Data processing agreement

Effective 1 November 2026

This is a translation. The Danish version is the one that applies.

1. Parties and background

This agreement applies between you as a customer of Striive (“the controller”) and Striive v/ Mathias Quist Michaelsen, Midgårdsvej 10, 8800 Viborg, Denmark, CVR no. 46826159, which operates Striive (“the processor”).

The agreement is an annex to and part of Striive’s terms of service and is made when you accept them. It applies for as long as the processor processes personal data on behalf of the controller and continues until the data has been deleted under section 11.

The agreement meets article 28(3) of the General Data Protection Regulation (GDPR). Terms have the meaning given in the GDPR. If this agreement and the terms of service conflict, this agreement prevails as regards the processing of personal data.

2. Processing on instructions

The processor processes personal data only on documented instructions from the controller. The instructions are given in this agreement with annex 1, in the terms of service, and through the choices and actions the controller and its team make in Striive, for example when a form is created, content is published, or the AI assistant is asked to carry out a task. Further instructions are given in writing.

Processing required of the processor by EU or Danish law may take place without instructions. The processor then informs the controller of the requirement before processing, unless the law prohibits this on important grounds of public interest.

The processor immediately informs the controller if, in its opinion, an instruction infringes data protection law.

The processor does not use the data for its own purposes. What the processor itself processes as a controller, such as data about the customer’s account and payment and the reference library, is described in Striive’s privacy policy and is not covered by this agreement.

3. Confidentiality

Only persons who need it to provide Striive get access to the personal data. They have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access is reviewed and removed when the need ends.

4. Security

The processor takes the technical and organisational measures required by GDPR article 32, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks to data subjects. The measures are described in annex 3.

The processor may change the measures as long as the level of security is not reduced.

The controller is responsible for the choices it makes in Striive itself, including who gets access to the website, whether two-factor sign-in is used, and what data is collected.

5. Sub-processors

The controller gives the processor a general authorisation to use sub-processors. The sub-processors used when the agreement is made are listed in annex 2 and at striiveai.com/en/legal/sub-processors.

The processor tells the controller by e-mail at least 30 days before a sub-processor is added or replaced. The controller may raise a reasoned objection within that period. If the parties cannot find a solution, the controller may cancel the subscription before the change takes effect and receives the prepaid part of the period back proportionately.

The processor imposes on each sub-processor, by written contract, the same data protection obligations as in this agreement, including sufficient guarantees of appropriate security. The processor remains fully liable to the controller for the sub-processor's performance of its obligations.

6. Transfers to third countries

The personal data is stored in the EU (Google Cloud, Stockholm). Transfers to countries outside the EU/EEA take place only to the sub-processors and for the purposes listed in annex 2, and only with a valid transfer mechanism under GDPR chapter V: an adequacy decision, including the EU-U.S. Data Privacy Framework for certified recipients, or the European Commission's standard contractual clauses.

By this agreement the controller instructs the processor to make these transfers.

7. Assistance with data subjects' rights

The processor assists the controller in responding to requests from data subjects for access, rectification, erasure, restriction, data portability and objection. The controller can itself view, correct and delete form submissions and other content in the editor and download consent records. What the controller cannot do itself in the editor, the processor does on written request without undue delay.

If the processor receives a request directly from a data subject, it forwards it to the controller and does not answer it itself without instructions.

8. Personal data breaches

The processor notifies the controller without undue delay and no later than 48 hours after becoming aware of a personal data breach affecting the controller's data, so the controller can meet its 72-hour deadline towards the supervisory authority.

The notification describes, as far as possible: the nature of the breach, including the categories and approximate number of data subjects and records; the likely consequences; the measures taken or proposed to address the breach and mitigate its effects; and a contact person. Information not known at once is given as it becomes available.

The processor keeps a log of all breaches, including those that need not be notified.

9. Other assistance

Taking into account the nature of processing and the information available to it, the processor assists the controller in meeting its obligations under GDPR articles 32 to 36, including data protection impact assessments and prior consultation of the supervisory authority.

Assistance beyond what Striive provides in the editor or in this agreement, and not caused by the processor's own circumstances, may be invoiced by time spent at a reasonable hourly rate agreed in advance.

10. Documentation and audits

The processor makes available all information necessary to demonstrate compliance with article 28 and this agreement. As a rule, this is done by the processor answering, on request and no more than once a year, the controller's written questions about the security of processing.

The controller, or an independent auditor bound by confidentiality, may also carry out an audit, including an inspection, with at least 30 days' notice, where this is necessary after a breach, an enquiry from an authority or reasoned doubt about compliance. The controller bears its own costs. An audit may not give access to other customers' data or endanger security. Audits of sub-processors take place through their own audit reports and certifications.

The supervisory authority and other authorities always have access as the law provides.

11. Deletion and return on termination

When the subscription ends, the website is kept for 30 days, or for 90 days if it was locked for non-payment, so the controller can resume the service. Before the deletion the controller can download consent records in the editor and ask for a copy of the website's content, media and form submissions in a common, machine-readable format.

The processor then deletes all personal data processed for the controller, including content, media, form submissions, consent records, AI conversations and compliance reviews. Backups are deleted automatically no later than 30 days after that. The controller is told by e-mail 7 days before the deletion.

This does not apply to data that EU or Danish law requires to be kept, such as accounting records. The processor keeps those only for as long as, and for the purpose, the law requires.

12. Liability and changes

The parties' liability under this agreement follows section 19 of the terms of service and GDPR article 82. The limitations in the terms of service do not apply to claims by data subjects.

Changes to this agreement are notified as changes to the terms of service. Changes required by new legislation or a decision of an authority may be made at shorter notice.

Annex 1. Description of the processing

Purpose: to provide Striive to the controller so the controller can build, edit, host and publish its website, receive form submissions, record visitors' consent, and use the AI assistant and the compliance review.

Nature of processing: storage, hosting, display, transmission, backup, processing with AI at the controller's request, deletion.

Duration: for as long as the subscription runs, and until deletion under section 11.

Categories of data subjects	Categories of personal data
People who submit forms on the website	The fields the controller has chosen, typically name, e-mail, phone and message. Striive does not store the sender's IP address.

Categories of data subjects	Categories of personal data
Visitors who answer the cookie banner	A random consent id, time, the chosen categories, the offered categories, the page address and the banner text version. No IP address or browser details. Deleted 3 years after the answer.
Members of the controller's team	Name, e-mail and role as they appear in the website's content and settings (their accounts are processed by Striive as controller).
People mentioned or shown on the website	Names, pictures, contact details and anything else the controller puts on the website.
People who appear in AI conversations	What the controller and its team write to the AI assistant, and the content the assistant works with.
People who appear in the compliance review	The controller's answers about its business and the review's results. The review reads published pages as an anonymous visitor and does not read visitors' data.

Special categories of data under article 9 and data on criminal offences are processed only if the controller itself collects them. The controller may do so only on a lawful basis, and must then assess itself whether Striive's measures are sufficient.

Annex 2. Sub-processors

When the agreement is made, the processor uses these sub-processors for the controller's data:

Sub-processor	Task	Location and transfer mechanism
Google Cloud EMEA Ltd. (Google Cloud)	Servers, database, media storage, backups and operational logs	EU, region europe-north2 (Stockholm)
Resend, Inc.	Sending e-mails, including notices of new form submissions (without the form's content)	Sending in the EU; account data, metadata and logs in the US. Standard contractual clauses
OpenRouter, Inc.	Relaying AI requests to the AI provider	US. Standard contractual clauses
Anthropic, Google and OpenAI	AI models that process requests from the AI assistant	US. EU-U.S. Data Privacy Framework or standard contractual clauses
Unsplash Inc.	Serving stock photos the controller has chosen for the website; the visitor's browser loads the image directly from Unsplash	Visitors' IP address and browser details. No cookies. US. Standard contractual clauses

The current list, including providers Striive uses as a controller, is at striiveai.com/en/legal/sub-processors.

Annex 3. Technical and organisational measures

- Location: all data is stored with Google Cloud in the EU (Stockholm). Data is encrypted at rest with Google's default encryption.
- Encryption in transit: all traffic to the editor and published websites uses HTTPS with HSTS. Certificates are issued automatically.

- Customer separation: each website's data is separated at database level by row-level security, which is always enforced. The server refuses to start if the separation is not active.
- Sign-in: users sign in with a one-time code sent to their e-mail address (stored only as a hash, valid for 10 minutes, at most 5 tries) or with a passkey, of which only the public key is stored. Two-factor sign-in (TOTP) with recovery codes, stored as hashes. Accounts are locked temporarily after repeated failed attempts. Sensitive actions require the user to confirm again. Session cookies are HttpOnly, Secure and bound to the host.
- Roles: each website has roles, so only the right people can edit, publish and manage billing.
- Web protection: Content Security Policy, protection against framing by other sites, and rate limits on sign-in and public forms.
- Secrets: keys and passwords for systems are kept in Google Secret Manager. Sensitive values in the database are encrypted with AES-256-GCM.
- Operational access: the servers can be reached only through Google's Identity-Aware Proxy with personal sign-in. Only ports 80 and 443 are open to the internet. The operating system installs security updates automatically.
- Backups: the database is backed up every 6 hours and media daily to separate, private storage in the EU. Copies are deleted automatically after 30 days. Restoring has been tested.
- Separate environments: testing happens in a separate Google Cloud project, never on customers' data.
- Logging: important actions are recorded in an audit log with who, what and when. Sign-in attempts are recorded.
- Data minimisation: form submissions and consent records are stored without IP addresses. Temporary raw page copies are deleted within 1 hour.
- Breaches and incidents: a written procedure for handling and notifying breaches, and a log of incidents.
- Confidentiality: only people with a work need have access, and they are bound by confidentiality.