Data Processing Addendum

Version 2026-09-08 | Effective September 8, 2026

SHA-256 content hash: 1672356057498bad007b66fc2178459228b4799c673ebc82cc6de63779501ea0

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 processor-contract requirements without changing the parties' roles for data Eloquend processes for its own account, security, billing, or legal purposes.

1. Parties, scope, and definitions

1.1 **Parties.** 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.

1.2 **Definitions.** "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, 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.

1.3 **What this DPA does not cover.** 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.

1.4 **Roles.** 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

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

2.2 **Nature and purpose.** Receiving, hosting, organizing, generating, editing, transcribing, formatting, exporting, securing, and transmitting Customer Content as configured and instructed.

2.3 **Data subjects.** Customer personnel, clients, prospects, professional contacts, people mentioned in Content, and other individuals whose data Customer submits.

2.4 **Categories of 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.

2.5 **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.

2.6 **Documented instructions.** 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

3.1 **Role and responsibility.** 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.

3.2 **Data minimization.** Customer will submit only personal data reasonably needed for its use of Eloquend and will not submit prohibited sensitive data or children's data.

3.3 **Notices and permissions.** 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.

3.4 **Passing information through.** 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.

3.5 **Using the available controls.** 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

4.1 **Instructions only.** Process Customer Personal Data only on documented instructions, unless applicable law requires other processing; where permitted, Eloquend will tell Customer before that processing.

4.2 **No sale, and no AI training.** Not sell Customer Personal Data, and not use it to train or improve any artificial-intelligence model, whether Eloquend's own or a provider's. Eloquend requires its AI subprocessors to do the same: every text and image request disallows provider training and asks for Zero Data Retention, so the provider retains no prompt or output content once the request completes.

4.3 **Confidentiality.** Ensure persons authorized to process Customer Personal Data are bound by confidentiality and receive appropriate data-protection and security direction.

4.4 **Security measures.** Implement and maintain technical and organizational measures appropriate to the risk and the nature of the Service.

4.5 **Assistance.** 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.

4.6 **Demonstrating compliance.** Make information reasonably necessary to demonstrate compliance with this DPA available to Customer, subject to confidentiality, security, privilege, and proportionality.

5. Security measures

5.1 **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; off-site backups encrypted before they leave the Service, so the backup provider holds ciphertext and no key; rate limiting; incident handling; and processor due diligence.

5.2 **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.

6.1 **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. Located in the United States for the production database and object storage (AWS us-east-1), with limited global support and subprocessors, under the EU–U.S. Data Privacy Framework where applicable and SCC Module Three. Retention follows the Account lifecycle, deletion workflows, and protected backup rotation; product-specific periods are listed in the Privacy Policy.

6.2 **Cloudflare, Inc.** 101 Townsend St., San Francisco, CA 94107, United States; privacyquestions@cloudflare.com; DPA and subprocessor terms. Off-site backup storage (R2). Holds a nightly encrypted copy of the database and of stored objects so a failure at Supabase is recoverable. File contents and file names are encrypted before they are sent and Cloudflare holds no decryption key; the folder structure, which carries only bucket and account identifiers, remains visible to it. Located in the United States (R2 Eastern North America location hint), under the EU–U.S. Data Privacy Framework where applicable and SCC Module Three. Database copies expire after 30 days; copies of objects deleted or replaced in the Service expire after 90 days. The current-state mirror follows the Service, so deleting Content removes it from the mirror at the next nightly run.

6.3 **GitHub, Inc.** 88 Colin P. Kelly Jr. St., San Francisco, CA 94107, United States; privacy@github.com; DPA and subprocessor terms. Runs the nightly backup job. Customer Personal Data passes through the runner in transit while it is read from Supabase, encrypted, and written to backup storage; nothing is retained after the job ends. Located in the United States on GitHub-hosted runner infrastructure, under the EU–U.S. Data Privacy Framework where applicable and SCC Module Three. No retention: the runner is destroyed when the job finishes, and job logs record object counts and paths, never Content.

6.4 **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. Located in the EEA, the United States, and global edge locations, under the EU–U.S. Data Privacy Framework where applicable and SCC Modules Two or Three as appropriate. Runtime logs are kept up to 1 day with no extended observability retention or log drain, and AI Gateway text and image prompt and output content is deleted after each request under Zero Data Retention.

6.5 **Anthropic PBC.** 548 Market Street, PMB 90375, San Francisco, CA 94104, United States; privacy@anthropic.com; commercial privacy terms. Claude text generation through Vercel AI Gateway, receiving the prompt, limited relevant context, generated output, and technical request metadata. Which approved provider serves a given feature, and in which order, is a routing decision that changes without changing this list. Located in the United States and approved provider infrastructure, under Vercel-negotiated Zero Data Retention ("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.

6.6 **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. GPT text generation through the Azure provider in Vercel AI Gateway, receiving the prompt, limited relevant context, generated output, and technical request metadata. Which approved provider serves a given feature, and in which order, is a routing decision that changes without changing this list. Located on Microsoft Azure infrastructure selected through AI Gateway, under 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.

6.7 **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. Image generation through Vercel AI Gateway, and voice transcription reached directly, receiving image prompts and outputs, voice audio, transcripts returned in the response, and technical request metadata. Located in the EEA, the United States, and provider subprocessors, with EEA processing where available, and adequacy, the EU–U.S. Data Privacy Framework where applicable, and SCC Module Three for restricted onward transfers. Images: no prompt or output content retention after the request under the gateway's ZDR terms, and no route reaches this subprocessor for images outside the gateway. Transcription endpoint: no application-state or abuse-monitoring content retention under current controls.

6.8 **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, receiving the recipient address, message content, delivery status, and technical metadata. Located in the United States with listed subprocessors, under applicable EU–U.S. Data Privacy Framework and SCC Module Three safeguards. Delivery diagnostics are kept up to 90 days; message and provider retention otherwise follow the applicable Resend service controls.

6.9 **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, receiving technical error, release, route, and performance context with default PII and replay disabled. Located in a Germany project region with limited approved global support and subprocessors, under the EU–U.S. Data Privacy Framework where applicable and SCC Module Three. Retained up to 30 days under the configured Developer plan.

6.10 **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, with no prompts, Content, names, email addresses, or full URLs. Located on EU Cloud with limited approved United States access and subprocessors, under the EU–U.S. Data Privacy Framework where applicable and SCC Module Three. Retained up to 12 months under the retention period PostHog applies to our plan, which Eloquend cannot extend; account-linked identifiers and events are also deleted through the account-deletion workflow, and there is no processing for United Kingdom or unclassified production traffic.

6.11 **Adding a subprocessor.** Before a new subprocessor begins processing Customer Personal Data, Eloquend records it in the change log below with the date it takes effect, and emails the address on each Business User's Account. Both happen at least 14 days before that date. Until it arrives the provider is listed only in the change log, never in the list above, which always describes the subprocessors in use today.

6.12 **Objecting.** 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.

6.13 **Change log.** Cloudflare and GitHub added, announced September 6, 2026, effective immediately as a correction to the list. This was a correction rather than a new arrangement: both have processed Customer Personal Data as part of the nightly off-site backup since August 18, 2026, and earlier versions of this list omitted them. The backup was also changed so that stored objects are encrypted before they reach Cloudflare, which previously received them unencrypted.

7. International transfers

7.1 **Transfer mechanisms.** 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.

7.2 **Which module applies.** 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.

7.3 **Clause options and annexes.** 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 list 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

8.1 **Breach notification.** 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.

8.2 **Data-subject requests.** 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

9.1 **Return and deletion.** 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.

9.2 **Audits.** 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

10.1 **Duration and priority.** 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.

10.2 **Governing law and contact.** 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.