BookMe AI — Data Processing Agreement (Cover Page)

Incorporating the Common Paper DPA Standard Terms (Version 1.1) • DPA Version 1.0 — Effective 31 July 2026

This Data Processing Agreement ("DPA") consists of (1) the Key Terms on this Cover Page and (2) the Common Paper DPA Standard Terms Version 1.1 posted at commonpaper.com/standards/data-processing-agreement/1.1/ ("DPA Standard Terms"), which are incorporated by reference. If there is any inconsistency between the parts of the DPA, this Cover Page will control. This DPA forms part of and supplements the BookMe AI Terms of Service and is electronically accepted by Customer upon account creation or execution of the Agreement.

Scope note: this DPA governs Customer Personal Data — the personal data of Customer's end customers and staff that Provider processes on Customer's behalf (Provider as Processor). It does not cover Customer's own account, billing, and marketing data, for which Provider acts as an independent Controller under its Privacy Policy (billing is processed via Revolut and is outside this DPA).

Key Terms

Provider	Mythril-Tech S.R.L., a company incorporated in Romania, registered office at Str. Rapsodiei nr. 7, Sc. 1, Et. 4, Ap. 10, Cluj-Napoca, Cluj County, Romania, CUI 47085909, trade registry no. J2022006613129 ("Provider"). Provider is the sole contracting entity under this DPA for all Customers.
Customer	The legal entity that accepts the Agreement and this DPA (the business using BookMe AI) ("Customer")
Service	BookMe AI: AI-powered WhatsApp appointment scheduling, including inbound message processing, automated replies, calendar availability checks, and appointment booking on Customer's behalf
Agreement	The BookMe AI Terms of Service available at /terms-of-service on the Service website, as accepted by Customer
Approved Subprocessors	As listed in Annex III below and maintained at /subprocessors on the Service website. Provider will give at least 10 business days' prior written notice of changes per Section 2.6 of the DPA Standard Terms; Customer may object within 30 days.
Provider Security Contact	security@mythril-tech.com
Security Policy	The security overview available at /security on the Service website
Report	Provider is an early-stage company and does not currently hold third-party audit certifications (e.g., SOC 2, ISO 27001). In lieu of a Report, Provider will make available its written Security Policy and will respond to reasonable security questionnaires per Section 5.3 of the DPA Standard Terms.
Governing Member State	Romania. The EEA SCCs, where applicable, are governed by the laws of Romania; disputes will be resolved in the courts of Romania (Cluj-Napoca).
Supervisory Authority	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Romania

Annex I(A) — List of Parties

Data exporter	Customer (Controller). Contact: as provided in Customer's account. Activities: provision of services to its end customers (including, where applicable, medical, dental, or other healthcare services); use of the Service for appointment scheduling.
Data importer	Provider (Processor). Contact: Provider Security Contact above. Activities: operating an automated WhatsApp-based appointment scheduling service with AI reply generation and calendar synchronization on behalf of Customer.

Annex I(B) — Description of Processing

Categories of Data Subjects	(a) Customer's end customers who communicate with Customer's WhatsApp number; (b) Customer's authorized users and practitioners (business staff who sign in or whose names and availability appear in connected calendars).
Categories of Personal Data	End-customer data: name, WhatsApp phone number, profile name; content and metadata of WhatsApp messages exchanged with the automated assistant (Conversation records); appointment data — requested service, date/time, practitioner, status, optional notes, linked calendar event ID (Appointment records). Customer staff data: account name, email, business profile details. Technical/credential data processed to operate the Service: WhatsApp Business Account ID, phone number ID, Meta access token, Google Calendar OAuth tokens.
Special Category Data (GDPR Art. 9)	Health data, where Customer is a healthcare provider (e.g., medical clinic, dental practice, therapy practice): the existence of an appointment, the type of service requested, and free-text messages sent by Data Subjects may reveal or imply information concerning health. No other Art. 9 categories are intentionally collected. Where Customer is not a healthcare provider, no Special Category Data is intended to be processed.
Special Category Data Restrictions or Safeguards	Data minimization by design: the automated assistant is instructed to collect only the data strictly necessary for scheduling (name, phone number, service type, time slot) and not to solicit symptoms, diagnoses, or other medical details. Customer obligation: Customer will not configure or use the Service to solicit health or other special category data beyond what scheduling inherently implies, and is responsible for a lawful basis under GDPR Art. 9(2) for its patient scheduling data. AI processing disclosure: message text is processed by the AI subprocessors in Annex III solely to generate scheduling replies; prompts and outputs are not used to train models. Customer should disclose the use of an automated assistant to its end customers; the assistant also identifies itself as automated. Purpose limitation: Customer Personal Data is not used for advertising, profiling, or model training. Encryption in transit (TLS 1.2+) and at rest (AES-256); database residency in the EU (Frankfurt); access restricted, need-to-know, MFA on administrative accounts. Retention and deletion per Annex I(B) Duration and Section 7 of the DPA Standard Terms.

Frequency of Transfer	Continuous (real-time message processing) for the duration of the Agreement.
Nature and Purpose of Processing	Collection, storage, transmission, AI analysis, automated response generation, calendar read/write, and appointment record creation, for the purpose of providing an automated receptionist and booking service via WhatsApp on Customer's behalf.
Duration of Processing	The term of the Agreement. Upon account deletion, Customer Personal Data is deleted from production systems immediately. Upon termination of the Agreement, Provider deletes or returns Customer Personal Data within 30 days. Encrypted backups are purged within 90 days. Data may be retained beyond these periods only where required by applicable law, with documented justification. Written confirmation of deletion is provided on request. Events already written to Customer's own Google Calendar remain under Customer's control and are not deleted by Provider.

Annex II — Technical and Organizational Measures

- **Encryption:** TLS 1.2+ for all data in transit; AES-256 encryption at rest for the production database and backups; WhatsApp transport end-to-end encrypted between Data Subject and the Business Platform endpoint.
- **Access control:** Role-based access with least privilege; per-tenant data isolation in the multi-tenant database; MFA required on all administrative accounts; access logging.
- **Data residency:** Production personal data is stored in the EU (Dublin, Ireland). AI processing and application compute involve transfers to the USA under the safeguards in Annex III.
- **Backups:** Automated daily backups with point-in-time recovery; backups purged within 90 days of deletion from production.
- **Data minimization by design:** The scheduling assistant operates under system instructions enforcing collection of scheduling data only; the assistant identifies itself as automated and does not solicit medical or other sensitive details.
- **Secure development:** OAuth tokens and API credentials stored encrypted in managed environment configuration; no credentials in source code; dependency and vulnerability monitoring.
- **Personnel:** All personnel with data access are bound by written confidentiality obligations.
- **Incident response:** Documented incident response process; Customer notified of Security Incidents without undue delay and no later than 72 hours after awareness, including nature of the breach, categories and approximate number of affected records, likely consequences, and measures taken or proposed. Government and authority requests are handled per Provider's Government Data Requests Policy and Section 6.1 of the DPA Standard Terms.
- **Data subject requests:** If an end customer contacts Provider directly with a data subject request, Provider notifies Customer within 5 business days and assists on documented instruction; Customer remains responsible for responding to its own customers.
- **Subprocessor management:** Written DPAs with all subprocessors incorporating GDPR Art. 28(3) obligations; transfers to the USA covered by the EU-U.S. Data Privacy Framework or the 2021 EEA SCCs, per each subprocessor's published terms.
- **Cooperation:** DPIA assistance and audit cooperation as set out in Sections 5 and 6 of the DPA Standard Terms.

Annex III — Approved Subprocessors

Subprocessor	Location	Processing task
Meta Platforms Ireland Limited (WhatsApp Business Platform / Cloud API)	Ireland (global infrastructure)	Delivery and receipt of WhatsApp messages between Data Subjects and the Service; hosting of WABA credentials.
Google LLC — Gemini API	USA	AI analysis of end-user WhatsApp message text and generation of automated scheduling replies. Paid API tier only; prompts and outputs are not used to train models.
Google LLC — Calendar API	USA (global)	Reading availability and creating/updating appointment events in Customer's connected calendar (customer name, phone, appointment times).
OpenAI, L.L.C.	USA	Alternative AI provider processing the same WhatsApp message text as Gemini, only where Customer selects OpenAI. API data is not used to train models.
Supabase, Inc.	USA (data hosted in EU region — Dublin, Ireland)	PostgreSQL database hosting of all stored tenant and end-customer data (conversations, appointments, configuration). EU-U.S. Data Privacy Framework participant.
Vercel, Inc.	USA	Application hosting and serverless compute; Customer Personal Data in transit during webhook/API processing and transient request logs. EU-U.S. Data Privacy Framework participant.
Twilio Inc.	USA	Legacy WhatsApp integration path only, for tenants connected before migration to the Meta Cloud API. Same message data as Meta. Not used for new tenants.

The current list is maintained at /subprocessors on the Service website. Provider will notify Customer at least 10 business days before adding or replacing a Subprocessor; Customer may object within 30 days per Section 2.6(a) of the DPA Standard Terms. If an objection cannot be resolved in good faith, Customer may terminate the Agreement with respect to the affected Service. Revolut Ltd processes Customer's own billing data with Provider acting as Controller and is therefore listed in the Privacy Policy, not in this Annex.

Acceptance

This DPA is accepted electronically by Customer upon creation of a BookMe AI account or execution of the Agreement, whichever occurs first, and takes effect on that date. No wet signature is required. Provider logs the accepting account, timestamp, and DPA version. Upon written request, Provider will countersign a copy of this Cover Page.

Provider: Mythril-Tech S.R.L. — Name/Title: _____ Date: _____

Customer: _____ — Name/Title: _____ Date: _____