlich vorgeschrieben.

> **Ergebnis:** Nach Bewertung aller Risiken und Maßnahmen wird das verbleibende Restrisiko als **NIEDRIG bis MITTEL** eingestuft. Die Verarbeitung kann unter Einhaltung der dokumentierten technischen und organisatorischen Maßnahmen rechtskonform durchgeführt werden.

2. Beschreibung der Verarbeitung

2.1 Verantwortlicher

Verantwortlich nach Art. 4 Nr. 7 DSGVO sind die Klinik-Kunden von Flowmatix. Flowmatix selbst tritt als Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO auf. Diese DPIA wird vom Auftragsverarbeiter erstellt, um seine Klinik-Kunden bei deren eigener Compliance-Pflicht zu unterstützen.

2.2 Zweck und Rechtsgrundlage

Zweck	Rechtsgrundlage
Patientenkommunikation via WhatsApp	Art. 6 Abs. 1 lit. b (Vertragsanbahnung), Art. 9 Abs. 2 lit. h (Gesundheitsversorgung)
Anamnese / Vorqualifizierung	Art. 9 Abs. 2 lit. a (ausdrückliche Einwilligung), Art. 9 Abs. 2 lit. h
KI-gestützte Bearbeitung (Claude)	Art. 9 Abs. 2 lit. a (ausdrückliche Einwilligung mit Anthropic-Disclosure)
Terminorganisation	Art. 6 Abs. 1 lit. b
Statistik / Reporting	Art. 6 Abs. 1 lit. f (berechtigtes Interesse)

2.3 Datenkategorien und Betroffene

Verarbeitet werden Stamm-, Kontakt-, Gesundheits-, Bild-, Termin-, Kommunikations- und Reisedaten von Patienten und Interessenten der jeweiligen Klinik (siehe AVV § 3 für vollständige Liste).

2.4 Technische Architektur (Kurzfassung)

- **Hosting:** Hetzner Online GmbH, Falkenstein/Nürnberg, Deutschland (ISO 27001)
- **Datenbank:** PostgreSQL 16 mit Row-Level Security (RLS), Multi-Tenant-Trennung pro Klinik
- **Frontend:** React (Vite), TLS 1.3, Cloudflare CDN/WAF
- **Backend:** Fastify/TypeScript, BullMQ Queue, Redis
- **WhatsApp-Provider:** 360dialog GmbH (Berlin) → Meta Cloud API
- **KI-Komponente:** Anthropic Claude API (Sonnet 4.5), Zero Data Retention API Mode
- **Authentifizierung:** JWT mit Refresh-Token-Rotation, optional MFA (TOTP), bcrypt cost factor 12

3. Notwendigkeit und Verhältnismäßigkeit

3.1 Notwendigkeit

Ohne automatisierte Vorqualifizierung müssten Kliniken jede Patientenanfrage manuell bearbeiten — bei einem typischen Volumen von 50–500 Anfragen pro Tag wäre dies wirtschaftlich nicht darstellbar. Die KI-gestützte Vorqualifizierung dient ausschließlich der Vorbereitung der ärztlichen Beurteilung und ersetzt diese nicht. Die Letztverantwortung für medizinische Entscheidungen verbleibt beim ärztlichen Personal der Klinik.

3.2 Datenminimierung

- Es werden nur Daten erhoben, die für die Vorqualifizierung und Terminbuchung erforderlich sind.
- Patientenfotos werden nur in der vom behandelnden Arzt geforderten Anzahl erhoben.

- Sensible Felder (z.B. Anamnese-JSON) sind in der Datenbank pseudonymisiert/verschlüsselt.
- An Anthropic werden Nachrichteninhalte gesendet — explizit ohne Klar-Identifier (Telefonnummer, Name werden vor dem API-Call entfernt, soweit für die Antwort nicht erforderlich).

3.3 Speicherbegrenzung (Art. 5 Abs. 1 lit. e)

Die Plattform implementiert einen automatisierten Retention-Scanner, der Patientendaten nach Ablauf der konfigurierbaren Aufbewahrungsfrist (Standard: 10 Jahre gemäß § 630f BGB) anonymisiert. Patienten können jederzeit über das CRM eine sofortige Löschung anfordern (Hard Delete via DSGVO Art. 17).

4. Risikobewertung

4.1 Identifizierte Risiken

Risiko	Eintrittswahrscheinlichkeit	Schadensschwere	Bewertung
Unbefugter Zugriff auf Patientendaten	Niedrig	Hoch	Mittel
Datenverlust durch System-Ausfall	Sehr niedrig	Mittel	Niedrig
Cross-Tenant-Datenleck (Klinik A sieht Daten von Klinik B)	Sehr niedrig	Sehr hoch	Mittel
Übertragung an US-Sub-Prozessoren (Anthropic, Cloudflare)	Hoch (kontinuierlich)	Mittel	Mittel
Fehlerhafte KI-Verarbeitung führt zu Falschinformation an Patient	Mittel	Mittel	Mittel
Patient widerruft Einwilligung — Daten werden nicht gelöscht	Niedrig	Hoch	Mittel
Mitarbeiter der Klinik missbraucht Zugriff	Niedrig	Hoch	Mittel
Phishing / Account-Übernahme bei Klinik-Mitarbeiter	Mittel	Hoch	Hoch
Ransomware / Erpressung	Niedrig	Sehr hoch	Mittel
Foto-Upload zu Google Drive ohne Klinik-Bewusstsein	Niedrig (jetzt opt-in)	Hoch	Niedrig

4.2 Maßnahmen zur Risikominderung

Zugriffsschutz

- Multi-Faktor-Authentifizierung (TOTP) für alle Klinik-Konten verfügbar — Empfehlung: für Admin-Rollen verpflichtend
- JWT mit kurzer Lebensdauer + Refresh-Token-Rotation
- Bcrypt cost factor 12 für Passwort-Hashing
- Rate-Limiting auf Login-Endpoints (5 Versuche / 15 Min)
- Session-Revocation bei verdächtiger Aktivität

Mandantentrennung

- PostgreSQL Row-Level Security erzwingt organization_id-Check auf Datenbankebene
- Anwendungs-Code nutzt Tenant-Context (AsyncLocalStorage)
- Kein BYPASSRLS für den Application-User
- Code-Reviews für alle Änderungen mit RLS-Bezug

Drittlandtransfers (Schrems II)

- EU-Standardvertragsklauseln (SCC 2021/914) mit allen US-Sub-Prozessoren
- Anthropic: Zero Data Retention API Mode aktiviert — Daten werden nicht zum Training verwendet
- Pseudonymisierung vor API-Aufruf an Anthropic (kein direkter Identifier)
- Cloudflare: Nur Routing/CDN, keine Inhaltsdaten gespeichert

KI-Risiken

- Bot ist auf 512 Tokens limitiert → kein Halluzinieren von medizinischen Diagnosen
- Strenge System-Prompts mit Verbot medizinischer Entscheidungen
- Prompt-Injection-Schutz durch Wrapping in `<patient_message>` Tags
- Bei photos-complete: automatische Übergabe an menschlichen Arzt-Reviewer
- Bei Aggression / komplexen Fragen: automatischer Handover
- Kein Bot-Antwort vor expliziter GDPR-Einwilligung

Verfügbarkeit und Wiederherstellung

- Tägliche, wöchentliche, monatliche Backups mit Off-Site-Replikation
- RTO: 4h, RPO: 24h
- 24/7 Monitoring (Grafana, Prometheus, Loki, Uptime Kuma)
- Disaster-Recovery-Plan dokumentiert und jährlich getestet

Audit-Trail

- Vollständiges Audit-Log aller Datenzugriffe (Art. 30 DSGVO „record of processing")

- Lesezugriffe auf Patientenakten werden mit User, IP, Timestamp protokolliert
- Audit-Log nicht durch Standard-User löschbar

Patientenrechte

- Daten-Export-Endpoint (Art. 15 + 20) — JSON-Download aller Patientendaten
- Hard-Delete-Endpoint (Art. 17) — vollständige Löschung mit Confirm
- Consent-Log dokumentiert jede Einwilligung mit Zeitstempel
- Auto-Anonymisierung nach Retention-Zeitraum

5. Bewertung des Restrisikos

Kategorie	Vor Maßnahmen	Nach Maßnahmen
Vertraulichkeit	Hoch	Niedrig
Integrität	Mittel	Niedrig
Verfügbarkeit	Mittel	Niedrig
Drittlandtransfer	Hoch	Mittel
KI-Halluzination	Mittel	Niedrig
Gesamt	**Hoch**	**Niedrig–Mittel**

6. Konsultation der Aufsichtsbehörde

Da das verbleibende Restrisiko als niedrig bis mittel eingestuft wird, ist eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO **nicht erforderlich**. Die DPIA wird intern dokumentiert und auf Anfrage der Aufsichtsbehörde oder von Klinik-Kunden zur Verfügung gestellt.

7. Regelmäßige Überprüfung

Diese DPIA wird mindestens jährlich oder bei wesentlichen Änderungen der Verarbeitung überprüft und aktualisiert. Wesentliche Änderungen umfassen:

- Einführung neuer Sub-Prozessoren
- Änderung der Zwecke oder Datenkategorien
- Wechsel des KI-Anbieters oder -Modells
- Bekanntwerden neuer Risiken (z.B. Sicherheitslücken)
- Änderungen der Rechtsprechung (z.B. Schrems III)

8. Verantwortlichkeiten

Rolle	Verantwortung
Geschäftsführung Flowmatix	Bastian Barkowski — Gesamtverantwortung, Freigabe der DPIA
Datenschutzbeauftragter	privacy@flowmatix.io
Technische Umsetzung	Engineering Team (Bastian Barkowski)
Sub-Prozessoren-Management	privacy@flowmatix.io

ERSTELLT VON

Bastian Barkowski · Flowmatix

Hude, April 2026

NÄCHSTE ÜBERPRÜFUNG

April 2027

oder bei wesentlicher Änderung