Terms of Service

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

1. The operator and these terms

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

Website: glossavia.co.uk
Contact and notices: hello@glossavia.co.uk
Address for service and correspondence: 36 Hamilton Mansions, Barking Riverside, London, IG11 0BU, United Kingdom

The customer is the organisation or other contracting person named in the agreed order or service agreement. These terms are for business and professional use, rather than consumer supply. Any mandatory rights that apply remain unaffected. A person accepting for an organisation must have authority to do so.

A service contract is formed only when the customer expressly accepts these terms through an authorised acceptance process and we confirm the agreed service in writing, including by email. A written order signed or expressly accepted by both parties may also form the contract. Receiving an invitation, signing into an existing account or receiving a copy of these terms does not, by itself, create a paid subscription.

Invited users must follow the access, confidentiality and acceptable-use rules applicable to their account. An individual reviewer or volunteer does not become personally liable for an organisation's fees by receiving or using an account. Separate signed participation or confidentiality agreements continue to apply and are not amended by publishing these terms.

2. The service

The customer supplies programme information, typically in English. Glossavia prepares multilingual campaign posts, including captions, calls to action, image headlines, accessible image descriptions and campaign images that retain the organisation's identity.

Posts are organised on a coordinated 30-day calendar. Authorised users can preview posts and move planned dates by drag and drop. Where configured and authorised, posts can be scheduled for delivery to a connected Facebook Page. The agreed order may specify the particular functions or access supplied.

A planned date is distinct from confirmed delivery. A calendar entry alone does not confirm that a post has been scheduled with Facebook or published. The customer must check delivery status and resolve uncertainty before relying on publication.

We will provide the agreed service with reasonable care and skill. We do not promise particular screening attendance, uptake, health outcomes or campaign responses. Glossavia does not provide individual diagnosis, interpret screening results or determine individual eligibility for care.

3. Accounts and invitations

Access is invitation-only. The customer must supply accurate account information, appoint authorised users and allocate permissions appropriate to their responsibilities. Users must protect credentials, use their own account, comply with assigned permissions and promptly report suspected unauthorised access.

The customer is responsible for lawful instructions given by its authorised users and must request removal or amendment of access when a role changes or ends. Users must not share credentials or use another person's account to bypass restrictions. We may verify an instruction where necessary to protect the workspace.

4. Source content and approval

The customer must have the rights, permissions and lawful authority needed to supply and use its source documents, branding, images, personal information and other content. It is responsible for checking that its programme information is accurate, current, lawful and appropriate for the intended audience and purpose.

Before scheduling or publishing, the customer must obtain suitable factual, clinical and target-language review and final approval from people with the appropriate competence and authority. Checks must cover, as relevant:

- clinical meaning, eligibility, qualifications, benefits, limitations and informed choice;
- the distinction between screening, further assessment, diagnosis and seeking advice about symptoms;
- translations, terminology, numbers, contact details, calls to action and link destinations;
- the saved image, headline and accessible description, including whether the description matches the actual image;
- audience suitability, readability, inclusion and rights to use branding or assets.

An automated check, completed review task or generated draft does not replace appropriate final approval. Changes to content, source information or saved images require relevant checks to be renewed. Customer responsibilities do not remove our obligation to provide the service with reasonable care and skill.

5. Automated content and translation

Machine translation and generated text or images can be incomplete, misleading, inconsistent or wrong. Content that reads fluently can still alter clinical meaning or omit an important qualification. An output may not be unique and may resemble material generated for another user.

Human review is required before external use. Do not use the service as the sole basis for an individual clinical, eligibility, safeguarding or other significant decision. The customer remains responsible for its decision to publish or use approved material. People receiving a screening invitation should read the information supplied and contact their screening service with questions.

6. Acceptable use

The customer and its users must not:

- use the service unlawfully or to produce misleading, discriminatory, abusive or rights-infringing material;

- submit material they are not authorised to use or disclose;
- upload patient-identifiable records, individual screening results, or special category or criminal offence data without an express prior written arrangement and the necessary legal conditions and safeguards;
- introduce malware, probe or circumvent security, obtain unauthorised access, or interfere with the service or other users;
- misrepresent generated content as independently clinically approved, certified or endorsed where that is not established;
- extract or disclose another customer's confidential information, or reverse engineer protected elements except to the extent permitted by mandatory law;
- use connected services outside their permissions or applicable provider terms.

We may take proportionate protective action where reasonably necessary and explain the reason where lawful and safe to do so.

7. Content ownership and licences

The customer retains its rights in the content, sources, evidence, branding and assets it supplies. It grants us a non-exclusive licence to host, copy, process, translate, adapt, generate from, display and transmit that material only as needed to provide the agreed service, follow lawful documented instructions, and complete permitted return, deletion or legal preservation. Authorised providers may exercise the necessary parts of that licence for those purposes.

This licence does not authorise us to sell customer content, use it in our own advertising or permit general model training on customer personal information. Any materially different use requires a separate lawful arrangement. Provider terms must support the agreed processing before content is submitted.

We and our licensors retain rights in Glossavia's software, methods, reusable templates, design components, platform documentation and branding. Subject to the contract, the customer receives a non-exclusive, non-transferable right for its authorised users to access and use the agreed service during the contract. It may use exported campaign material as permitted below.

To the extent we own assignable intellectual property rights in customer-specific generated campaign output, we assign those rights to the customer when the output is created. This excludes our underlying platform and reusable materials, and third-party content. Where our retained materials are embedded in a lawful output, we grant a continuing, non-exclusive licence to use them as part of that output for the customer's campaign purposes, including after the service ends.

Third-party assets remain subject to their applicable licences. We do not guarantee that generated output is copyrightable, exclusive or free of third-party rights. These limits do not excuse any express obligation we agree concerning rights or reasonable care. Reviewer contributions supplied under a separate signed agreement remain governed by that agreement; these terms do not transfer them to another customer automatically.

8. Confidentiality

Each party must protect non-public information received from the other that is marked confidential or would reasonably be understood as confidential. It may use that information only for the contract and share it only with people or authorised providers who need it and are subject to appropriate confidentiality obligations.

The duty does not cover information shown to be lawfully public, already known without restriction, independently developed, or lawfully received from another source without restriction. Disclosure required by law is permitted, with prior notice where lawful and practicable and disclosure limited to what is required. Confidentiality continues after termination for as long as the information remains confidential. Separate signed confidentiality commitments are not reduced.

9. Data protection

Each party must comply with data protection law applicable to its activities. Our Privacy Policy explains processing for which we are controller. It is a notice and does not turn acceptance into consent for unrelated processing.

Where we process customer personal information on the customer's behalf, the processing schedule below forms part of the contract. If the customer is a processor, it must have authority from its controller to appoint us. An expressly agreed, more specific data processing agreement takes priority for its subject matter.

The customer must provide necessary information to individuals and ensure a valid lawful basis and any additional conditions. A processing contract or confidentiality agreement does not supply missing consent, authority or transparency.

10. Connected services and Facebook

The customer must have authority to connect a Facebook Page and grant the permissions needed for publishing. Third-party services have their own terms, permissions, technical limits and availability. The customer must maintain necessary authorisations and check the destination Page, timing and approved content before scheduling.

If an instruction is accepted by Facebook, publication may proceed without Glossavia remaining open. Disconnecting a Page or closing an account does not necessarily cancel a previously accepted scheduled post or remove a published post. The customer must confirm cancellation or removal with the destination service and ask for assistance where needed.

We are responsible for performing our agreed integration functions with reasonable care and skill. We cannot control a provider's independent processing, outages or changes; this does not exclude responsibility for our own breach.

11. Charges and commercial arrangements

No paid service is currently offered under these terms. Paid services may be introduced in due course, with no launch date or price promised here. Existing access does not automatically become a paid subscription.

Before any charge applies, the customer must expressly agree in writing to the service, price and currency, applicable VAT, payment dates, duration, renewal, cancellation and refund terms. No fee is payable and there is no automatic renewal or authority to take payment under these general terms alone. We will provide the relevant commercial terms before requesting agreement to a paid service.

Any later price change requires express agreement or a clearly agreed change process. An invited user, reviewer or volunteer does not become personally responsible for an organisation's fees by receiving an account.

12. Availability and support

We aim to operate the service reliably, but there is no guaranteed uptime, uninterrupted availability, fixed response time or service credit unless specifically agreed in writing. Maintenance, security action and provider disruption may affect access.

Contact hello@glossavia.co.uk for support. We will use reasonable care in investigating reported faults and take reasonable steps to communicate material disruption. The customer should retain suitable copies of essential source material and approved exports. This does not transfer our agreed backup, security or restoration obligations to the customer.

13. Suspension and ending the service

We may suspend affected access where reasonably necessary for security, unlawful use, a material breach, or a legal requirement. We will give prior notice where practicable, limit suspension to what is reasonably needed and restore access when the reason is resolved. For non-payment, suspension applies only to undisputed overdue charges after written notice and at least 14 days to pay or resolve the matter.

Either party may end the contract for a material breach that cannot be remedied or remains unremedied 30 days after written notice describing it. Immediate termination may be used where continued performance would be unlawful.

Unless an expressly agreed fixed term or cancellation arrangement applies, either party may end the service on 30 days' written notice. We may withdraw a feature or the service with reasonable notice, and will normally give at least 30 days where practicable. Where our withdrawal ends a prepaid service other than because of the customer's breach, we refund the unused prepaid portion unless a more favourable agreed remedy applies.

After termination, access ends except for any agreed export access. Unless otherwise agreed or prohibited by law, the customer has 30 days to request and receive a reasonably usable export. Production customer personal information is then returned or deleted within the following 30 days under the processing schedule. Lawfully required records and separately governed contribution records are handled under their applicable notices and agreements. Accrued rights, confidentiality, permitted output use and provisions intended to survive continue.

14. Liability

Nothing excludes or limits liability for death or personal injury caused by negligence; fraud or fraudulent misrepresentation; or any liability that cannot lawfully be excluded or limited.

Subject to those exceptions, each party's total aggregate liability to the other arising from the contract in a contract year, whether in contract, tort including negligence, breach of statutory duty or otherwise, is limited to the greater of **£5,000** and the total fees paid or payable for that contract year. A contract year is each successive 12-month period from the contract's start. Claims attributable to the same event or related series are allocated to the contract year in which the first relevant event occurred; they do not create a new cap in each later year.

Subject to the same exceptions, neither party is liable to the other for indirect or consequential loss. Direct loss, including reasonable direct data-recovery or remedial costs caused by a breach, is not automatically excluded merely because it concerns data or business activity; it remains subject to the lawful aggregate cap.

The cap does not reduce fees properly payable under the contract. Nothing limits an individual's statutory data protection rights, the powers of a regulator or any liability that law prevents the

parties from limiting. Allocation between the parties applies only to the extent legally permitted and reasonable. No indemnity or disclaimer overrides these safeguards.

The parties must take reasonable steps to mitigate recoverable loss. These provisions apply only so far as permitted by law, including applicable reasonableness requirements. They do not make the customer responsible for our negligence merely because it approved content.

15. Changes, notices and governing law

An agreed order prevails over an inconsistent general term where it expressly varies that term. The processing schedule or an agreed data processing agreement takes priority on its data protection subject matter. A change to an existing contract requires agreement or a change process already expressly agreed; publishing revised terms does not retrospectively amend it.

Operational and contractual notices may be sent by email to the parties' agreed contact addresses. The sender should retain evidence of delivery and seek acknowledgement for termination, breach or dispute notices. This does not replace rules for formal service of legal proceedings.

A future incorporation does not automatically substitute a different contracting party or transfer personal information without the necessary arrangements. Assignment or novation of the contract requires the other party's written consent, not to be unreasonably withheld where its rights and protections are maintained.

If a provision is unenforceable, the remainder continues to the extent lawful. Delay in exercising a right is not a waiver. Except where expressly agreed, a person who is not a party has no contractual enforcement right under the Contracts (Rights of Third Parties) Act 1999; individuals' statutory rights remain unaffected.

The contract and related non-contractual disputes are governed by the law of **England and Wales**. Its courts have exclusive jurisdiction, subject to any mandatory legal rights.

Customer data processing schedule

This schedule applies only to personal information processed on the customer's behalf. The security and provider register below forms part of this schedule. Additional customer-specific requirements must be agreed before the relevant processing. This schedule does not authorise patient-record processing.

A. Scope and instructions

The subject matter is preparation, storage, review and optional delivery of the customer's screening campaign material. Processing includes receiving, storing, generating, translating, organising, displaying, reviewing, exporting, transmitting and deleting information to provide the agreed service. The duration is the service period plus the agreed return/deletion period, except any retention required by UK law.

Expected data subjects are authorised staff, contractors, contributors and business contacts, and people lawfully and incidentally included in authorised campaign material. Expected data types are names, business contact details, authorised attribution or images, review comments, approval and delivery records, and other ordinary personal information specifically identified in lawful source material. Patient-identifiable, special category and criminal offence data are excluded unless a separate written arrangement describes them and establishes the required safeguards.

The customer determines the lawful purposes, accuracy, content and permitted use, provides required notices and permissions, and has the right and obligation to issue lawful documented instructions. The contract, agreed order and authorised workspace actions constitute instructions within this scope. We process only on those instructions, including for international transfers, unless UK law requires otherwise; we inform the customer of that requirement before processing unless legally prohibited.

We inform the customer promptly if an instruction, in our opinion, infringes applicable data protection law and may pause the affected processing while it is resolved.

B. People, security and assistance

We ensure people authorised to process customer personal information are bound by confidentiality or an appropriate statutory duty. We implement technical and organisational measures appropriate under Article 32 UK GDPR, considering risk, including authorised account access, role permissions, secure transport and session handling, credential protection, incident handling and appropriately tested continuity and restoration measures. The implemented measures and service limits are set out in the security schedule below; any additional requirements must be expressly agreed and supported before processing.

Taking account of the processing and information available to us, we assist the customer with individuals' rights requests through appropriate technical and organisational measures insofar as possible, and with its obligations for security, breach notification, data protection impact assessments and prior consultation. We notify the customer of a personal data breach affecting its data without undue delay after becoming aware, and provide available information and reasonable updates. We do not decide the customer's regulatory notification obligations for it.

Security schedule

The implemented controls include invitation-only accounts; assigned roles and permissions; server-side checks for workspace and protected-file access; password hashing; secure HttpOnly session cookies; password-reset links valid for one hour; session revocation after password reset; and application sign-in/reset rate limits. Passwords must meet the configured minimum of 12 characters.

The canonical site uses HTTPS. Service credentials and connected Page tokens are stored using application-level AES-GCM encryption. This is not a claim of end-to-end encryption of every campaign record. Optional web push uses encrypted payloads. Account and relevant workspace actions create audit records. Signed participation documents use protected downloads, rather than public asset URLs.

Access must be limited to authorised people and reviewed when a role or engagement ends. Report suspected incidents to hello@glossavia.co.uk. We will notify an affected controller of a personal data breach without undue delay after becoming aware and provide available information and reasonable updates. This does not promise a staffed 24-hour security operation or a particular incident response time.

Hosting storage, provider backups and recovery depend on the hosting service and any agreed organisational arrangement. We do not claim independent penetration testing, security certification, a tested disaster-recovery objective, separate tenancy for every organisation, a guaranteed restore point or automatic deletion of all historical copies. No patient-record or sensitive-data processing is authorised by this schedule. Any additional security or recovery requirement must be agreed and supported before the relevant processing begins.

C. Subprocessors and transfers

The customer gives general written authorisation for the relevant processor/subprocessor services identified in the provider and transfer register below, only to the extent necessary for the agreed functions and subject to lawful provider arrangements. Independent controller activities are identified separately and are not converted into subprocessing by this authorisation. Customer-specific entity, location or safeguard requirements must be settled before the affected processing; these terms do not authorise an otherwise unlawful transfer.

We give at least 30 days' prior written notice of an intended subprocessor addition or replacement, allowing a reasonable opportunity to object on substantiated data protection grounds. We work to resolve the objection; if no lawful, reasonable solution is possible, either party may end the affected service before the change and we refund unused prepaid charges for that service. If urgent action is needed to prevent unlawful or insecure processing, we may pause the affected service while seeking an authorised solution; urgency does not waive required authorisation.

We impose data protection obligations equivalent to the relevant obligations in this schedule by a binding written agreement with each subprocessor, including sufficient guarantees of appropriate technical and organisational measures. We remain fully responsible to the customer for a subprocessor's performance of those obligations. Restricted transfers require the customer's instructions and a lawful UK transfer mechanism, the applicable data protection test or assessment, and any necessary additional protections.

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.
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.

Service	Purpose and information involved	Role and international processing
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.

D. Evidence, audit and deletion

We make available information necessary to demonstrate compliance with Article 28 and allow and contribute to audits, including inspections, by the customer or its mandated auditor. Reasonable notice, confidentiality and security arrangements may protect other customers and systems, but must not make the statutory audit right ineffective or prevent urgent or regulatory action.

At the customer's choice, we delete or return customer personal information after the service ends, and delete existing copies unless UK law requires storage. The default timetable is a 30-day export period followed by production deletion within 30 days, unless the customer instructs lawful earlier deletion or the parties agree otherwise. Recoverable backups must be access-restricted, expire on the agreed verified schedule and have deletions reapplied after restoration. Provider backup retention varies; no universal 90-day expiry or independently tested recovery objective is promised. Any required backup-deletion deadline must be agreed and supported before processing. We must identify any continuing copy that cannot immediately be deleted, its lawful purpose and applicable retention arrangements, and restrict further use accordingly. We confirm completion on request and identify any lawful exception and its duration.

Contact for instructions or incidents: hello@glossavia.co.uk.

Copyright: © 2026 Glossavia.