Löschkonzept

Internes Prozessdokument gemäß Art. 5 Abs. 1 lit. e DSGVO (Speicherbegrenzung)

Verantwortlich: Bastian Barkowski · Flowmatix · privacy@flowmatix.io
Version: 1.0 · **Stand:** April 2026 · **Nächste Überprüfung:** April 2027

> Dieses Löschkonzept konsolidiert alle Aufbewahrungsfristen und Löschroutinen der Flowmatix-Plattform an einem zentralen Ort. Es dient als Nachweis für Aufsichtsbehörden, Enterprise-Kunden und interne Audits.

1. Rechtsgrundlage und Grundsatz

Gemäß Art. 5 Abs. 1 lit. e DSGVO (Speicherbegrenzung) müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Nach Zweckerfüllung sind Daten zu löschen oder zu anonymisieren.

Flowmatix betreibt als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) gegenüber seinen Klinik-Kunden ein zweistufiges System: **(1) automatisierte Retention-Scanner** laufen täglich und prüfen alle Datenkategorien; **(2) manuelle Löschanfragen** werden innerhalb von 24 Stunden durch den Platform Owner umgesetzt.

2. Aufbewahrungsfristen nach Datenkategorie

Datenkategorie	Aufbewahrungsfrist	Rechtsgrundlage	Löschmethode	Automatisiert?
Patientendaten (Stammdaten, Kontakt)	10 Jahre ab letztem Behandlungskontakt	§ 630f BGB (ärztliche Dokumentationspflicht)	Hard Delete (kryptographische Schlüssellöschung + DB-Löschung)	Ja — Retention-Scanner täglich
Gesundheitsdaten / Anamnese (Art. 9)	10 Jahre (konfigurierbar 3–30 Jahre pro Klinik)	§ 630f BGB; Klinik-spezifische Anforderungen	AES-Schlüssel-Rotation + Feldverschlüsselung-Löschung; danach Anonymisierung	Ja — Retention-Scanner täglich
Patientenfotos	10 Jahre (konfigurierbar)	§ 630f BGB	Cloudflare R2 Object-Deletion + DB-Referenz-Löschung	Ja — Retention-Scanner täglich

WhatsApp-Nachrichtenverläufe	Vertragsdauer + 90 Tage	Art. 6 Abs. 1 lit. b DSGVO (Vertrag)	Hard Delete aus events-Tabelle (payload wird bereits bei Speicherung auf NULL gesetzt)	Ja — 90-Tage-Cleanup
Termindaten	10 Jahre (wie Patientenakte)	§ 630f BGB	Hard Delete mit Patientenakte	Ja
Reise-/Flugdaten	72 Stunden nach geplantem Ankunftsdatum	Art. 6 Abs. 1 lit. b DSGVO; Zweckbindung	Automatische Feldleerung (flight_info = NULL)	Ja — täglicher Cleanup
Einwilligungsnachweise (Consent-Log)	3 Jahre nach letztem Patientenkontakt	Art. 7 Abs. 1 DSGVO (Nachweispflicht)	Anonymisierung (Personenbezug entfernen, Timestamp + Consent-Status behalten)	Ja — Retention-Scanner
Klinik-Mitarbeiterdaten	Dauer Beschäftigung + gesetzliche Fristen (3 Jahre Arbeitsrecht, 10 Jahre Finanzdaten)	§ 147 AO, BetrVG	Soft-Delete → Hard Delete nach Fristablauf	Teilweise — manuelle Prüfung empfohlen
Rechnungs- und Abrechnungsdaten	10 Jahre	§ 147 AO (Buchführungspflicht)	Hard Delete nach Ablauf	Ja — Retention-Scanner
Stripe-Zahlungsdaten	10 Jahre (Stripe-seitig)	§ 147 AO; Stripe-Policy	Löschantrag an Stripe nach Fristablauf	Nein — manuell über Stripe Dashboard
Anwendungslogs (App-Logs)	30 Tage	Art. 6 Abs. 1 lit. f DSGVO (Systemsicherheit)	Automatische Log-Rotation (Loki, Docker)	Ja
Audit-Logs	365 Tage	Art. 5 Abs. 2 DSGVO (Rechenschaftspflicht)	Automatische Löschung durch db-retention-cleanup.sh (täglich 03:30 UTC)	Ja
BullMQ / Queue-Jobs (fehlgeschlagen)	48 Stunden	Art. 5 Abs. 1 lit. e DSGVO (Minimierung)	Redis ZEXPIRE / removeOnFail:	Ja

			172800s	
Session-Tokens (Redis)	30 Tage (Refresh-Token-Lebensdauer)	Art. 6 Abs. 1 lit. b DSGVO	Redis TTL + db-retention-cleanup.sh	Ja
Webhook-Events	30 Tage	Art. 6 Abs. 1 lit. f DSGVO	db-retention-cleanup.sh	Ja
Website-Seitenzugriffe (page_views)	90 Tage	Art. 6 Abs. 1 lit. f DSGVO	db-retention-cleanup.sh	Ja
Anthropic API (Trust & Safety)	Bis zu 30 Tage (Anthropic-seitig)	Anthropic API Terms; SCC	Automatisch durch Anthropic; keine Nutzung für Training	Ja (Anthropic-seitig)

3. Automatisierte Löschroutinen

Script / Mechanismus	Ausführungszeit	Betroffene Daten
db-retention-cleanup.sh	Täglich 03:30 UTC	webhook_events (30d), page_views (90d), idempotency_keys (7d), sessions (30d), audit_log (365d), queue_jobs (7d), VACUUM ANALYZE
data-retention.sh	Täglich 02:00 UTC	Patientendaten nach konfigurierbarer Frist (Standard 10 Jahre), Soft-Delete-Bereinigung
cleanup-offboarded-orgs.sh	Monatlich 03:00 UTC	Vollständige Löschung abgemeldeter Klinik-Orgs nach Kündigungsfrist
Redis TTL (automatisch)	Kontinuierlich	Sessions, Refresh-Tokens, Queue-Jobs, MFA-Tokens, Rate-Limits
BullMQ removeOnFail: 172800s	Kontinuierlich	Fehlgeschlagene Queue-Jobs (48h)
Log-Rotation (Loki/Docker)	Täglich	Anwendungslogs (30 Tage), System-Logs

4. Manuelle Löschprozesse

4.1 Betroffenenrecht auf Löschung (Art. 17 DSGVO)

1. Patient oder Klinik stellt Löschantrag per E-Mail an privacy@flowmatix.io oder über CRM-Interface
2. Identitätsprüfung innerhalb von 24h
3. Hard Delete im CRM ausführen (löscht alle verknüpften Datensätze transaktional)
4. Bestätigung der Löschung an Antragsteller innerhalb von 72h
5. Eintrag im Audit-Log

Ausnahmen vom Löschrecht: Gesetzliche Aufbewahrungspflichten (§ 630f BGB, § 147 AO) gehen dem Löschrecht vor. In diesen Fällen wird die Verarbeitung eingeschränkt (Art. 18 DSGVO) statt gelöscht.

4.2 Klinik-Offboarding

1. Nach Kündigung: 30-tägige Übergangsphase (Klinik kann Daten exportieren)
2. Nach 30 Tagen: Org-Status auf „offboarded" gesetzt
3. Nach weiteren 30 Tagen: cleanup-offboarded-orgs.sh löscht alle Daten der Org
4. Auf Anfrage: sofortige vollständige Löschung möglich
5. Löschbestätigung schriftlich per E-Mail

4.3 Sub-Processor-Löschung

Bei Beendigung eines Sub-Processor-Vertrags oder auf Anfrage:

- **Anthropic:** Kein persistentes Datenlager (API-Verarbeitung only); 30-Tage-Safety-Daten laufen automatisch ab
- **Cloudflare R2:** Bucket-Löschung über Cloudflare Dashboard
- **Stripe:** Kundendaten-Löschantrag über Stripe Dashboard nach 10-Jahres-Frist
- **360dialog:** Datenlöschung durch 360dialog auf Anfrage gemäß DPA

5. Sonderfall: Laufende Rechtsstreitigkeiten

> Bei laufenden Rechtsstreitigkeiten, Behördenanfragen oder Datenpannen-Untersuchungen können reguläre Löschfristen ausgesetzt werden (Legal Hold). Entscheidung trifft ausschließlich Bastian Barkowski (privacy@flowmatix.io). Beginn und Ende eines Legal Hold werden dokumentiert.

6. Nachweis und Dokumentation

- Alle automatischen Löschvorgänge werden in den jeweiligen Script-Logs dokumentiert: `/opt/flowmatix/logs/`
- Manuelle Löschvorgänge werden im Audit-Log der Plattform verzeichnet (Aktion: `gdpr_patient_deleted`)

- Dieses Löschkonzept wird mindestens jährlich oder bei wesentlichen Änderungen aktualisiert

---