Privacy Policy

Effective 23 November 2026 | Version 1.0
Next scheduled review: 23 February 2027

1. Who is responsible for your information?

Glossavia is operated by **Euan Chand, trading as Glossavia**, in his own capacity. Glossavia is not currently an incorporated company. References to "we", "us" and "our" in this policy mean Euan Chand trading as Glossavia.

Website: glossavia.co.uk
Privacy contact: hello@glossavia.co.uk
Address for correspondence: 36 Hamilton Mansions, Barking Riverside, London, IG11 0BU, United Kingdom

Euan Chand is the controller where he decides why and how personal information is used for Glossavia's own website operation, enquiries, account administration, security and business records. Privacy questions and requests should be sent to the contact above.

This policy explains our handling of personal information under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and, where relevant, the Privacy and Electronic Communications Regulations 2003 (PECR), as amended.

2. Customer content and our different roles

An organisation using Glossavia is normally the controller of personal information in its source material, campaign content and customer-directed review records. We process that information on its documented instructions as a processor. If the organisation itself acts as a processor, we may act as its subprocessor. The actual activities determine these roles.

Our processing terms with the organisation govern that work. The organisation is responsible for its lawful basis, required notices and permissions. If your request concerns information processed solely on its behalf, contact that organisation; we will assist it as required by law and our agreement.

Where we organise contributions to Glossavia ourselves, we are controller of the related contributor administration and feedback records. Any separate participant privacy notice also applies to that activity. This policy does not replace participant information or consent where those are required, or change a signed participation agreement.

3. What information do we collect?

We collect information directly from you, from your organisation or an authorised person inviting you, through your use of the service, and from an optional service connection you authorise.

- **Website and security information:** IP address, browser or device information, request times, requested resources, response or error information and records needed to investigate misuse or faults. Hosting providers may also process technical request information.
- **Enquiries and support:** your name, organisation, email address, any telephone number you choose to provide, your message, attachments and related correspondence. This includes demonstration requests.

- **Accounts and invitations:** name, email address, assigned role, permissions, assigned languages, invitation and account status, password authentication records, session identifiers, sign-in times, IP address, browser information and relevant activity history. Password authentication uses a password hash rather than a readable password.
- **Campaign information:** source documents, supporting evidence, branding, images, generated text, image descriptions, review comments, approvals, planned dates and delivery records. Personal information is included only to the extent it appears in those records.
- **Contributor records, where applicable:** background or language competence supplied for the agreed role, contributions, scores, comments, completion records, and participation or confidentiality agreement records, including signing evidence.
- **Facebook Page connections, if used:** Page names and identifiers, Page tasks or permissions returned by Meta, Page access tokens, the account holder who connected the Page, connection times, and post, scheduling and delivery identifiers or statuses. The connection requests pages_show_list, pages_read_engagement and pages_manage_posts. We do not ask you for your Facebook password.
- **Device notifications, if enabled:** a browser push endpoint, subscription keys, account association and notification delivery information.
- **Business records, if applicable:** contracting and billing contact details, agreed charges, invoices and payment status. These terms do not mean that a payment service or paid subscription is already in operation.

Information required to administer an account or provide a requested service must be supplied for that purpose; otherwise we may be unable to give access or respond. Optional information and optional connections can be declined.

4. Patient information and sensitive information

Glossavia is intended for programme and campaign communication, rather than patient records or individual care. Use public or synthetic source information wherever possible. Do not upload patient-identifiable information, individual screening results, medical records, or other special category or criminal offence data unless a separate written arrangement expressly permits the processing and the necessary safeguards and legal conditions have been established in advance.

Do not include sensitive personal information in support requests. If it is submitted in error, notify hello@glossavia.co.uk promptly so we can assess the incident and agree appropriate restriction, removal or return. Public availability does not, by itself, remove data protection obligations.

5. Why do we use information, and on what basis?

For information for which we are controller, the following bases apply as relevant to the activity:

- **Answering enquiries and arranging demonstrations:** legitimate interests in responding to requested contact and managing prospective relationships. Contract applies where necessary to take steps at an individual's request before entering a contract with that individual.
- **Administering organisational accounts, invitations and access:** legitimate interests in providing the requested workspace, maintaining appropriate permissions and managing the relationship. An employee is not treated as personally party to an organisation's contract merely because they use its account.
- **Performing an agreement with an individual:** contract, only where that person is a party and the particular processing is necessary to perform it. This may include necessary administration of an individual's access or confidentiality agreement.

- **Security, fault investigation and service administration:** legitimate interests in protecting information, preventing misuse and operating the service reliably. A specific legal obligation may apply to particular incident or compliance records.
- **Managing agreed contributions and feedback:** legitimate interests in administering contributions, evaluating service quality, documenting completed work and improving Glossavia, subject to any separate applicable notice and agreement. Identifiable attribution requires its own appropriate basis and agreement.
- **Invoices and legal records:** legitimate interests in business administration and legal obligation where accounting, tax or other law requires retention.
- **Complaints and legal claims:** legal obligation where applicable, and legitimate interests in resolving concerns and establishing, exercising or defending legal claims.
- **Optional device notifications:** consent to use the requested notification channel. You can turn notifications off in your account on that device or revoke browser permission. Necessary records of an underlying account event may still be processed on the relevant basis above.

We assess necessity and balance legitimate interests against your rights and reasonable expectations. Processing of customer-controlled content follows the customer's documented instructions; the customer determines the applicable lawful basis.

Account and service messages are not permission for unrelated marketing. If marketing is introduced, we will apply the relevant UK GDPR and PECR requirements, obtain consent where required and provide an opt-out. We do not rely on acceptance of these terms as marketing consent.

6. Cookies and similar technologies

The following inventory describes storage used by the implemented account system and security layer. Optional technologies apply only when their associated feature is used.

Technology	Provider and purpose	Duration and choice
__Secure-glossavia.session_token	Glossavia first-party account cookie, using Better Auth; recognises your authorised signed-in session. Secure, HttpOnly and SameSite=Lax.	Seven-day session lifetime, renewed during continued use; removed on sign-out. Necessary for the sign-in service you request.
__Secure-glossavia.dont_remember	First-party authentication preference, used if a non-persistent session is requested.	Session cookie where set. Necessary to apply that session choice.
__cf_bm	Cloudflare bot protection; helps distinguish legitimate traffic from automated abuse. Observed on the public site.	Expires after 30 minutes of continuous inactivity. Used for service security.
Cloudflare challenge cookies, such as cf_clearance and cf_chl_*, if a challenge is presented	Cloudflare security verification. These are conditional; the list does not mean every cookie is set on every visit.	For the challenge or configured clearance period shown by the browser. Used only when the security feature requires them.
Service-worker registration and browser push subscription	First-party support for device notifications you choose to enable; your browser stores the subscription.	Remains until disabled or removed through the account/browser or the subscription becomes invalid. Optional; browser permission is requested.

Session-data cookie caching is disabled in the current account configuration. The application does not include an advertising pixel or a separate audience-analytics tracker. Infrastructure providers still process technical and security information needed to deliver the site. Services you separately visit, including Meta authorisation pages and external social links, use their own technologies under their own notices.

We use the PECR exception for technologies strictly necessary for the requested account or security function only where its conditions are met. We obtain consent before introducing any technology that requires it, and provide any information or free objection control required for another applicable exception. Consent to optional technologies is separate from acceptance of service terms.

You can restrict or remove cookies in your browser, although blocking necessary authentication storage may prevent sign-in. Device notifications can be disabled in your account on that device or through browser permissions. Contact hello@glossavia.co.uk about storage choices or unexpected technologies.

7. Who receives information?

Necessary service providers receive the information needed for their function. Hosting and account operation use the application-hosting chain; AI and translation services receive content only for the relevant requested processing. Email and optional publishing or notification services receive the corresponding message or connection information.

The provider and transfer register below identifies the current implementation. We may also disclose necessary information to professional advisers, regulators, courts or authorities where lawful. Customer-controlled personal information may be shared with subprocessors only under the required authorisation and processing protections. Information is not sold through these service terms.

Provider and transfer register

This register identifies the services used by the implementation and their roles. Optional services receive information only when configured and used for the relevant task. Supplier services, legal entities and subprocessors remain subject to their applicable account terms; this register does not claim a bespoke contract, UK-only processing or a particular regional setting that has not been established.

Service	Purpose and information involved	Role and international processing
OpenAI / ChatGPT Sites; Cloudflare infrastructure	Published application hosting, database and file storage, delivery and security; account, workspace, uploaded content and technical request information.	Hosting processor/subprocessor chain. OpenAI's published Sites DPA identifies OpenAI OpCo, LLC for a UK-based individual operator. Cloudflare provides the underlying infrastructure. Processing may include the US and other provider locations; no UK-only residency is promised.

Service	Purpose and information involved	Role and international processing
OpenAI API	Source extracts, prompts, campaign text or images needed for generation, translation or checking. Account administration and API usage metadata are also processed.	Content processor under the applicable API agreement; the UK DPA route identifies OpenAI OpCo, LLC. Provider locations and the available transfer terms apply. Separate provider-controller purposes may apply to account, security or legally required records.
Microsoft Azure Translator	Text submitted to the configured translation route.	Processor/subprocessor under the applicable Microsoft agreement and Products and Services DPA. Microsoft and its relevant contracting affiliate provide the service; processing location depends on the Azure resource and service routing. A UK-only region is not asserted.
Resend - Plus Five Five, Inc.	Email addresses, account/service messages, attachments and delivery information.	Email processor/subprocessor, with separate controller purposes for its own account/security administration. Resend states that stored customer data is in the US; selecting a sending region does not change that storage location. Its DPA includes UK transfer provisions.
Zoho Mail	Enquiries, support correspondence, contact details and attachments delivered to hello@glossavia.co.uk.	Mailbox processor under the relevant Zoho agreement, with its own account/security purposes where applicable. The domain uses Zoho UK mail-routing endpoints; this alone is not proof that all storage or access is UK-only.
Upstash QStash, if enabled	Background job identifiers, step information and delivery metadata. Queue wake-up requests do not include source text, campaign images, names or review scores.	Task-delivery processor/subprocessor under the applicable Upstash agreement. Regional processing and transfers depend on the configured service.
Meta/Facebook, if connected	Page identifiers and access permissions, selected campaign text/images and scheduling or delivery information.	Connected publishing recipient; Meta has separate controller activities under its own terms and notices. Its international operations and applicable terms govern that processing. It is not represented as our processor for all activities.
Apple, Google, Mozilla or Microsoft browser push service, if enabled	Device push endpoint, encrypted notification payload and technical delivery information.	The provider selected by your device/browser delivers notifications under its applicable terms; its own controller activities and international infrastructure may apply.
GoDaddy domain routing/forwarding, while used	Technical requests to a forwarded hostname, such as IP address, requested address and browser information; it does not provide the campaign workspace.	Domain infrastructure provider with its own service/privacy terms and international processing. Public DNS currently uses GoDaddy nameservers.

Provider documents: ChatGPT Sites DPA, OpenAI API DPA, OpenAI subprocessors, Cloudflare privacy information, Microsoft DPA, Resend DPA, Zoho DPA information, Upstash DPA, Meta privacy information, GoDaddy privacy information.

Further supplier details, including the applicable contracting entity, service locations, safeguards and available contractual evidence for a particular organisational arrangement, can be requested from hello@glossavia.co.uk. They must be settled before processing that requires additional authorisation or safeguards. New services are not authorised merely because the software could connect to them.

AI-provider controls

OpenAI API: text-generation and text/image-checking requests use store: false where implemented, limiting retained application response state. This is not a Zero Data Retention guarantee. OpenAI's published API policy says API inputs and outputs are not used for general model training by default unless the account holder opts in. Its standard abuse-monitoring rules can retain relevant data for up to 30 days, with endpoint-specific and legal/safety exceptions. No special Zero Data Retention approval or account-specific regional arrangement is claimed here. We do not authorise model-training use of customer personal information through our service terms.

Microsoft Azure Translator: the implementation submits text to the Translator text-translation service. Microsoft's published policy says submitted text is processed without being stored by that translation service. This does not mean Glossavia's saved sources and translations, or separate operational records, are immediately deleted.

We use only the information needed for the requested task, keep credentials on the server, and restrict sensitive source material as described in section 4. Human review remains necessary for campaign use. Provider retention and safety rules are distinct from our own retention rules in section 10.

Provider information: OpenAI API data controls, Azure Translator privacy.

8. International processing

Providers may process information, or permit access to it, outside the UK. We do not describe the service as UK-only hosting. The register above explains the known processing arrangements, including US storage by relevant providers and resource-dependent routing. It does not promise that data stays in the UK.

Where we initiate a restricted transfer, it must be supported by applicable UK adequacy regulations, appropriate safeguards such as the UK International Data Transfer Agreement or UK Addendum, or a lawful exception used only where its conditions are met. Where required, a data protection test or transfer risk assessment and any necessary additional measures must be completed before the restricted transfer. Our notice does not represent that a bespoke assessment or regional arrangement exists for every possible customer use. You may request information about safeguards or a copy by emailing us, subject to necessary protection of confidential information.

9. Security and access

Glossavia uses invitation-only accounts and assigned roles and permissions. The account implementation uses password hashing, secure session cookies, sign-in rate limiting and HTTPS. Service credentials and connected Page tokens use encrypted storage in the application. These measures do not mean that every stored record is separately encrypted or that the service has independent security certification.

We apply security appropriate to the processing, restrict access to people who need it for their role and handle personal data incidents under applicable law and customer agreements. No online service can guarantee absolute security. Protect your credentials and report suspected misuse promptly.

10. How long do we keep information?

The following rules describe how we determine and review retention. Deletion is managed by the operator and relevant providers; it is not presented as an automatic expiry of every stored copy. Customer instructions, a separate signed participant notice or a specific legal requirement may require a different documented period. We review necessity rather than retaining every record for the longest period in the list.

- **Unsuccessful or inactive enquiries:** up to 12 months after the last substantive contact. Relevant correspondence about an established contractual relationship may be retained with its business records.
- **Unused invitations:** review after 30 days and withdraw if no longer required; remove unnecessary invitation records following that review. Password-setup/reset links have a separate configured one-hour validity. Minimal security evidence may follow the log rule below.
- **Active accounts:** for the period of authorised access. Disable access promptly when it ends; review and delete or minimise inactive account details within 90 days. Necessary agreement, contribution or audit evidence follows the separate rules below.
- **Routine technical and security logs:** review necessity at least every 90 days and remove or minimise records no longer needed. Provider infrastructure logs follow their applicable service rules. Records needed for a specific incident, complaint, contractual audit or claim may be retained for that purpose and the applicable limitation period.
- **Customer source and campaign records:** for the agreed service period and the customer's documented retention instructions. Unless agreed otherwise, allow a 30-day export period after termination and delete or return production copies within 30 days after that period ends, subject to legal preservation requirements.
- **Facebook access tokens:** while the authorised connection is needed. Disconnect and remove unnecessary active credentials promptly; retain old credentials only where strictly necessary to resolve an existing delivery operation, then remove them. Minimal delivery evidence follows the campaign or business-record rule. Deleting our copy does not remove records held independently by Meta.
- **Notification subscriptions:** while enabled and needed; remove the server-side subscription when disabled or when an invalid subscription is identified. Browser-side removal follows the browser's controls.
- **General contractual, billing and necessary rights-request or complaint evidence:** normally up to six years after the relevant relationship or matter ends, unless a different legal period applies. Retain only the evidence needed, rather than every attachment or working copy.
- **Independently organised contributor records:** review identifiable review material and routine support correspondence for deletion or anonymisation within 12 months after the contribution activity ends. Under existing participation arrangements, signed agreements and the minimum contribution and audit evidence may be kept for up to ten years after participation ends, with annual necessity reviews. This does not extend all account or campaign data to ten years.
- **Backups and provider copies:** copies held for recovery or service resilience follow the applicable provider arrangements, which can differ from active-system deletion. Access must be

restricted to the continuing lawful purpose and deletion instructions reapplied after restoration. We do not promise a universal 90-day backup expiry or immediate erasure of every provider copy. Ask us for the applicable arrangements for your information; any required customer-specific deletion commitment must be agreed before that processing.

We may retain genuinely anonymous aggregate information for longer. De-identification must be effective; merely removing a name may not make information anonymous. Any legal hold must be specific, access-restricted and reviewed. Retention dates are not a promise that all provider copies are erased instantly.

11. Your rights and choices

Depending on the processing and legal conditions, you may request access, correction, erasure, restriction or a portable copy of your information. You may object to processing based on legitimate interests, including explaining your particular circumstances. You may object to direct marketing at any time. Where processing relies on consent, you may withdraw it without affecting earlier lawful processing.

Content generation is not intended to make decisions about an individual that have legal or similarly significant effects. The service is not for individual screening eligibility or care decisions. Any proposed change involving significant automated decisions needs a separate assessment, notice and applicable safeguards.

Send requests to **hello@glossavia.co.uk**. We may ask for proportionate identity information. We respond without undue delay, normally within one calendar month, and explain any lawful extension or adjustment. Requests are normally free, subject to statutory exceptions. For information processed solely for a customer, we assist that customer with the response.

12. Complaints and changes

To raise a data protection complaint, email **hello@glossavia.co.uk**. We acknowledge complaints within 30 days, investigate without undue delay, keep you appropriately informed and communicate the outcome.

You can also complain to the Information Commissioner's Office (ICO), the UK's data protection supervisory authority: **ico.org.uk/make-a-complaint/**. You do not have to obtain our permission to contact the ICO.

We will review this policy when processing changes, notify affected people of material changes where required, and record a new effective date. A revised notice does not itself authorise a new use or replace any consent required. A future incorporated operator will require proper contractual and data-protection arrangements and appropriate notice.

Contact: hello@glossavia.co.uk
Copyright: © 2026 Glossavia.