

Data Processing Agreement

For businesses using Tephlo to handle their customers' personal data. You decide what is processed and why; we process it on your instructions, and this document says exactly how.

Last updated 6 September 2026

Revision Draft 1.1 — factual content refresh

Version 2 · Effective 6 September 2026

TEPHLO AI ENTERPRISES

9A Kenneth Lekara Luka Street, Lokogoma, FCT, Nigeria

Tephlo · hello@tephlo.com

<https://legal.tephlo.com>

Exported from the published pages on 2026-10-02T17:17:50.686Z. The pages are the authoritative text.

IN PLAIN LANGUAGE

You are the controller of your customers' personal data. We are your processor. This document is the contract for that relationship.

- We process your customers' data only to run the service for you, and not for our own purposes. We do not use it to train AI models.
- Annex II lists the security measures that are actually implemented. Where a measure is organisational rather than technical, and we cannot verify it from the code, it is marked as a gap rather than claimed.
- The [sub-processor list](#) is part of this agreement. You are notified before a new one starts, and you can object.
- We tell you about a personal data breach without undue delay after becoming aware of it, and help you meet your own notification duties.
- On request or on termination we delete your data. Section 12 says exactly what that removes, what it does not, and what happens with backups.

1. Scope

This Data Processing Agreement ("DPA") forms part of the [Terms of Service](#) between TEPHLO AI ENTERPRISES ("Processor", "we") and the business operating a Tephlo workspace ("Controller", "you"). It applies to personal data we process on your behalf when you use the service, and takes effect on **[EFFECTIVE DATE]** or when you first accept the Terms, whichever is later.

Terms such as "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" carry the meanings given to them in the Nigeria Data Protection Act 2023. Where that law uses different labels, the equivalent concepts apply.

2. Roles of the parties

You are the controller of the personal data in your workspace: your customers' messages and identifiers, the knowledge you upload, and the configuration you set. We are the processor. Where you are yourself acting as a processor for someone else — an agency running a workspace for a client — we are a sub-processor, and your own controller's instructions reach us through you.

We are an independent controller for a narrow, separate set of data: the accounts of the people who administer your workspace, our billing and support records, and platform security and audit records. That processing is described in the [Privacy Policy](#), not here.

3. Processing on your instructions

We process personal data only on your documented instructions, including for international transfers, unless required otherwise by law — in which case we tell you before processing, unless that law forbids it.

Your instructions are:

- this DPA and the Terms of Service;

- your configuration of the service — the channels you connect, the knowledge you upload, the retention and privacy settings you choose, and the optional features you enable;
- your use of the console and the API, including exports and deletions you request;
- any further written instructions we agree with you.

We will tell you if, in our opinion, an instruction infringes applicable data protection law. We are not obliged to give you legal advice, and we may decline to act on an instruction that would put other customers or the platform at risk.

4. Our obligations

- **Purpose limitation.** We use your customers' personal data only to provide, secure and maintain the service for you. We do not sell it, do not use it for advertising, and do not use it to train AI models.
- **Confidentiality.** Access is limited to personnel who need it to operate the platform, under an obligation of confidentiality.
- **Security.** We implement the technical and organisational measures in Annex II, and will not materially weaken them during the term.
- **Assistance.** We assist you, taking into account the nature of the processing and the information available to us, with data subject requests (section 8), with breach notification (section 9), and with data protection impact assessments and prior consultations, for which this document and the [Security Overview](#) are the primary input.
- **Records.** We maintain records of the categories of processing carried out on your behalf, and make them available on request.

5. Your obligations

- You are responsible for having a lawful basis for the processing you instruct, and for telling your customers what happens to their data — including that an automated assistant answers them and that a person may take over.
- You configure retention, privacy settings and optional features. The defaults are documented; what applies to your workspace is what you set.
- You do not upload special categories of personal data (health, biometric, political, religious and similar) or children's data without a lawful basis and appropriate safeguards, and you keep your knowledge base free of personal data that does not need to be there.
- You keep your accounts secure and remove access promptly when someone leaves your team.

6. Security measures

Annex II lists the measures in force. They are described at a level a reviewer can check, and where a measure is organisational — personnel vetting, security training, formal policy review — it is marked as an open item rather than asserted, because this document should not be the first place such a claim appears.

No certification. We hold no SOC 2 report and no ISO 27001 certificate, and no independent auditor has assessed these measures. If your procurement process requires one, tell us before you sign rather than after.

7. Sub-processors

You give general authorisation for us to engage sub-processors. The current list, with the purpose, data categories and location of each, is published at [legal / sub-processors](#) and forms part of this DPA.

Before a new sub-processor starts processing your data, we will update that page and notify workspace administrators by email, giving **[SUB-PROCESSOR NOTICE PERIOD]** notice. If you reasonably object on data protection grounds within that period, we will work with you on an alternative; if none is available, you may terminate the affected part of the service without penalty for the remainder of the term.

We impose data protection obligations on each sub-processor that are no less protective than those in this DPA, and remain responsible to you for their performance.

One nuance about messaging providers. Where you connect your own WhatsApp Business account or Telegram bot, that provider is processing under your own relationship with them, not as our sub-processor. Where you use a number the platform shares, our relationship with the provider applies. Both cases are marked on the sub-processor page.

8. Data subject requests

The service gives your administrators the tools to answer most requests without involving us:

- **Access and portability.** An export produces a structured record of one customer's data with your workspace — conversations, the full transcript, escalations, sessions on shared numbers, routing records, memberships, remembered facts, tickets and care cases, customer-scoped cached answers, Smart Updates consent and send history, carts, potential-order requests and appointments. Review excerpts are represented by metadata; their message text is already disclosed in the transcript.
- **Erasure.** A deletion permanently removes that customer's conversations and messages, escalations, transcripts of media in those conversations, sessions, routing records, memberships, queued outbound messages and in-flight processing records, and clears their short-lived working state. Anything already accepted for processing before the deletion is suppressed rather than delivered afterwards.
- **Rectification and restriction.** Handled by editing or removing the underlying records in the console.

Every export and deletion is recorded in an audit trail that identifies the subject by a salted hash rather than by their identifier, so the audit itself does not recreate the data you just erased.

Scope of the per-customer erasure. It removes the conversations and messages, the escalations raised from them, the routing, session and membership records, queued deliveries, the entries stored by the customer-memory feature, and the tickets captured for your team with

their summaries, care cases, customer-scoped cached answers, review excerpts, Smart Updates consent and send records, carts, potential-order requests and appointments. Related operational rows and withheld reply drafts are erased but are not all separately disclosed in an export. The deletion audit itself is retained, identifying the subject only by a salted hash, so that the erasure can be evidenced without recreating what it removed.

If a data subject contacts us directly about your workspace, we will not respond substantively — we will refer them to you and tell you promptly.

9. Personal data breaches

We notify you without undue delay after becoming aware of a personal data breach affecting personal data we process for you. The notice will describe, as far as we know at the time: the nature of the breach and the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point. Where the full picture is not available immediately, we send what we have and follow up as we learn more, rather than delaying the first notice.

We will assist you with your own notification obligations to a supervisory authority or to affected individuals. Notifying us of a breach in your own systems, or a compromised staff account, is your responsibility — write to hello@tephlo.com.

10. Audit and information

On request, and no more than once a year unless a supervisory authority or a breach requires otherwise, we will provide the information reasonably necessary to demonstrate compliance with this DPA: this document, the [Security Overview](#), our answers to a reasonable security questionnaire, and a description of any material change to the measures in Annex II.

Because there is no third-party certification to hand you instead, an on-site or third-party audit is available on the terms in **[AUDIT TERMS]** — scope, notice, confidentiality and costs to be agreed. We will not give access to another customer's data or to anything that would compromise the security of the platform.

11. International transfers

The service is delivered using providers that operate internationally, and the AI provider may route a request to a model provider in another country. Personal data will therefore be transferred across borders.

The transfer mechanism relied on for each sub-processor is **[TRANSFER MECHANISM]**, to be confirmed by counsel before this document is used as a signed agreement. We will not claim a mechanism is in place before it is.

12. Deletion and return of data

You can export your data at any time during the term through the console and the API. On termination, or on your written request, we delete the personal data we process for you.

Deleting a workspace removes:

- conversations, messages, escalations and captured tickets;
- knowledge sources and their indexed chunks, the product catalogue, remembered customer facts, care cases, Smart Updates records, carts, potential-order requests and appointments;
- channel configuration and encrypted credentials, staff accounts and their credential records, invites and pending signups;
- uploaded media and extracted text, including the files themselves in object storage, removed by a cleanup job that commits together with the deletion; physical removal depends on that worker and the storage provider succeeding;
- usage records, analytics rows, email delivery records for the workspace, and queued work belonging to it.

Two categories survive, deliberately:

- **Platform audit records** showing that administrative actions took place — a deletion, a credential change, a routing change — with the actor and the stated reason. They contain no message content, and two of these tables are protected against modification by the database itself.
- **Encrypted backups**, which are not edited individually. Deleted data leaves the backup set as backups are pruned on their schedule. Until then it remains encrypted and is restored only in a disaster, after which the deletion is reapplied.

Unless you instruct otherwise, a terminated workspace is deleted within **[POST - TERMINATION RETENTION PERIOD]**, so a mistaken termination can be undone. We will confirm the deletion in writing on request.

13. General

This DPA runs for as long as we process personal data for you. If it conflicts with the Terms of Service on the treatment of personal data, this DPA prevails. Liability under this DPA is subject to the limitations in the Terms. If a provision is held invalid, the rest remains in force, and the parties will agree a valid replacement with equivalent effect.

Annex I — Details of the processing

Subject matter

Provision of an AI customer-support assistant and agent console across WhatsApp, Telegram, web chat and enabled commercial API integrations.

Duration

The term of the Terms of Service, plus the deletion window in section 12.

Nature and purpose

Receiving and storing customer messages; retrieving relevant passages from your knowledge base; generating replies through an AI provider; routing conversations to your team; capturing requests such as callbacks and complaints; managing saved carts, potential-order requests and appointments; producing analytics for you; and, where permitted by the relevant controls, interpreting images, transcribing voice notes, reading documents, generating spoken replies and

remembering stated customer preferences. Smart Updates records topic consent and preferences and sends eligible approved updates.

Categories of data subjects

The customers and prospective customers who message your workspace, and any individuals they mention in a message.

Categories of personal data

Channel identifiers (a phone number on WhatsApp, a user id on Telegram, a randomly generated visitor id in web chat, or the identifier supplied by an API integration); the content of messages sent and received, which may contain anything a customer chooses to write; conversation and escalation metadata; captured request summaries and care-case records; stated preferences where customer memory is allowed; Smart Updates consent and send history; saved-cart selections and price snapshots, potential-order requests and appointment details; transcripts, images, extracted document text and spoken reply content where the relevant features are enabled.

Special categories

Not intended. The service is not designed for them and you agree not to instruct their processing without a lawful basis and safeguards. A customer may nonetheless volunteer such information in a free-text message; the platform treats it as ordinary message content.

Frequency

Continuous, for as long as your channels are live.

Annex II — Technical and organisational measures

These are implemented in the platform today. The [Security Overview](#) explains each in plain language.

1. **Workspace isolation.** Workspace records carry their ownership, and access is checked against the authenticated principal or authorised channel/API configuration. Supplying a record identifier does not itself grant access to it. Conversations are keyed by workspace, channel, receiving identity and customer.
2. **Access control.** Role-based permissions; authorisation re-checked against the database on every request, so a disabled account, a changed role or a suspended workspace takes effect immediately; short-lived access tokens; refresh tokens that rotate and whose whole family is revoked if an old one is replayed; account lockout after repeated failures.
3. **Multi-factor authentication.** Enforced for platform operator accounts in production and available to your administrators; the authenticator secret is stored encrypted.
4. **Encryption in transit.** HTTPS throughout; production configuration refuses to start with a non-HTTPS provider endpoint, requires TLS to the cache, and requires an encrypted connection to a managed database.
5. **Encryption at rest.** Channel credentials, authenticator secrets, invite payloads, email bodies, staged uploads, media job payloads and extracted document text are encrypted with authenticated symmetric encryption; supported key rings allow staged key rotation. Passwords are stored only as hashes, not in readable form.

6. **Message authenticity.** Inbound WhatsApp webhooks are verified by HMAC signature over the original request body. Activation and health controls depend on the channel and its ownership; a single send failure does not automatically disable a platform-shared channel.
7. **Log hygiene.** Email addresses, phone numbers, URLs, tokens, signatures and stack traces are redacted at the logging boundary. Audit and analytics records store categories and counts, never message content.
8. **Audit trails.** Administrative actions — credential changes, routing changes, privacy exports and deletions, platform configuration — are recorded with the actor, target and stated reason. Two audit tables are append-only at the database level: an update or delete is rejected by the database, not merely by the application.
9. **File safety.** Documents a customer sends are scanned for malware before anything opens the bytes, and the scan fails closed — no scanner means no parsing. Executables, archives, macro-enabled documents, encrypted files and PDFs containing active content are rejected outright; extraction runs under hard bounds; infected files are deleted unparsed and can never be downloaded through the application.
10. **Private storage.** Uploaded media is stored under opaque, backend-generated keys partitioned per workspace, with no public access and no pre-signed links; customer filenames never appear in storage keys.
11. **Sensitive-data minimisation.** The assistant refuses to request payment instruments, credentials, bank details and government identity numbers, in English, French and Spanish. Text kept for optional quality review is masked for emails, phone numbers, long numbers and labelled codes before storage.
12. **Resilience.** Work is staged in a durable outbox with retries, backoff and a dead-letter queue; duplicate deliveries are collapsed; failing providers are isolated by circuit breakers so one outage does not cascade.
13. **Backups and recovery.** An encrypted backup procedure, restore procedure and integrity checks are documented. Their operation, schedule and key management must be confirmed for the deployment.
14. **Data lifecycle.** Time-limited caches and working state, per-customer erasure and workspace deletion. Current memory extraction sets a 180-day expiry; expired facts are excluded on read. Physical removal by retention sweeps or object-storage cleanup depends on the relevant worker being enabled and running.
15. **Change management.** Version-controlled code and database migrations, automated checks on every change (linting, type checking, tests, migration checks), and staged rollout of risky features behind flags that default to off.
16. **Organisational measures.** Personnel confidentiality undertakings, background checks, security training, formal policy review and an incident response plan owned by a named person: **[ORGANISATIONAL MEASURES TO BE CONFIRMED]**. These are not claimed here until the company can evidence them.

Contact

General questions about this document go to hello@tephlo.com. Questions about personal data, including requests from individuals, should go to the data protection contact at **[DATA PROTECTION CONTACT]**; until that address is published, the general address above reaches the same team. A

request about your own data — access, erasure, correction, objection or a complaint — can also be sent through the [privacy request form](#), which puts it in front of the team as a tracked request rather than a message in a mailbox.

Postal address: **[REGISTERED COMPANY NAME], [REGISTERED ADDRESS]**.