FLOWMATIX

Data Processing Agreement (DPA)

pursuant to Article 28 GDPR

Version 2.0 · April 2026

CONTROLLER

[Name of the Clinic]
[Street, Number]
[Postal code, City, Country]
represented by: [Management / Owner]
— hereinafter "Controller" —

PROCESSOR

Flowmatix – Automation
Owner: Bastian Barkowski
An der Moorbäke 6, 27798 Hude, Germany
Email: legal@flowmatix.io
— hereinafter "Processor" —

Recitals

The Controller uses the services of the Processor to automate patient communication, pre-qualification, appointment management, and AI-assisted preparation of medical assessments. In doing so, personal data of patients and prospective patients of the Controller is processed. This agreement governs the data protection obligations of the parties pursuant to Article 28 GDPR and supersedes all previous data processing arrangements.

§ 1 Subject Matter and Duration

(1) Subject Matter

The subject matter of this agreement is the processing of personal data by the Processor in the context of providing the Flowmatix CRM and automation platform to the Controller.

(2) Duration

The agreement begins upon execution and runs for an indefinite period. It terminates automatically with the termination of the underlying main contract or may be terminated by either party with four weeks' written notice. The right to extraordinary termination for good cause remains unaffected.

§ 2 Nature and Purpose of Processing

Personal data is processed exclusively for the following purposes:

- Digital patient communication via WhatsApp and comparable channels
- Pre-qualification of patients based on anamnesis data
- AI-assisted preparation of patient files for medical assessment (using the Anthropic Claude API)
- Organization of consultations, surgery dates, and follow-ups
- Sending reminders, aftercare messages, and treatment plans
- Management of patient documents, photos, and medical information
- Provision of statistics and reporting to the Controller
- Technical support and maintenance of the platform

No medical diagnosis or treatment recommendation is provided by the Processor. Final responsibility for medical decisions remains with the Controller and its medical staff.

§ 3 Categories of Personal Data

- **Master data:** First and last name, gender, age / date of birth, language, country
- **Contact data:** Phone number (WhatsApp), email address
- **Health data (Art. 9 GDPR):** Anamnesis, hair status, pre-existing conditions, medications, allergies, previous treatments, smoker status, blood thinners, other medical information
- **Image data:** Patient photos (front, side, donor area, close-ups)
- **Appointment data:** Consultation and surgery dates, calendar bookings
- **Communication content:** WhatsApp messages, voice messages (transcribed), documents
- **Travel data:** Flight data (voluntarily provided by the patient), driver / hotel info
- **Consent records:** GDPR consent logs with timestamps

§ 4 Categories of Data Subjects

- Patients and prospective patients of the Controller
- Employees and medical staff of the Controller (limited, as required for platform usage)

§ 5 Obligations of the Processor

(1) Documented Instructions

The Processor processes personal data exclusively on documented instructions from the Controller, including with regard to transfers to third countries, unless legally required otherwise.

(2) Confidentiality

The Processor ensures that all persons authorized to process personal data are bound by confidentiality or are subject to an appropriate statutory duty of confidentiality. Staff are trained on data protection on a regular basis.

(3) Security of Processing

The Processor implements all required measures pursuant to Article 32 GDPR. A detailed description of technical and organizational measures is provided in **Annex 1**.

(4) Assistance

The Processor assists the Controller, taking into account the nature of processing, with appropriate technical and organizational measures in responding to data subject requests and in complying with obligations under Articles 32–36 GDPR (in particular security, breach notification, and data protection impact assessments).

§ 6 Sub-Processors

(1) General Authorization

The Controller grants the Processor general written authorization to engage further processors ("Sub-Processors") for the provision of the service. The Sub-Processors engaged at the time of contract conclusion are listed in **Annex 2**.

(2) Changes

The Processor will inform the Controller of any intended changes regarding the addition or replacement of Sub-Processors at least 30 days in advance via email to the registered contact address. The Controller may object to the change in writing within 14 days for compelling data protection reasons. In case of objection, both parties are entitled to extraordinary termination.

(3) Sub-Processor Obligations

The Processor contractually obligates each Sub-Processor to at least the same data protection obligations as set forth in this DPA. If a Sub-Processor fails to meet its data protection obligations, the Processor remains fully liable to the Controller for the performance of that Sub-Processor's obligations.

§ 7 International Data Transfers

Where personal data is transferred to third countries outside the EEA, the Processor ensures that one of the following safeguards under Articles 44 et seq. GDPR is in place:

- An adequacy decision by the EU Commission, or
- EU Standard Contractual Clauses (SCC) in the current version (Implementing Decision (EU) 2021/914), supplemented where necessary by additional measures following the Schrems II case law, or
- Binding corporate rules (BCR), or
- Explicit consent of the data subject to the specific transfer pursuant to Art. 49(1)(a) GDPR.

A complete list of all third-country transfers and their legal bases is provided in **Annex 2**.

§ 8 Personal Data Breach Notification

The Processor will notify the Controller without undue delay, and in any event within **24 hours** of becoming aware of any personal data breach (Art. 33 GDPR). The notification will contain at minimum:

- Description of the nature of the breach (categories and approximate number of affected data subjects and records)
- Name and contact details of the Data Protection Officer or other contact point
- Description of likely consequences
- Description of measures taken or proposed to address the breach

The Processor assists the Controller in fulfilling its notification obligations to the supervisory authority and, where applicable, the affected data subjects.

§ 9 Data Subject Rights

The Processor assists the Controller in handling data subject requests under Articles 12–22 GDPR, in particular:

- **Right of access (Art. 15):** The platform provides an export function (JSON format) to download all stored patient data.
- **Right to rectification (Art. 16):** Master data and patient records can be updated by the Controller at any time.
- **Right to erasure (Art. 17):** The platform offers a complete deletion function ("hard delete") that irreversibly removes all personal data.
- **Right to restriction (Art. 18):** The Controller can place patient records in read-only status.
- **Right to data portability (Art. 20):** The export function provides data in a structured, commonly used, machine-readable format (JSON).

- **Right to object (Art. 21):** The Controller can deactivate automated processing at any time.

§ 10 Audit Rights

The Controller has the right to monitor compliance with this agreement by the Processor. Upon request, the Processor will provide all information necessary to demonstrate compliance.

Audits may be conducted on-site or remotely with four weeks' prior notice, no more than once per calendar year and limited to one business day, unless there are specific indications of a data protection breach. In lieu of an on-site audit, the Processor may submit a current report from an independent auditor (e.g., ISO 27001, SOC 2, BSI C5).

§ 11 Retention and Deletion

The Processor stores personal data only for as long as is necessary to provide the agreed services or as required by statutory retention obligations. The platform implements an automated retention scanner that anonymizes patient data after the configurable retention period (default: 10 years pursuant to § 630f BGB) has expired.

Upon termination of the agreement, the Processor will delete or anonymize all personal data within **30 days**, unless the Controller expressly requests return in a structured format. Deletion will be confirmed in writing upon request.

§ 12 Liability

The liability of the parties is governed by Article 82 GDPR. The Processor shall only be liable if it has not complied with the obligations specifically directed at processors under the GDPR or if it has acted contrary to or outside the lawful instructions of the Controller.

Liability of the Processor for medical decisions, treatment measures, or therapeutic recommendations is excluded. These remain exclusively the responsibility of the Controller.

§ 13 Data Protection Officer

The Processor's Data Protection Officer can be reached at: **privacy@flowmatix.io**. The Controller will inform the Processor of the name and contact details of its Data Protection Officer (if appointed) without undue delay.

§ 14 Governing Law and Jurisdiction

This agreement is governed exclusively by German law, excluding the UN Convention on Contracts for the International Sale of Goods. The place of jurisdiction for disputes arising from or in connection

with this agreement is Hude (or the nearest competent court in Germany), provided the Controller is a merchant, legal entity under public law, or special public-law fund.

§ 15 Final Provisions

(1) Should individual provisions of this agreement be or become invalid, the validity of the remaining agreement shall not be affected. The parties will replace the invalid provision with a valid provision that comes as close as possible to the economic and legal purpose of the invalid provision.

(2) Amendments and supplements to this agreement must be made in writing. This also applies to the waiver of this written form requirement.

(3) In case of conflict between this DPA and the main contract, the provisions of this DPA prevail.

CONTROLLER

[Name]

Place, Date, Signature

PROCESSOR

Bastian Barkowski · Flowmatix

Hude, _____, _____

Annex 1 — Technical and Organizational Measures (TOMs)

This annex describes the technical and organizational measures implemented pursuant to Article 32 GDPR to ensure a level of protection appropriate to the risk.

1. Confidentiality

Measure	Implementation
Physical access control	Servers in certified data centers (Hetzner Online GmbH, Falkenstein/Nuremberg, Germany) — ISO 27001 certified. Physical access only for authorized personnel with two-factor authentication.
System access control	Multi-factor authentication (TOTP) for all platform accounts. Session cookies with refresh-token rotation. Bcrypt password hashing (cost factor 12).
Data access control	Role-based access control (RBAC) with 6 roles. Row-level security (RLS) at the database level enforces tenant separation. Each employee only sees data of their own clinic.
Tenant separation	Multi-tenant architecture with strict separation per clinic (organization_id) at all layers. PostgreSQL row-level security prevents cross-tenant access even in case of application bugs.
Pseudonymization	Sensitive fields (e.g. anamnesis data) are stored encrypted. Audit logs contain user IDs instead of names.

2. Integrity

Measure	Implementation
Transfer control	Transport encryption (TLS 1.3) for all external connections. WhatsApp communication end-to-end encrypted via the WhatsApp protocol.
Input control	Complete audit log of all data accesses and changes with timestamp, user ID, IP address and user agent. Read access to patient records is logged pursuant to Art. 30 GDPR.
Encryption at rest	Database backups encrypted with AES-256. Sensitive fields additionally encrypted at the application layer.

3. Availability and Resilience

Measure	Implementation
Availability control	Daily, weekly and monthly automated backups with off-site replication. 24/7 monitoring with alerting (Grafana, Prometheus, Loki, Uptime Kuma). Geographically redundant DNS.
Recoverability	Recovery Time Objective (RTO): 4 hours. Recovery Point Objective (RPO): 24 hours. Disaster recovery plan documented and tested annually.
Resilience	Circuit breaker for external APIs, automatic failover for database connections, Redis persistence with AOF + RDB.

4. Procedures for Regular Review

Measure	Implementation
Data protection management	Data Protection Officer appointed (privacy@flowmatix.io). Records of processing activities maintained pursuant to Art. 30 GDPR. Data Protection Impact Assessment (DPIA) for the processing of health data documented.
Incident response management	Documented process for detecting, reporting and handling data protection incidents. Notification obligation to the Controller within 24 hours (see § 8).
Privacy by design	Privacy-by-design principle. Data minimization. Purpose limitation. Default settings are privacy-friendly (e.g. Google Drive auto-upload disabled by default).
Sub-processor management	Sub-processors are vetted for GDPR compliance before engagement. Written agreements with all sub-processors (see Annex 2).

Annex 2 — Sub-Processors

The following sub-processors are engaged at the time of contract conclusion. Changes will be communicated pursuant to § 6(2) of this DPA.

Name & Address	Purpose	Data processed	Third-country transfer	Safeguards
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting, server infrastructure, backups	All	No (EU/DE)	DPA pursuant to Art. 28 GDPR
Anthropic, PBC 548 Market St, PMB 90375, San Francisco, CA 94104, USA	AI language model (Claude) for processing patient messages	Message content, anamnesis (no direct identifier)	Yes (USA)	EU Standard Contractual Clauses (SCC) 2021/914 + Zero Data Retention API mode
360dialog GmbH Torstraße 61, 10119 Berlin, Germany	WhatsApp Business Solution Provider (BSP)	Phone numbers, message content	Indirectly via Meta (Ireland/USA)	DPA pursuant to Art. 28 GDPR + SCC for Meta components
Meta Platforms Ireland Ltd. 4 Grand Canal Square, Dublin 2, Ireland	WhatsApp infrastructure (Cloud API)	Message content, phone numbers	Yes (USA)	EU Standard Contractual Clauses (SCC) 2021/914
Stripe Payments Europe Ltd. 1 Grand Canal Street Lower, Dublin 2, Ireland	Payment processing	Name, email, payment data	Indirectly (Ireland/USA)	EU Standard Contractual Clauses (SCC) 2021/914
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107, USA	CDN, DDoS protection, web application firewall	IP addresses, HTTP headers	Yes (USA)	EU Standard Contractual Clauses (SCC) 2021/914
Brevo (formerly Sendinblue) 106 boulevard Haussmann, 75008 Paris, France	Transactional emails (verification, notifications)	Email addresses, content	No (EU/FR)	DPA pursuant to Art. 28 GDPR
Google Ireland Ltd. Gordon House, Barrow Street, Dublin 4, Ireland	*Optional*: Google Calendar sync, Google Drive photo backup (only if explicitly enabled by the Controller)	Appointments, patient photos (only if opt-in)	Yes (USA)	EU Standard Contractual Clauses (SCC) 2021/914 — Controller's own Google Workspace DPA required

AviationStack apilayer Data Products GmbH, Vienna, Austria	Flight status lookup (only if flight tracking is enabled)	Flight numbers (not patient-related)	No (EU/AT)	DPA pursuant to Art. 28 GDPR

Note on third-country transfers: All transfers to the USA are based on the EU Standard Contractual Clauses (SCC) pursuant to Implementing Decision (EU) 2021/914 in the current version. Additional technical and organizational measures (e.g. encryption, pseudonymization) are reviewed and implemented as appropriate to meet the requirements of the CJEU's "Schrems II" ruling.

Annex 3 — Controller Instructions

The Controller issues the following standing instructions to the Processor for the processing of personal data:

1. Processing exclusively for the purposes set out in § 2 of this agreement.
2. Storage of data exclusively on servers within the EEA (Hetzner Germany), with the exception of the sub-processors listed in Annex 2.
3. Processing of health data (Art. 9 GDPR) only with explicit consent of the data subject, documented in the platform's consent log.
4. Automatic anonymization of patient data after expiry of the configured retention period (default: 10 years).
5. On request of the Controller, complete deletion ("hard delete") of a patient record within 24 hours.
6. Provision of data exports in JSON format on request of data subjects.
7. No use of data for own purposes, in particular no training of AI models with patient data.
8. Immediate notification of any requests by authorities or supervisory bodies relating to the processed data.

Further individual instructions may be issued by the Controller at any time via email to **privacy@flowmatix.io**. The Processor will implement the instruction without undue delay or, if in its view an instruction violates data protection law, will inform the Controller of this without undue delay.