TEMPLATE: requires review by qualified legal counsel before signing. This is not legal advice.

Data Processing Agreement

Last updated: September 26, 2026

1. Parties

This Data Processing Agreement ("DPA") is entered into between:

- Data Processor: Corebee Chat LTD ("Corebee", "Processor", "we" or "us"), the provider of the Corebee customer support platform.
- Data Controller: the customer ("Controller", "you" or "your") who has entered into a service agreement with Corebee and determines the purposes and means of the processing of personal data.

This DPA forms part of the Terms of Service (https://corebee.ai/terms) between the parties and is governed by the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the UK GDPR and other applicable data protection law.

2. Definitions

- "Controller" means the customer who determines the purposes and means of the processing of personal data.
- "Processor" means Corebee, which processes personal data on behalf of the Controller.
- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Processing" means any operation performed on personal data, including collection, storage, alteration, retrieval, use, disclosure or deletion.
- "Sub-processor" means any third party engaged by the Processor to process personal data on behalf of the Controller.
- "Data Subject" means an identified or identifiable natural person whose personal data is processed.
- "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Subject Matter and Duration

Subject matter

This DPA governs the processing of personal data by the Processor on behalf of the Controller through the Corebee customer support platform, solely to fulfil the Processor's obligations under the service agreement.

Duration

This DPA remains in effect for the duration of the service agreement and ends with it, subject to the return and deletion obligations in section 14.

4. Nature and Purpose of Processing

The Processor processes personal data on behalf of the Controller to:

- Provide AI customer support, including automated replies and conversation routing
- Store and manage support conversations across channels (chat, email, WhatsApp, SMS, social media and voice calls)
- Manage contact records and conversation history
- Maintain and serve knowledge base content used to answer customers (it is not used to train AI models)
- Provide analytics, reporting and performance metrics on support operations

5. Types of Personal Data

- Names and display names

- Email addresses and phone numbers
- Conversation content: messages, attachments, call audio and transcripts
- IP addresses and device information (browser, user agent, operating system)
- Usage data (pages visited, events, session information) and cookie identifiers
- Custom data fields defined by the Controller (for example account IDs or plan information)

6. Categories of Data Subjects

- End users and customers of the Controller who contact it through channels managed by Corebee
- The Controller's team members (agents and administrators) who use the Corebee platform

7. Sub-processors

The Controller gives general authorisation for the Processor to engage the sub-processors below. Each has agreed to data protection obligations no less protective than this DPA.

Sub-processors (22, list last changed 2026-09-26):

- Supabase: Primary database (Postgres), authentication, real-time, file storage. Location: India (AWS ap-south-1, Mumbai). Transfer: SCCs.
- Vercel: Application hosting, CDN, edge middleware. Location: India (Mumbai, bom1) + global CDN edge. Transfer: SCCs.
- Upstash: Redis cache (rate limits, sessions). Location: United States (AWS us-east-1). Transfer: DPF + SCCs.
- Anthropic: AI model inference. Location: United States. Transfer: DPF + SCCs.
- OpenAI: AI model inference (chat, summarization, routing). Location: United States. Transfer: DPF + SCCs.
- Google LLC (Gemini): AI model inference. Location: United States. Transfer: DPF + SCCs.
- Telnyx: Phone numbers, voice calls and SMS delivery. Location: United States. Transfer: SCCs.
- Fly.io: Hosting for the real-time voice servers. Location: United States (Ashburn, Virginia). Transfer: SCCs.
- Deepgram: Speech-to-text for voice calls. Location: United States. Transfer: SCCs.
- Cartesia: Text-to-speech for voice calls. Location: United States. Transfer: SCCs.
- Twilio: SMS and WhatsApp delivery. Location: United States. Transfer: DPF + SCCs.
- Meta Platforms (WhatsApp Business, Messenger, Instagram): Message routing for organisations that connect these channels. Location: United States + Ireland. Transfer: DPF + SCCs.
- Resend: Transactional email send and inbound email receive. Location: United States. Transfer: DPF + SCCs.
- Inngest: Background-job orchestration for AI auto-reply and workflows. Location: United States. Transfer: SCCs.
- Firebase (Google Cloud): Push notifications. Location: United States. Transfer: DPF + SCCs.
- Polar (Polar Software AB): Subscription billing. Location: EU / United States. Transfer: SCCs.
- Stripe: Payment processing for Corebee subscriptions. Location: United States + EU. Transfer: DPF + SCCs.
- PostHog (EU Cloud): Product analytics and session replay. Location: European Union (Frankfurt). Transfer: SCCs.
- Sentry: Error tracking. Location: United States. Transfer: DPF + SCCs.
- Firecrawl (Mendable): Crawling the website pages a customer imports into its knowledge base. Location: United States. Transfer: SCCs.
- Jina AI: Reading the website pages a customer imports into its knowledge base. Location: Vendor-managed (see its privacy policy). Transfer: SCCs.
- Cloudflare: DNS, DDoS protection, edge caching, browser rendering for knowledge-base imports. Location: Global edge. Transfer: DPF + SCCs.

"SCCs" means the Standard Contractual Clauses approved by the European Commission (Implementing Decision 2021/914), our primary transfer mechanism for personal data leaving the EEA, including to our hosting in India. "DPF" means the EU-U.S. Data Privacy Framework, relied on in addition where a US sub-processor has self-certified; it does not cover transfers to India.

Changes to sub-processors

Corebee will notify the Controller at least 30 days before adding or replacing a sub-processor, by email to the Controller's account address. The Controller may object on reasonable data protection grounds within 14 days. Corebee will then use reasonable efforts to offer a change that avoids the objected-to sub-processor; if none is reasonably available, either party may terminate the affected service by written notice.

8. Security Measures

The Processor implements technical and organisational measures appropriate to the risk, in line with Article 32 GDPR, including:

- Tenant isolation: Every customer workspace is isolated in the database with Postgres row-level security, and every server-side read is also filtered by the workspace it belongs to.
- Encryption in transit: TLS 1.2 or higher on every connection, with HSTS.
- Encryption at rest: AES-256 encryption at rest for the database and file storage (Supabase on AWS), plus AES-256-GCM application-layer encryption for integration tokens and credentials.
- Access control: role-based permissions for the Controller's team. Two-factor authentication (authenticator app) is available to every user in Settings, Security. Requiring it for a whole team is not available yet.
- Audit log: records settings changes, with the old and new value and who made them; conversation assignments and resolutions; data exports; messages sent by your team; actions the ai assistant proposed, ran or failed. Sign-in events are not recorded in it yet.
- Protection of server-side requests against forgery (SSRF), rate limiting, and DDoS protection through Cloudflare

SOC 2 readiness work is underway; Corebee is not SOC 2 certified and has no SOC 2 report yet. More detail: Security practices (https://corebee.ai/security) and the Trust center (https://corebee.ai/trust).

9. Data Subject Rights

The Processor assists the Controller in responding to data subject requests under Chapter III GDPR (access, rectification, erasure, portability, restriction and objection). It responds to requests forwarded by the Controller within 72 hours of receipt and completes the requested action without undue delay. A request received directly is passed to the Controller and not answered without the Controller's authorisation, unless the law requires otherwise.

10. Breach Notification

The Processor notifies the Controller of a personal data breach without undue delay and in any event within 72 hours of becoming aware of it (Article 33 GDPR). The notice describes the nature of the breach, the categories and approximate number of data subjects and records concerned, a contact point, the likely consequences, and the measures taken or proposed. The Processor cooperates with the Controller's investigation and remediation.

11. Data Retention

Conversations, transcripts and attachments are kept until you delete them, unless you set a retention window per company (30 days to 2 years) in the agency console. Until deletion is switched on, a window is a preview and nothing is deleted.

- Retention windows are set per company in the agency console: 30, 90, 180, 365 or 730 days after a conversation's last activity, or forever.
- A window starts in preview mode, which only reports what would be deleted. Deletion needs an agency administrator to switch it on for that company, with a typed confirmation.
- Records needed for billing reconciliation are held back from deletion and reported as held.
- The Controller may delete specific data at any time in the product or by contacting Corebee support.
- Encrypted backups are kept for up to 90 days on a rolling schedule, so deleted data leaves backups within that period.

12. International Data Transfers

Primary hosting location: Customer data is stored and processed primarily in Mumbai, India: the database runs on Supabase (AWS ap-south-1) and the application on Vercel (bom1). Other sub-processors in section 7 operate in the United States, the European Union or globally, as shown in the Location column.

India has no European Commission adequacy decision, so transfers to India and any onward transfer to the United States are third-country transfers under Chapter V GDPR. For transfers from the EEA, the UK or Switzerland we rely on:

- Standard Contractual Clauses (SCCs), our primary mechanism, including for our Indian hosting. A copy is available on request.
- The EU-U.S. Data Privacy Framework, in addition, where a US sub-processor has self-certified. It does not cover India.
- For the United Kingdom, the UK Addendum to the EU SCCs approved by the ICO.
- A transfer impact assessment covering the destination's laws and the safeguards in place (encryption, tenant isolation, access control), available on request.

13. Audit Rights

The Processor makes available the information needed to demonstrate compliance with this DPA and Article 28 GDPR, and allows for audits by the Controller or an auditor it mandates, with at least 30 days' written notice (unless a supervisory authority requires less), during business hours and under confidentiality. The Controller bears the cost unless the audit finds material non-compliance.

The Processor may answer audit requests with written responses to reasonable questionnaires and with independent reports once available. SOC 2 readiness work is underway; Corebee is not SOC 2 certified and has no SOC 2 report yet.

14. Termination and Data Deletion

When the service agreement ends, the Processor will, at the Controller's election, return all personal data in a structured, machine-readable format (JSON or CSV) or delete it, unless the law requires it to be kept.

After an account ends, we delete its data on written request within 30 days, and confirm in writing. The Controller should state its choice within 30 days of termination.

15. Processor Obligations

- Process personal data only on the Controller's documented instructions, unless the law requires otherwise (and then tell the Controller first, where allowed)
- Bind everyone authorised to process personal data to confidentiality
- Maintain the measures in section 8
- Engage sub-processors only as set out in section 7
- Assist the Controller with its obligations under Articles 32 to 36 GDPR
- Tell the Controller immediately if an instruction appears to infringe data protection law

16. Governing Law

This DPA is governed by the law that governs the service agreement. If this DPA and the service agreement conflict on the processing of personal data, this DPA prevails.

17. Contact

Questions about this DPA, DPA requests and audit requests: jonathan@corebee.ai.

Signatures

Processor

Company: Corebee Chat LTD

Name: _____

Title: _____

Date: _____

Signature: _____

Controller

Company: _____

Name: _____

Title: _____

Date: _____

Signature: _____