Data Processing Addendum

Version 2026-07-21 | Effective July 21, 2026

SHA-256 content hash: a85586510186a3f52d7074175fd66f40a29df51a1a66a4aa61aee06645937af0

This Data Processing Addendum forms part of the Eloquend Terms of Service when a Business User acts as a controller or processor and asks Eloquend to process personal data on its or a client's behalf.

It is designed to meet GDPR and UK GDPR processor-contract requirements without changing the parties' roles for data Eloquend processes for its own account, security, billing, or legal purposes.

Automatic application

No separate signature is needed when a Business User uses Eloquend as its processor or subprocessor.

Documented instructions

The Terms, product configuration, user actions, and lawful written requests are the customer's documented instructions.

Approved subprocessors

Eloquend may use the listed infrastructure, AI, security, and email providers subject to appropriate processor terms.

Deletion and assistance

Eloquend supports rights requests, incidents, assessments, and deletion in proportion to the processing and available information.

1. Parties, scope, and definitions

This Data Processing Addendum ("DPA") is between the Business User that accepted the Eloquend Terms of Service ("Customer") and Boostify, CVR 44697327, c/o Christian Nymark Jensen, Vestre Alle 1, 4. th, 9000 Aalborg, Denmark ("Eloquend"). Telephone: +45 61 61 67 61, Monday–Friday, 09:00–16:00 Danish time (CET/CEST), excluding Danish public holidays, with voicemail outside those hours. This DPA applies only when Eloquend processes Customer Personal Data as Customer's processor or subprocessor.

"Customer Personal Data" means personal data contained in Inputs, Content, files, audio, client material, or other data submitted by or for Customer that Eloquend processes on Customer's behalf. "Data Protection Law" means the EU GDPR, UK GDPR, Danish data-protection law, and other personal-data law applicable to that processing. The terms controller, processor, data subject, personal data, processing, personal data breach, and supervisory authority have the meanings in applicable Data Protection Law.

This DPA does not apply where Eloquend acts as an independent controller, including for Account administration, security, fraud prevention, billing, legal compliance, service communications, and product analytics as described in the Privacy Policy. LinkedIn, Stripe, Google, and other third parties may act independently under their own terms for processing directly controlled by them.

Where Customer is a controller, Eloquend is its processor. Where Customer is a processor for another controller, Eloquend is Customer's subprocessor. A Customer acting as processor confirms that the relevant controller has authorized Customer to appoint Eloquend and the listed subprocessors, and that Customer may give the instructions in the Terms and this DPA. Customer remains the contact point for that controller unless law or a written agreement requires otherwise.

2. Processing details and instructions

Item	Details
Subject and duration	Providing Eloquend during the Account relationship and applicable deletion, backup, legal-hold, or return period.

Item	Details
Nature and purpose	Receiving, hosting, organizing, generating, editing, transcribing, formatting, exporting, securing, and transmitting Customer Content as configured and instructed.
Data subjects	Customer personnel, clients, prospects, professional contacts, people mentioned in Content, and other individuals whose data Customer submits.
Personal data	Names, professional details, contact information, profile and writing preferences, correspondence, voice, image or likeness, opinions, draft and published Content, and technical data Customer submits.
Sensitive data	The Service is not designed for special-category data, government identifiers, financial credentials, children's data, or similarly sensitive data, and Customer must not submit it unless Eloquend has expressly agreed in writing.

Customer instructs Eloquend to process Customer Personal Data to provide, secure, support, and maintain the configured Service, including through approved subprocessors. The Terms, this DPA, Account configuration, user actions, and lawful written requests are Customer's documented instructions. Eloquend will notify Customer if, in its reasonable opinion, an instruction infringes Data Protection Law, unless law prohibits notice. Eloquend may suspend the affected processing while the parties resolve the concern.

3. Customer obligations

- If Customer is a controller, Customer determines the purposes and essential means and is responsible for its instructions, legal basis, transparency, data-subject rights, data accuracy, retention choices, and use of Outputs. If Customer is a processor, it will process and instruct Eloquend only within the authority and documented instructions of the relevant controller.
- Customer will submit only personal data reasonably needed for its use of Eloquend and will not submit prohibited sensitive data or children's data.
- Customer will ensure that authorized users, clients, and data subjects receive required notices and that Customer has the rights and permissions needed for Eloquend and its subprocessors to process the data.
- A Customer acting as processor will promptly pass relevant requests, notices, incidents, and compliance information between Eloquend and the controller and will not give Eloquend an instruction that exceeds the controller's authorization.
- Customer will use available Account controls, access restrictions, exports, deletion tools, and human review appropriate to the nature and risk of its processing.

4. Eloquend processor obligations

- Process Customer Personal Data only on documented instructions, unless applicable law requires other processing; where permitted, Eloquend will tell Customer before that processing.
- Ensure persons authorized to process Customer Personal Data are bound by confidentiality and receive appropriate data-protection and security direction.
- Implement and maintain technical and organizational measures appropriate to the risk and the nature of the Service.
- Taking into account the nature of processing, assist Customer through available product controls and reasonable additional measures with data-subject requests, security, breach obligations, impact assessments, and regulator consultations.
- Make information reasonably necessary to demonstrate compliance with this DPA available to Customer, subject to confidentiality, security, privilege, and proportionality.

5. Security measures

Eloquend's measures include, as appropriate to the relevant system: encrypted transport; managed encryption at rest; restricted service-role and production access; hashed or protected authentication credentials; server-restricted OAuth tokens; row-level authorization; separation of public and private storage; logging that avoids Content where practicable; dependency and vulnerability management; backups and recovery controls; rate limiting; incident handling; and processor due diligence.

Security is a shared responsibility. Customer is responsible for authorized-user access, strong credentials, endpoint security, appropriate Content, and promptly revoking access that is no longer needed. Eloquend may update measures as technology and risks evolve, provided the overall protection is not materially reduced during a Subscription without a valid reason and appropriate notice.

6. Subprocessors

Customer gives general written authorization for Eloquend to use the subprocessors below. Eloquend will require each subprocessor to protect Customer Personal Data through written obligations materially consistent with the applicable requirements of this DPA. Eloquend remains responsible for its subprocessor's performance to the extent required by Data Protection Law.

Provider and contact	Service, data, and purpose	Principal location and transfer safeguard	Retention control
Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513; privacy@supabase.io; DPA and subprocessor terms	Authentication, Account and Content database records, private object storage, backend functions, backups, and related infrastructure.	Production database and storage in the EEA region selected for Eloquend; limited global support and subprocessors. Adequacy, EU–U.S. Data Privacy Framework where applicable, and SCC Modules Two or Three as appropriate.	Account lifecycle, deletion workflows, and protected backup rotation; product-specific periods are listed in the Privacy Policy.
Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, United States; privacy@vercel.com; DPA and subprocessor terms	Application hosting, server functions, request handling, transient country-code derivation, deployment diagnostics, and AI Gateway routing. Content and technical request data are involved only as needed to provide those services.	EEA, United States, and global edge locations. EU–U.S. Data Privacy Framework where applicable and SCC Modules Two or Three as appropriate.	Pro runtime logs up to 1 day; no extended observability retention or log drain. AI Gateway prompt and output content is deleted after each request under ZDR.
Anthropic PBC, 548 Market Street, PMB 90375, San Francisco, CA 94104, United States; privacy@anthropic.com; commercial privacy terms	Primary Claude text generation through Vercel AI Gateway; prompt, limited relevant context, generated output, and technical request metadata.	United States and approved provider infrastructure. Vercel-negotiated ZDR terms and applicable adequacy or SCC Module Three safeguards.	ZDR: no prompt or output content retention after the request; no prompt training or prompt caching.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, United States, and the applicable Microsoft affiliate identified in the incorporated provider terms; privacy contact; data-protection terms	Fallback GPT text generation through the Azure provider in Vercel AI Gateway; prompt, limited relevant context, generated output, and technical request metadata.	Microsoft Azure infrastructure selected through AI Gateway. Vercel-negotiated ZDR terms and applicable EU–U.S. Data Privacy Framework or SCC Module Three safeguards.	ZDR: no prompt or output content retention after the request; no prompt training or prompt caching.

Provider and contact	Service, data, and purpose	Principal location and transfer safeguard	Retention control
OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland; privacy@openai.com; DPA and subprocessor terms	Direct image generation and voice transcription; image prompts and outputs, voice audio, transcripts returned in the response, and technical request metadata.	EEA, United States, and provider subprocessors. EEA processing where available; adequacy, EU–U.S. Data Privacy Framework where applicable, and SCC Module Three for restricted onward transfers.	Images: up to 30 days for abuse monitoring, subject to documented safety or legal exceptions. Transcription endpoint: no application-state or abuse-monitoring content retention under current controls.
Plus Five Five, Inc. d/b/a Resend, 2261 Market Street #5039, San Francisco, CA 94114, United States; privacy@resend.com; DPA and subprocessor terms	Transactional email delivery and diagnostics; recipient address, message content, delivery status, and technical metadata.	United States and listed subprocessors; applicable EU–U.S. Data Privacy Framework and SCC Module Three safeguards.	Delivery diagnostics up to 90 days; message and provider retention otherwise follow the applicable Resend service controls.
Functional Software, Inc. d/b/a Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105, United States; legal@sentry.io; DPA and subprocessor terms	Sanitized application error monitoring and diagnostics; technical error, release, route, and performance context with default PII and replay disabled.	Germany project region with limited approved global support and subprocessors; EU–U.S. Data Privacy Framework where applicable and SCC Module Three.	Up to 30 days under the configured Developer plan.
PostHog, Inc., 2261 Market Street #4008, San Francisco, CA 94114, United States; privacy@posthog.com; DPA; subprocessor register	Minimized EU Cloud product analytics: sanitized browser events and limited account-linked events. No prompts, Content, names, email addresses, or full URLs.	EU Cloud with limited approved United States access and subprocessors; EU–U.S. Data Privacy Framework where applicable and SCC Module Three.	Less than 12 months through annual whole-project rotation, with earlier account-linked deletion where applicable. No processing for United Kingdom or unclassified production traffic.

Eloquend will give at least 14 days' advance notice by Account email or another durable legal notice before a new subprocessor materially processes Customer Personal Data. Customer may object on reasonable data-protection grounds during that period. The parties will try in good faith to resolve the objection through safeguards or a reasonable alternative. If no reasonable alternative is available, Customer may stop the affected processing or terminate the affected Subscription and receive a refund of unused prepaid fees.

7. International transfers

Processing by Eloquend in Denmark of Customer Personal Data received from a Customer in the EEA is not, by itself, a restricted transfer under GDPR Chapter V. Eloquend may use approved subprocessors in the EEA, United States, and other listed locations. For an onward restricted transfer, Eloquend will use an adequacy decision, the EU–U.S. Data Privacy Framework where applicable, or the European Commission Standard Contractual Clauses. Module Three applies where Eloquend transfers Customer Personal Data as processor to a subprocessor.

If a restricted transfer directly from Customer to Eloquend requires Standard Contractual Clauses, Module Two applies when Customer is controller and Eloquend is processor; Module Three applies when Customer is processor and Eloquend is subprocessor. A separate controller-to-controller transfer involving Eloquend as an independent controller is outside this DPA and would use Module One where required. The UK International Data Transfer Addendum applies only to a restricted transfer governed by UK Data Protection Law.

For any clauses incorporated directly between Customer and Eloquend, the exporter and importer roles follow the actual transfer rather than being fixed by this DPA; Clause 7 applies; Clause 9 uses Option 2 and the 14-day notice period above; the optional wording in Clause 11 does not apply; Danish law and competent Danish courts apply where the clauses permit; and Datatilsynet is the competent supervisory authority where GDPR permits. The parties and contact details above complete Annex I.A, “Processing details and instructions” completes Annex I.B, applicable law determines Annex I.C, “Security measures” completes Annex II, and the subprocessor table completes Annex III. Eloquend will apply supplementary technical, contractual, or organizational measures where reasonably required and provide available information reasonably needed for Customer’s transfer assessment, subject to security and confidentiality limits.

8. Personal data breaches and data-subject rights

Eloquend will notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. The notice will include information reasonably available about the nature of the breach, likely consequences, affected data and people, mitigation, and a contact point. Initial information may be provided in phases. Notice is not an admission of fault or liability.

If Eloquend receives a request from a data subject concerning Customer Personal Data, it will ordinarily direct the person to Customer and will not respond on Customer’s behalf unless instructed or legally required. Taking into account the nature of processing, Eloquend will support Customer through available search, export, correction, disconnection, and deletion functions and reasonable additional assistance. Customer is responsible for verifying the requester and determining the legally required response.

9. Return, deletion, and audits

During the Account relationship, Customer may use Eloquend’s export and deletion controls. At the end of the Service, Eloquend will delete or return Customer Personal Data at Customer’s choice where required, unless applicable law requires retention. Deletion from protected backups occurs as backups rotate; retained copies remain protected and are not used for ordinary business purposes.

Customer may request compliance information no more than once per year unless a personal data breach, regulator request, or substantiated compliance concern justifies more frequent review. Eloquend will first provide reasonably available third-party reports, certifications, written questionnaires, policies, or summaries. If those materials are insufficient and an audit is reasonably necessary to demonstrate compliance, Customer or an independent auditor that is not a competitor may conduct a proportionate remote, on-site, or technical audit. An audit requires reasonable advance notice, occurs during normal business hours, is limited to relevant systems and evidence, follows Eloquend’s security and confidentiality requirements, and must not expose another customer’s data or privileged material. Customer bears ordinary audit costs unless the audit establishes Eloquend’s material breach of this DPA, in which case Eloquend bears its own costs and Customer’s reasonable external audit costs.

10. Priority, liability, duration, and contact

This DPA begins when it applies under the Terms and continues while Eloquend processes Customer Personal Data. If it conflicts with the Terms on processor obligations, this DPA controls. The Terms’ liability provisions apply to this DPA except where Data Protection Law prohibits that result; neither document limits regulator powers, administrative fines, or data-subject rights.

The governing law and dispute terms in the Terms apply. Questions, instructions, or subprocessor objections may be sent to support@eloquend.com; formal legal notices should also be copied to chris@eloquend.com. You may also call +45 61 61 67 61 Monday–Friday, 09:00–16:00 Danish time (CET/CEST), excluding Danish public holidays. Voicemail is available outside those hours.