DATA PROCESSING AGREEMENT

Protokol | Version 2026-06-01

This Data Processing Agreement ("DPA") is between the customer identified in the Protokol account ("Controller") and Y. VERTA HOLDINGS LTD (company no. 516052958), trading as Protokol ("Processor"). It forms part of the Protokol Terms of Service.

§1. Definitions

"GDPR" means the UK General Data Protection Regulation and, where applicable, the EU GDPR (Regulation (EU) 2016/679). "Personal Data", "Data Subject", "Processing", "Controller", "Processor", and "Supervisory Authority" have the meanings given in Article 4 of the GDPR. "Sub-processor" means any third-party processor engaged by the Processor to carry out Processing on behalf of the Controller.

§2. Subject Matter and Duration

The Processor processes Personal Data solely to deliver the Services: joining, recording, transcribing, and analysing meetings; extracting compliance answers; drafting recap emails; and filing outputs to connected third-party services as instructed by the Controller. Processing continues for the duration of the active subscription and for up to 90 days thereafter, unless earlier deletion is requested.

§3. Obligations of the Processor

- Process Personal Data only on documented instructions from the Controller.
- Ensure authorised persons are subject to a binding duty of confidentiality.
- Implement appropriate technical and organisational measures (Article 32 GDPR) — see Annex III.
- Assist the Controller in responding to Data Subject rights requests (Chapter III GDPR).
- Assist the Controller in ensuring compliance with Articles 32-36 GDPR.
- At the choice of the Controller, delete or return Personal Data after end of Services.
- Allow for and contribute to audits by the Controller on 30 days written notice.
- Notify the Controller of any Personal Data breach within 72 hours of becoming aware.

§4. Sub-processors

General authorisation is granted under Article 28(2) GDPR to engage the sub-processors listed below. The Processor will notify the Controller at least 30 days before adding or replacing any sub-processor, giving opportunity to object.

Sub-processor	Purpose	Region
Google	Calendar & Drive integration; Gemini AI transcription/analysis	EU / US
Microsoft	Outlook calendar & Teams integration	EU / US
Supabase	Database, auth & file storage	EU (eu-central-1)
Brevo	Transactional email (recaps)	EU
Paddle	Payments (merchant of record)	EU / US
Hetzner	Meeting-bot server hosting	EU (Germany)
Vercel	Dashboard hosting & CDN	Global edge

§5. International Transfers

Where Personal Data is transferred outside the UK or EEA, the Processor ensures appropriate safeguards including UK-approved SCCs or the UK International Data Transfer Addendum. Primary storage is in EU (eu-central-1). Sub-processor transfers are subject to equivalent SCCs, available on request.

§6. Liability and Indemnification

Each party's liability is subject to the Terms of Service limitations. The Processor's aggregate liability for DPA breaches shall not exceed fees paid in the 12 months preceding the claim.

§7. Governing Law

This DPA is governed by the laws of England and Wales. The parties submit to the exclusive jurisdiction of English courts,

without prejudice to data subjects' rights before any Supervisory Authority.

Annex I: Parties

Controller: The individual or organisation identified in the Protokol account.

Processor: Y. VERTA HOLDINGS LTD (company no. 516052958), trading as Protokol. Contact: support@getprotokol.app.

Annex II: Description of Processing

- Data Subjects: advisers/professionals (account holders); their clients; meeting participants.
- Personal Data: audio recordings; transcripts; speaker labels; calendar metadata; compliance answers; name and email.
- Purpose: AI-powered meeting intelligence — transcription, summarisation, compliance-answer extraction, follow-up drafting, and filing.
- Duration: Subscription term + 90 days post-termination (or earlier deletion on request).

Annex III: Technical and Organisational Measures

- Encryption in transit: All data transmitted over TLS 1.2+. HTTPS enforced.
- Encryption at rest: AES-256 via Supabase (AWS eu-central-1).
- Data residency: Primary database and file storage in EU (eu-central-1, Frankfurt).
- Access controls: Row-Level Security (RLS) at database layer; service-role keys never exposed to browser.
- Audit logging: Append-only audit trail; records cannot be modified by application code.
- Personnel: Production data access limited to authorised personnel on need-to-know basis; all subject to confidentiality.
- Incident response: Personal Data breach notification within 72 hours of becoming aware (Article 33 GDPR).
- Vulnerability management: Dependencies regularly reviewed; security patches applied on risk-prioritised basis.

Agreed on behalf of the Controller:

Signature / Date

Agreed on behalf of the Processor:

Y. VERTA HOLDINGS LTD / Date