Data Processing Addendum

Version 1.0, 14 November 2026

This Data Processing Addendum (the "Addendum") forms part of the GymAscend App Service Agreement (the "Agreement") between GymAscend Limited ("GymAscend") and the Customer. It applies whenever GymAscend processes personal data of Members and Staff on behalf of the Customer.

1. Scope and Roles

1.1 Terms defined in the Agreement have the same meaning in this Addendum. **"Data Protection Law"** means all laws on the protection of personal data that apply to the processing, including Regulation (EU) 2016/679 (the "GDPR"), the UK GDPR, US state privacy and consumer health data laws, Canada's Personal Information Protection and Electronic Documents Act and Australia's Privacy Act 1988. The terms "controller", "processor", "personal data", "processing" and "personal data breach" have the meaning given in the GDPR.

1.2 The Customer is the controller of the personal data of Members and Staff processed through the Services (or the "business" or "regulated entity" under US state laws). GymAscend is the Customer's processor (or "service provider").

1.3 GymAscend is established in Ireland. The provisions of the GDPR that apply to processors therefore apply to GymAscend for all processing under this Addendum, wherever the Customer is located.

1.4 GymAscend acts as an independent controller only for its own account, billing and contract records, for the security of the Services, and for the aggregated statistics described in Section 9.3 of the Agreement.

1.5 Annex 1 describes the processing.

2. Instructions

2.1 GymAscend shall process personal data only on the documented instructions of the Customer. The Agreement, this Addendum and the settings selected by the Customer in the Dashboard constitute those instructions.

2.2 GymAscend may process personal data otherwise only where required by law, and in that case shall inform the Customer beforehand unless the law prohibits it.

2.3 GymAscend shall inform the Customer promptly if, in its opinion, an instruction infringes Data Protection Law.

2.4 The Customer is responsible for the lawfulness of its instructions and for complying with its own obligations as controller under Data Protection Law, including giving any notice and obtaining any consent that is not collected through the App.

3. Confidentiality

GymAscend shall ensure that every person it authorises to process personal data is bound by an obligation of confidentiality and has access to personal data only to the extent needed to provide the Services.

4. Security

4.1 GymAscend shall implement the technical and organisational measures described in Annex 2. These measures are appropriate to the risk, taking into account that the personal data includes health data.

4.2 GymAscend may update these measures, provided that the overall level of protection is not reduced.

5. Subprocessors

5.1 The Customer authorises GymAscend to engage the subprocessors listed in Annex 3. GymAscend also publishes the current list on its website.

5.2 GymAscend shall give the Customer at least 30 days' notice, by email or in the Dashboard, before adding or replacing a subprocessor. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may terminate the Agreement by written notice and GymAscend shall refund any Fees prepaid for the period after the date of termination.

5.3 GymAscend shall impose on each subprocessor, by written contract, data protection obligations no less protective than those in this Addendum, and remains liable to the Customer for the performance of its subprocessors.

6. Assistance

6.1 **Data subject requests.** GymAscend shall provide the Customer with tools in the Dashboard, or with assistance on request, to respond to requests from Members to access, correct, delete, export or restrict the processing of their personal data, or to withdraw consent. If a Member contacts GymAscend directly, GymAscend shall forward the request to the Customer within 7 days and shall not respond to it itself, unless the Customer so requests or the law so requires. Members may also delete their account in the App.

6.2 **Consent records.** GymAscend shall keep, on behalf of the Customer, a record of each Member's acceptance of the Member Terms of Use and of the separate consent to the processing of health data, including the date, time and version accepted.

6.3 **Assessments.** GymAscend shall provide the information that the Customer reasonably needs to carry out a data protection impact assessment or to consult a supervisory authority in relation to the Services.

7. Personal Data Breaches

7.1 GymAscend shall notify the Customer without undue delay, and in any event within 48 hours after becoming aware of it, of any personal data breach affecting personal data that GymAscend processes on behalf of the Customer.

7.2 The notification shall describe, to the extent known, the nature of the breach, the categories and approximate number of individuals and records concerned, the likely consequences, and the measures taken or proposed. GymAscend shall provide further information as it becomes available.

7.3 GymAscend shall take reasonable steps to contain the breach and shall assist the Customer in meeting its own obligations to notify supervisory authorities and individuals, including under the GDPR and US breach notification and health data laws. The Customer decides whether and how to notify them, unless the law imposes that obligation on GymAscend directly.

8. Return and Deletion

8.1 For 30 days after termination of the Agreement, the Customer may request an export of the personal data in a standard format.

8.2 GymAscend shall then delete the personal data within 90 days. Copies held in backups are deleted as the backups expire, within a further 35 days, and remain protected until then.

8.3 GymAscend may retain personal data only where the law requires it, and shall then process it only for that purpose.

9. Audits

9.1 GymAscend shall make available to the Customer the information reasonably needed to demonstrate compliance with this Addendum, and shall respond to one written security questionnaire per year.

9.2 Where that information is not sufficient to meet a requirement of a supervisory authority, or following a personal data breach, the Customer may audit GymAscend's compliance with this Addendum, itself or through an independent auditor bound by confidentiality, on 30 days' written notice, during business hours and at the Customer's own cost. Audits are limited to one in any 12-month period, unless a supervisory authority requires more.

10. International Transfers

10.1 GymAscend may process personal data in the countries in which it and its subprocessors operate, as listed in Annex 3.

10.2 Where personal data subject to the GDPR or the UK GDPR is transferred to a country that is not covered by an adequacy decision, GymAscend shall rely on an approved transfer mechanism: the recipient's certification under the EU-US Data Privacy Framework (and its UK extension) where the recipient is certified, and otherwise the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with the UK Addendum where required.

10.3 Where the Customer is located outside the European Economic Area and GymAscend returns personal data to the Customer, Module Four (processor to controller) of those Standard Contractual Clauses applies to the extent required by the GDPR and is incorporated into this Addendum by reference. For that purpose, the governing law and the competent courts are those of Ireland.

10.4 If a transfer mechanism ceases to be valid, GymAscend shall adopt another valid mechanism without undue delay.

11. US State Law Terms

11.1 Where US state privacy or consumer health data laws apply, including those of California, Connecticut, Nevada and Washington, GymAscend:

1. shall process personal data only for the business purposes set out in the Agreement and this Addendum;
2. shall not sell or share personal data and shall not use it for targeted advertising;
3. shall not retain, use or disclose personal data outside its direct business relationship with the Customer, or combine it with personal data from other sources, except as those laws permit;
4. shall process consumer health data only under this Addendum and on the Customer's instructions;
5. shall provide the same level of privacy protection as those laws require of the Customer, and shall notify the Customer if it can no longer meet its obligations; and
6. shall assist the Customer in responding to consumer requests.

11.2 GymAscend certifies that it understands these restrictions and shall comply with them.

12. General

12.1 This Addendum remains in force for as long as GymAscend processes personal data on behalf of the Customer.

12.2 Each party's liability under this Addendum is subject to the limitations in Section 13 of the Agreement, except to the extent that Data Protection Law does not permit such a limitation.

12.3 In the event of conflict between this Addendum and the rest of the Agreement in relation to personal data, this Addendum prevails. Where the Standard Contractual Clauses apply and conflict with this Addendum, the Standard Contractual Clauses prevail.

Annex 1: Details of the Processing

Item	Details
Subject matter and duration	Provision of the Services under the Agreement, for its duration and the return and deletion period in Section 8
Nature of processing	Collection, storage, hosting, organisation, analysis (including automated scoring of engagement), generation of training plans and nutrition estimates, AI chat responses, messaging, export and deletion
Purposes	Operating the App and the Dashboard for the Customer; personalised training and nutrition features; class booking; messaging between coaches and Members; community feed; indicating to Staff which Members may need attention; support and security
Data subjects	Members, aged 16 or over; Staff
Personal data	Name, email, sign-in identifiers (Google, Apple), profile photo, membership details declared in the App, gym code, workout plans and logs, class bookings, messages with Staff, community reactions, AI assistant conversations, engagement and at-risk scores, device and usage data, badge or access identifier if the feature is used
Health data (special category)	Body weight and measurements, injuries and limitations, fitness goals, meal photos and nutrition estimates, and health information that Members choose to share with the AI assistant. Processed only with the Member's explicit consent, which the Member may withdraw in the App
Frequency	Continuous
Retention	For as long as the Member holds an account, then deleted within 30 days; health data deleted within 30 days after consent is withdrawn; all personal data deleted in accordance with Section 8 when the Agreement terminates

Annex 2: Security Measures

- All traffic between the App, the Dashboard and the servers is encrypted with TLS.
- The database and file storage are kept on storage encrypted at rest by the hosting provider.
- The database is not reachable from the internet. Only the application server can connect to it.

- Passwords are stored as salted hashes, never in plain text. Sign-in uses expiring tokens.
- Requests are rate-limited to slow down attacks, and standard security headers are applied.
- Each gym's data is kept logically separate, with access checks on every request. Staff see only what their role allows.
- Multi-factor authentication is enabled on every administrator account used to run the Services (hosting, code repository, AI provider, email provider).
- Server access uses personal SSH keys only, limited to the persons who need it.
- Automatic daily snapshots of the server are taken, encrypted and kept for no more than 35 days.
- Security updates are applied to servers and dependencies on a regular schedule.
- AI providers are used under terms that prohibit them from training their models on Member data.
- Every person with access is bound by confidentiality, and a written incident procedure is used for the notifications in Section 7.

Annex 3: Subprocessors

Subprocessor	Service	Location of processing
Amazon Web Services, Inc.	Server and database hosting (Lightsail), file storage (S3), account and notification emails (SES)	United States (us-east-1)
Anthropic (Anthropic Ireland, Limited as contracting entity)	AI assistant, plan and message drafts, meal photo analysis	United States
Google LLC (Firebase)	Push notifications, sign-in with Google	United States
Apple Inc.	Push notifications on iOS, sign-in with Apple	United States
Independent contract developer (an individual, bound by the European Commission's Standard Contractual Clauses). Identity disclosed to the Customer on request	Maintenance, bug fixing and support, with access to production systems	Pakistan