Privacy policy

Effective 1 November 2026

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

1. Controller

The controller for the processing described here is Striive v/ Mathias Quist Michaelsen, Midgårdsvej 10, 8800 Viborg, Denmark, CVR no. 46826159, which operates Striive. Write to admin@striiveai.com with questions about your personal data or to exercise your rights.

This policy covers the data Striive decides about itself: about customers and their teams, about people who sign up, write to us or report content, about businesses we make demo sites for, and about visitors to striiveai.com.

The data that forms part of customers' own websites, such as form submissions and visitors' consent answers, we process as a processor for the customer. The customer is the controller for it, and you should contact the business that owns the website. The terms are in the data processing agreement.

2. Your account and your website

When you sign up or are invited to a website, we process your e-mail address, your name, your passkeys (the public key, the name the passkey was given, and when it was created and last used), your two-factor key if any (encrypted) and your recovery codes (only as a one-way hash), your profile picture, your preferences, which websites you are a member of and in which role, and when you last signed in. You sign in with a code we send to your e-mail address, or with a passkey. A passkey is deleted when you remove it, and otherwise with the account.

Purpose: to give you access to Striive and provide the service. Legal basis: the contract (GDPR article 6(1)(b)). If you are a member of a customer's team without being a customer yourself, the basis is our and the customer's legitimate interest in giving the team access (article 6(1)(f)).

Retention: for as long as you are a member of at least one website. When your last membership ends, we e-mail you, and your account is deleted 30 days later with everything that belongs to it, unless you become a member of a website again before then. You can ask for the account to be deleted sooner.

When you set up your website, you can describe your business in your own words. The AI assistant reads what you write (section 4) and finds the business's name, town, website and any CVR number. With them we look the business up: we read the website you mention. We send the name and the town to Google's Places API (Google Maps Platform) and show you the places Google finds. And we look up the CVR number or the name in the CVR register through Datafordeleren. You choose what goes in.

Google receives the name and the town as you wrote them, and the id of the place you choose. Google does not receive your e-mail address or anything else about your account. Of Google's answer we keep only the place's id. The name, address, opening hours, phone and picture are fetched from Google again when they are shown, and are stored only when you accept them. Google processes the requests as an independent controller under its own terms for Google Maps Platform and may process them in the United States (section 12). Datafordeleren is run by the Danish Agency for Climate Data

(Klimadatastyrelsen) and serves the Danish Business Authority's public CVR register. It receives the CVR number of the name. We keep what the register says about the business: name, CVR number, address, company form, phone, e-mail and industry. We do not read owners from the register.

Purpose: to help you set up the website from information about your business. Legal basis: the contract (article 6(1)(b)). Retention: the lookup (what you wrote, the lookups we made, the place's id and the CVR register's answer, each with its time) is kept with the website and deleted with it. What you accept becomes part of the website's content, which we process as a processor for the customer.

3. Purchase, subscription and bookkeeping

When you buy a subscription, we record your e-mail address, the website's name, the billing interval and your consent to the terms: when you accepted, the wording you saw, and the version of the terms, the data processing agreement, the privacy policy and the withdrawal form you received. Stripe processes your name, address, e-mail and card details; we receive only Stripe's customer and subscription numbers and the status of payments. If you buy as a business and type its CVR number, we look the number up in the CVR register through Datafordeleren (section 2) and fill in the business's name and address, which you can correct.

Purpose: to make and perform the contract, to be able to document what you accepted, and to comply with the Danish Bookkeeping Act. Legal basis: the contract (article 6(1)(b)), legal obligation (article 6(1)(c)) and our legitimate interest in documenting the contract in a dispute (article 6(1)(f)).

- A sign-up that is never paid is deleted after 30 days.
- The record of your consent is kept for 5 years after the subscription has ended.
- A sign-up where payment went through but setting up the website failed is kept for 5 years.
- Invoices, payments and records of AI usage are kept for 5 years after the end of the financial year they relate to (Danish Bookkeeping Act).

The price for the first months, the one-time AI credit and the money-back guarantee are each given once per customer (sections 4, 5 and 8 of the terms). So with each payment we record a hash of the payment card's fingerprint from Stripe and a hash of your normalised e-mail address. Both are computed with a secret key (HMAC-SHA-256 with a "pepper"), so neither the card nor the address can be read from them; we never store the fingerprint or the address itself for this purpose. If you use the guarantee, withdraw (section 7) or cancel a yearly plan with a refund, we also record the website, Stripe's subscription, invoice and credit note numbers, the amount, the date and which kind of refund it was.

Purpose: to give the price for the first months, the one-time credit and the guarantee once per customer and to document the refund. Legal basis: our legitimate interest in being able to keep to these terms (article 6(1)(f)), and for the credit note the Danish Bookkeeping Act (article 6(1)(c)). Retention: for as long as we offer any of them, also after the website has been deleted, as they could otherwise be used again. If we stop offering all of them, we delete the records.

If you withdraw with «Fortryd aftale», we use the name and e-mail address you give to send the receipt for your withdrawal. They are deleted from the record as soon as the receipt has been sent; the receipt itself is in your inbox.

4. The AI assistant

When you use the AI assistant, we process your messages, the replies and the website content the assistant works with, as well as how much was used, by which model and at what price. Messages and content are sent through OpenRouter to the AI provider behind the chosen model (Anthropic, Google or OpenAI). To bill usage, Metronome receives the website's id and name, Stripe's customer number, the model name and the number of tokens, but no content.

Purpose: to provide the AI features and bill usage. Legal basis: the contract (article 6(1)(b)). Website content the assistant works with is processed as a processor for the customer.

Retention: conversations are kept until you delete them and are erased 30 days after that, or when the website is deleted. We do not use your content to train AI models.

5. E-mails about the service

We send e-mails the service needs: confirming your address, sign-in codes and invitations, the order confirmation, payment reminders, the reminder 7 days before the price for the first months moves to the full price, receipts for refunds and withdrawals, notices of closure and deletion and the like. We use your e-mail address and name. Legal basis: the contract (article 6(1)(b)). We send no newsletters or marketing. If we do later, it will only be with your consent.

6. Security and abuse

To protect accounts and the service, we record sign-in sessions (IP address, browser details and a device label), sign-in attempts (e-mail address, IP address, browser details and the result) and an audit log of important actions (who, what, when, IP address and browser details). Legal basis: our legitimate interest in securing the service and investigating abuse (article 6(1)(f)).

When you sign in, we form a fingerprint of your browser from what it sends (such as its type and language) and a few details the sign-in page reads (time zone, languages, screen size, operating system and number of processor cores). The fingerprint is hashed in memory, used only to limit sign-in attempts, never stored, and no longer counted after ten minutes. The sign-in page also stores a cookie in your browser holding a random, signed device id, so you are counted as your own device and cannot be locked out by others with the same kind of device; it names no account, grants no access and expires after 365 days. Both are strictly necessary to protect the sign-in you asked for, and our basis is legitimate interest (Article 6(1)(f)).

- Sessions expire after at most 90 days and are deleted 30 days after they expired or ended.
- Sign-in attempts are deleted after 90 days.
- The audit log is deleted after 24 months, and no later than 12 months after the website it concerns has been deleted.
- Sign-in codes are stored only as a one-way hash, together with the account or e-mail address and the browser they were sent to. A code is valid for 10 minutes, and codes are deleted 8 days after they were sent.
- One-time links for confirming an e-mail address and for invitations are deleted 30 days after they were used or expired.

7. Enquiries and reports of content

If you write to us, we process your name, your e-mail address and the content of your message in order to answer. If you report content on a website hosted by Striive, we process the information you give in the report to handle it, tell you the outcome and document the case, and we may tell the customer about the report without revealing who you are, unless that is necessary and you have been told.

Legal basis: our legitimate interest in answering enquiries (article 6(1)(f)) and, for reports, our legal obligations under the Digital Services Act (article 6(1)(c)). Retention: 3 years after the case is closed.

8. Demo sites for businesses

We may make a demo site for a business to show what Striive can do. To do so we read the business's public website and public information and let AI extract facts about the business, such as its name, address, opening hours, services and contact details. This may include names and contact details of people shown on the website. Reviews from other platforms are not stored.

Legal basis: our legitimate interest in presenting Striive to the business (article 6(1)(f)). The source is the business's own public website. The demo site is not publicly searchable and is deleted when its period ends, by default after 28 days, unless the business takes it over. The raw page copies are deleted no later than 1 hour after they were read. You can always object, and we then delete the demo site.

9. The reference library

The reference library holds screenshots, text, colours and fonts from public websites that Striive customers and the AI assistant use as design inspiration. The screenshots may show names or pictures of people who appear on the websites. We also record which websites a user has viewed or saved as a favourite in the library.

Legal basis: our legitimate interest in offering design inspiration (article 6(1)(f)) and, for Striive customers' websites, section 16 of the terms. Retention: until the website is removed from the library. A website is removed at once if its owner asks, or if you object to a screenshot of you. Records of what a user viewed or saved are deleted with the user's account.

10. Visiting striiveai.com and signing up in the app

If you accept analytics cookies in the cookie banner on striiveai.com, we use Google Analytics to measure how many people visit the site, which pages they read and where they come from. Google receives the pages you view, the page you came from, your browser, device, screen size and language, an approximate location derived from your IP address and a random id from the cookie. Google Analytics does not store the IP address. We don't use the data for advertising and have turned off Google's advertising features and Google signals.

If you have said yes to statistics, either on striiveai.com or on the sign-up page in the app, our server also sends events from the app to Google Analytics: that you go to payment (plan, amount and currency), that you create an account (that you signed up with e-mail), that you have paid (plan, amount, VAT, currency and the payment's id at Stripe), and that the editor offers to be installed as an app, whether you accept or decline, and that it is installed. Each event carries Google Analytics' random id and the number of your visit from the cookie __Secure-striive_measure, so we can see how many visits to striiveai.com end in a sign-up. The events are sent from our server and carry neither your IP address nor details of your browser, so Google places them at our server, not at you. We never send your e-mail, name, phone number or customer id to Google. We can link the payment's id to your account ourselves; Google cannot.

Legal basis: your consent (article 6(1)(a), and section 3 of the Danish cookie order). Retention: Google Analytics deletes data tied to the individual visitor after 2 months; after that we only have totals. You can withdraw your consent under “Cookie settings” at the bottom of every page. See the cookie declaration at striiveai.com/en/legal/cookies. The same applies to the events from the app. You change your choice under "Cookie settings" at the bottom of every page on striiveai.com or at the bottom of the app's sign-up pages. The editor itself has no consent setting; it follows your latest choice. If you say no, the app sends no new events to Google.

Without consent Google Analytics is not loaded, the site sets no analytics cookies, and we keep no log of visits. Fonts are served from our own server. If you submit a form on the site, such as a report of content, section 7 applies.

11. Who we share data with

We never sell personal data. We use these providers as processors, each only for its purpose and under a data processing agreement. The full list, with what each receives and where, is at striiveai.com/en/legal/sub-processors.

- Google Cloud: operation, storage and backups in the EU (Stockholm).
- Google Workspace: our e-mail at striiveai.com.
- Google Analytics (Google Ireland Limited): visitor statistics on striiveai.com and counting sign-ups and purchases in the app, only with your consent.
- Stripe: payments, subscriptions, receipts and invoices.
- Resend: sending the service’s e-mails.
- Metronome: measuring and billing AI usage.
- OpenRouter and the AI providers Anthropic, Google and OpenAI: the AI assistant.
- screenshotapi.net: screenshots of public websites for the reference library.
- Unsplash: searching stock photos in the editor.

When you set up a website or buy as a business, Google (Places API) and Datafordeleren receive the data section 2 names. They are not our processors but independent controllers under their own terms.

We disclose data to authorities only when the law requires it, and to advisers such as our accountant and lawyer when necessary and under a duty of confidentiality.

12. Transfers outside the EU

Stripe, Resend, Metronome, OpenRouter, Anthropic, Google (including for Google Analytics and the Places API), OpenAI and Unsplash may process data in the United States, and screenshotapi.net (JFreaks Software Solutions Pte. Ltd.) in Singapore. The transfers rely on the European Commission’s adequacy decision for the EU-U.S. Data Privacy Framework where the recipient is certified under it, and otherwise on the European Commission’s standard contractual clauses (for Singapore always the standard contractual clauses), which form part of the provider’s data processing agreement. Resend keeps account data, metadata and logs about sent e-mails in the United States. Metronome states no location for data in the EU. For Google’s Places API, Google is an independent controller, and the transfer follows Google’s Controller-Controller Data Protection Terms: the EU-U.S. Data Privacy Framework, where Google LLC is certified, and otherwise the standard contractual clauses between controllers. Datafordeleren processes the data in Denmark. Write to us for a copy of the relevant transfer mechanism.

13. Automated decisions

We make no decisions about you based solely on automated processing, including profiling. Reports of content are always assessed by a person.

14. Your rights

You have the right:

- to access the data we process about you,
- to have inaccurate data corrected,
- to have data erased,
- to have processing restricted,
- to object to processing based on our legitimate interest,
- to receive the data you have provided in a common, machine-readable format (data portability),
- to withdraw a consent where processing is based on consent, without affecting processing before the withdrawal.

Write to admin@striiveai.com. We answer within one month. We may ask you to confirm who you are. The rights may be limited by law; for example, we may not delete accounting records early.

You can complain to the Danish Data Protection Agency (Datatilsynet), Carl Jacobsens Vej 35, 2500 Valby, Denmark, datatilsynet.dk. We would like the chance to solve the problem first, so please write to us.

15. Cookies in the editor

The editor at app.striiveai.com uses strictly necessary cookies, which require no consent, and reads the cookie __Secure-striive_measure, which tells it whether you said yes or no to statistics (section 10). See the cookie declaration at striiveai.com/en/legal/cookies.

16. Changes

If we change this policy materially, we tell customers by e-mail before the change applies. The date at the top shows when the current version took effect, and earlier versions are available on request.