

Security and data handling

One page for the person in your organisation who has to sign this off. If you need a longer questionnaire answered, send it and we will answer it in full rather than send you a certificate we do not hold.

What we do with your content

WHAT	WHERE IT GOES	WHY
Your brief, plan, brand voice and article text	Commercial AI model APIs	To research, write and score the article
The finished article and its brief	Proofed, over its API	Human editing, returned as tracked changes
Your style guide, glossary and preferred spellings	Stylus, in your own project	So the engine and the editor work to the same rules
Audio or video you upload	A transcription model, then stored with your project	Only what you choose to upload
Competitor pages we crawl	Fetches by our crawler at a rate limit	Public pages only. Nothing behind a login
Payment card details	Stripe only	We never see them. We hold a customer reference
Your email address	Our mail provider	Delivery notifications and account email

What does not leave. We do not use your material for any other customer, as a training sample or in our marketing. We do not sell it, and we share it only with the subprocessors listed below. You can ask us to delete it at any time after delivery and we will do so within thirty days.

Subprocessors

SUBPROCESSOR	PURPOSE	WHAT REACHES IT
Anthropic	By default: research, article generation, planning, scoring, briefs. Any text task can be routed to either model provider	Brief, plan, brand voice, research notes, article text, and page text read for imports and competitor analysis
OpenAI	By default: images, transcription, embeddings, clean-up of transcripts and uploads, reading your website at setup. Any text task can be routed to either model provider	Image prompts and your visual reference images, uploaded audio, transcripts and uploaded documents, your homepage text, page text for embedding, and the brief, brand voice and article text of any task routed to it
Proofed	Human editing, and optional sign-in with a Proofed account	The article to be edited, its brief, the project name and the article title
Stylus	Style guides and voice profiles	Account name and email, style rules, preferred spellings, voice samples
Stripe	Payments and subscriptions	Name, email, billing details, card data held by Stripe
Mailgun	Transactional email	Email address, message content
Google	Optional sign-in and Search Console performance data	Only if you connect it
Cloudflare Turnstile	Bot protection on the sign-in form	Request metadata
Slack	Internal notifications to our team	Name, email, IP address and approximate location, device type, article titles on editing orders, account deletions
ip-api.com	Approximate location of an IP address, for those notifications	IP address VERIFY
Fathom Analytics	Cookieless visit analytics on our website and sign-in pages	Page visits and request metadata

How the application is secured

Authentication	Passwordless. Sign-in is by an emailed link that works once and expires after fifteen minutes, or with a Google or Proofed account. There is no password login, so there is no password to leak. The sign-in request is rate limited and the form is bot-protected. Single sign-on through your own identity provider is not available.
Authorisation	Policy-based authorisation on the core content models, with ownership checks elsewhere. Workspace membership governs access.
API access	OAuth 2, used by AI assistants over MCP, and personal access tokens, with idempotency keys on write operations. A personal token is either account-wide or limited to one project, read-only or read-write. On the REST API a project token cannot reach any other project. VERIFY
URLs	Projects, articles, briefs and other content records are addressed in URLs by UUID, never by an incrementing integer.
Outbound webhooks	Signed HMAC-SHA256, so your systems can verify a request came from us.
Inbound integration endpoints	CMS and style-guide callbacks are verified by HMAC signature, and a connected site with no secret is refused. Connecting a CMS uses a signed, single-use state. Stripe events are verified by Stripe's signature and Proofed status callbacks by a shared key.
Fetching your URLs	Every user-supplied URL, and every redirect it leads to, passes a server-side request forgery guard that refuses private and other non-public network addresses. A request carrying your CMS credentials never follows a redirect to another host.
Prompt injection	Content is sanitised and length-limited before it reaches a model, with clear delimiters between instructions and content.
Payments	Stripe webhook signatures are validated. Integration secrets are encrypted at rest. VERIFY
Storage	Uploaded audio, video, documents and transcripts are held in private storage. Generated images, and the visual reference images you upload, are served from public addresses containing a random identifier, so that they can be embedded and published.
Transport	HTTPS to the application and to every model, editing, style-guide, email and payment provider. VERIFY

What we do not claim

We hold no security certification. We are not going to imply one on a questionnaire, and if that is a requirement for your organisation you should know it now rather than three weeks into a procurement process. What we will do is answer any questionnaire you send, in full, in writing, and tell you plainly where the answer is "not yet".

To be completed before issue

Fill these before this document is sent to anyone. Each is marked in the body with an orange badge.

- Hosting country, region and legal entity, stated once and identically everywhere.
- Data retention and deletion periods, per data type. The live-system behaviour is now filled in from the code (routes/console.php, ProfileController::destroy, media:prune-orphans). Still open: backups, and whether deletion reaches Proofed, Stylus, the model providers and Slack, which the code does not do.
- Each model provider's current position on retention and training from API traffic, checked on the day you answer.
- Backup frequency, retention and restore testing.
- Incident notification commitment and the contact address for it.
- Whether a data processing agreement is available, and from whom.
- API access: the MCP endpoint accepts a project-limited personal token but does not enforce its project limit (routes/ai.php, app/Mcp/Tools). Fix it, or keep the claim to the REST API as written.
- Payments: WordPress application passwords saved before 28 August 2026 may still be stored in plain text (app/Models/DistributionDestination.php). Re-encrypt existing rows before issue.
- Transport: the code does not force HTTPS or send HSTS, so confirm it on the server. The ip-api.com lookup is plain HTTP (app/Services/Geo/IpGeolocator.php), and it uses the free endpoint, so check ip-api's terms for commercial use. Move it to HTTPS or remove it, and drop its subprocessor row if removed.
- Model provider terms: the OpenAI calls use the Responses API, including background mode, and do not opt out of response storage. Check OpenAI's current retention for stored responses.
- Hosting: the code shows servers managed with Laravel Forge, files on the server's own disk, and a database-backed queue, session and cache. The cloud provider, region and entity are not in the repository.

Hosting	[Country, region, provider and legal entity] VERIFY
Retention	Articles, briefs and uploads are kept until you delete them or the account is deleted. Records of the requests made to the model providers for your work, which include the text sent and returned, are kept until the account is deleted. Activity logs are deleted after 90 days. [Backup copies] VERIFY
Deletion	On request, within thirty days. An account can also be deleted from its settings: this permanently removes its projects, articles and briefs at once, and their stored files within a week. [Copies held by subprocessors and in backups] VERIFY
Backups	[Frequency, retention, restore testing] VERIFY
Model provider terms	[Each provider's current retention and training position, with the date checked] VERIFY
Incident notification	[Commitment and contact address] VERIFY
Data processing agreement	[Available / in preparation, and from whom] VERIFY

Who to contact

Security and data questions: [email] . We aim to answer any questionnaire within five working days.

[YOUR COMPANY NAME] · COMPANY NUMBER [NUMBER] · [REGISTERED OFFICE] · DERIVED FROM THE APPLICATION AS
BUILT; CONFIRM AGAINST PRODUCTION BEFORE ISSUE