GymEzy SaaS Services Agreement

Admin platform agreement for gyms, fitness clubs and business customers

Last updated: 7 June 2026

Provider: Managezy Limited

Registered Business Name: GymEzy

CRO registration number: 812735

Registered office: 46 Enterprise Centre, Lavery Avenue, Park West Business Park, Dublin 12, D12 PP48, Ireland

Website: www.gymezy.eu

Contact: help@gymezy.eu

VAT number: not yet issued; will be provided once registered.

This document is intended to apply to the English-language version of the GymEzy service. Where a Hungarian version is also made available, both versions are intended to have the same meaning. If an Order Form or signed agreement specifies a prevailing language, that clause will take priority.

1. Parties and structure

This SaaS Services Agreement ("Agreement") is entered into between Managezy Limited, trading as GymEzy, and the business customer identified in the applicable order form, proposal, online sign-up, invoice or other ordering document ("Customer").

The Customer must be a business, gym, fitness club, studio or other organisation. The GymEzy SaaS platform is not sold directly to private individuals as a consumer subscription.

This Agreement applies together with any accepted order form, pricing plan, data processing terms and other schedules expressly incorporated by reference. If there is a conflict, a signed order form takes priority, followed by this Agreement, followed by any online policy.

2. Key definitions

"Admin Platform": the GymEzy web-based administration environment used by Customer owners, managers, reception staff, trainers and maintenance users.

"Member App": the GymEzy mobile application made available to members of the Customer.

"Services": the SaaS platform, Member App, support, hosting, maintenance and related functionality provided by the Provider.

"Customer Data": all data, content, records and information submitted to, stored in or generated by the Services on behalf of the Customer.

"Personal Data": has the meaning given to it in the GDPR and includes any equivalent concept under applicable data protection law.

"Order Form": any written, electronic or online order accepted by both parties or otherwise accepted through the Provider's sign-up process.

3. Scope of the Services

The initial Services include the following modules and functionality, subject to the selected plan and configuration:

- Member App;
- staff and reception administration;
- owner dashboard;
- trainer module;
- maintenance module;
- marketing automation for push and in-app system messages;
- AI churn prediction based on aggregated or anonymised trends;
- QR code and PIN based access functionality without a gate-control hardware module;
- staff shift and overtime tracking; and
- optional payment collection integration through Stripe.

The Services do not include SMS services, SMS marketing, e-mail newsletter services, gate control hardware, physical gate integration, direct gate actuation, trainer payout or earnings reporting, unless a separate written schedule expressly states otherwise.

iBeacon functionality is optional and is not part of the standard launch scope. The Services may include location tracking where enabled by the Customer and the relevant user, but do not include proximity/iBeacon tracking by default.

4. Subscription term, renewal and cancellation

The Services are provided on a monthly subscription basis. The subscription renews automatically each month unless terminated in accordance with this Agreement.

The Provider will send a renewal confirmation reminder to the Customer at least one (1) month before the next renewal date, summarising the upcoming renewal, the applicable fee and the cancellation option. Receipt of the reminder is not a condition for renewal.

There is no free trial unless expressly stated in an Order Form. There is no minimum fixed term unless expressly agreed in writing.

Either party may terminate the subscription for convenience by giving at least 30 days' written notice.

Fees paid are non-refundable, including where the Customer elects to terminate during a paid subscription month, except where mandatory law requires otherwise.

5. Fees, invoicing and payment

The Customer must pay the fees specified in the applicable Order Form or pricing plan. Fees are exclusive of VAT and other taxes unless expressly stated otherwise. The Provider's VAT number is not yet issued and will be provided once registered.

Payment processing is handled through Stripe where card or online payment functionality is used. The Provider does not store full card numbers or card security codes.

If any undisputed amount is overdue, the Provider may suspend access to the Services after giving reasonable notice. If non-payment continues, the Provider may terminate the subscription and handle Customer Data in accordance with clause 17.

The Provider may change pricing by giving at least 30 days' notice. The updated pricing will apply from the next renewal period after the notice period, unless otherwise agreed.

6. Customer responsibilities

The Customer is responsible for its use of the Services, the accuracy and legality of Customer Data, the configuration of user permissions, and the conduct of its owners, managers, staff, trainers, maintenance users and members.

The Customer must ensure that it has an appropriate legal basis for collecting and processing any Personal Data submitted to the Services, including member, staff, trainer and maintenance worker data.

The Customer is responsible for gym membership terms, class rules, health and safety rules, refunds to members, gym access decisions, pricing to members, and all communications sent to members through the Services.

The Customer must not use the Services to store health data, injury data, medical condition data, fitness assessment data, body composition data, heart rate data or other special category data unless a separate written agreement and compliant configuration have been approved by the Provider.

7. User accounts and access control

The Services use role-based access control. The Customer is responsible for assigning appropriate roles to its users and for promptly removing access when a user no longer requires it.

Only manager-level and owner-level users may access payment-related information made available within the Services. Trainers can access only the member data associated with their own classes or assigned participants, according to the configuration selected by the Customer.

Administrator multi-factor authentication is supported and must be used where required by the Provider's security configuration or the Customer's internal policies.

The Customer must keep account credentials confidential and must notify the Provider promptly if it suspects unauthorised access.

8. Marketing automation and member communications

The Services may enable the Customer to send push notifications and in-app messages to members. SMS services and e-mail newsletters are not included in the standard Services.

Examples of system messages include membership expiry notices, class reminders, inactive member notifications, promotion or offer notifications configured by the Customer, and churn-risk related operational notifications.

The Customer is solely responsible for determining whether a message is a service message, transactional notice or marketing communication under applicable law, and for obtaining, recording and retaining any required consent or other lawful basis.

The Provider does not send its own marketing communications to the Customer's gym members unless separately agreed and lawfully authorised.

9. AI analytics and churn prediction

The AI churn prediction feature is designed to produce business-level trend insights, such as the number of members who joined, the number of members who cancelled and how frequently members attend.

The AI feature is not designed to use identifiable Personal Data, does not create individual member profiles, and does not make decisions that produce legal or similarly significant effects for members.

The Customer decides whether to enable the AI module. The AI module may be disabled by the Customer where the selected plan and configuration permit.

Where an AI provider such as the Anthropic Claude API is used, the Provider intends to submit only anonymous or aggregated data and not identifiable Personal Data.

10. Hosting, infrastructure and subcontractors

The core Services are hosted in Hungary on servers operated by Work Mit Uns Kft. in the ATW server hotel at H-1117 Budapest, Hauszmann Alajos u. 3. Work Mit Uns Kft. also provides the e-mail (SMTP) and push notification delivery infrastructure used by the Services.

The Provider may use subcontractors and service providers to provide hosting, database operation, e-mail delivery, push notification infrastructure, payment processing, security, support and AI analytics. The current key service providers include Work Mit Uns Kft., Stripe Payments Europe Ltd and Anthropic (Claude API), subject to the limitations described in this Agreement, the Privacy Policy and the Subprocessor List.

No SMS provider is used for the standard Services. No support chat tool is included in the standard Services.

The Provider will ensure that subcontractors processing Personal Data on behalf of the Customer are bound by written data protection obligations that are substantially equivalent to those required by applicable data protection law.

11. Security

The Provider will implement appropriate technical and organisational measures to protect Customer Data against unauthorised access, accidental loss, destruction, damage and unlawful processing.

The current security measures include role-based access control, administrator MFA, encrypted databases, encrypted backups, audit logs, daily and monthly backups, and disaster recovery backups to a separate server.

The incident response contact is help@gymezy.eu. The Provider will notify the Customer without undue delay and, where feasible, within 72 hours of becoming aware of a Personal Data breach affecting Customer Data.

12. Support and service levels

The Provider will provide support during standard support hours of 9:00 to 17:00 on business days, with 24/7 availability for critical incidents where operationally required.

The Provider aims to respond to support requests within one hour. Response time is not a guarantee of final resolution time.

The Provider targets 99.5% service availability measured annually, excluding planned maintenance, emergency maintenance, Customer-side failures, third-party outages outside the Provider's control, internet connectivity failures and force majeure events.

Planned maintenance will be notified at least one week in advance where reasonably practicable.

13. Intellectual property rights

All rights, title and interest in and to the Services, software, source code, object code, user interface, databases, documentation, trade marks and know-how belong to the Provider or its licensors.

The Customer receives a limited, non-exclusive, non-transferable, non-sublicensable right to access and use the Services during the subscription term for its internal business operations.

The Customer retains ownership of Customer Data. The Customer grants the Provider the rights necessary to host, process, transmit, display and otherwise use Customer Data solely to provide, secure, maintain and improve the Services in accordance with this Agreement.

14. Confidentiality

Each party must keep confidential all non-public information disclosed by the other party that is marked confidential or would reasonably be understood to be confidential, including business, technical, commercial, financial and security information.

Confidential information may be used only for the purpose of performing this Agreement and may be disclosed only to personnel, professional advisers and subcontractors who need to know it and are bound by appropriate confidentiality obligations.

The confidentiality obligations do not apply to information that is publicly available, independently developed, lawfully received from a third party without restriction, or required to be disclosed by law.

15. Data protection

For gym member data and Customer staff, trainer and maintenance worker data processed through the Services, the Customer acts as controller and the Provider acts as processor, except where the Provider processes data for its own independent purposes described in the Privacy Policy.

The Data Processing Terms in Schedule 2 form part of this Agreement and govern the processing of Personal Data by the Provider on behalf of the Customer.

The Customer authorises the Provider to process Personal Data to provide the Services, maintain security, provide support, generate backups, perform troubleshooting, comply with lawful instructions and delete or return data following termination.

16. Suspension

The Provider may suspend access to all or part of the Services if:

- the Customer fails to pay undisputed fees when due;
- the Customer or its users materially breach this Agreement;
- suspension is necessary to protect the security, integrity or availability of the Services;
- the Customer's use creates a legal or regulatory risk for the Provider; or
- suspension is required by law or a competent authority.

The Provider will use reasonable efforts to give prior notice of suspension where practicable, unless immediate suspension is required for security, legal or operational reasons.

17. Termination and data export

Either party may terminate this Agreement for material breach if the breach is not remedied within 14 days after written notice, or immediately where the breach is incapable of remedy or creates serious security, legal or financial risk.

On termination or expiry, the Customer may request export of Customer Data. The Customer has 30 days to specify where the backup or export should be sent. If the Customer does not provide instructions within that period, the Provider may delete the data.

After the applicable retention period, the Provider will delete or anonymise Customer Data unless legal retention obligations require continued storage.

18. Warranties and disclaimers

The Provider warrants that it will provide the Services with reasonable skill and care and in substantial accordance with this Agreement.

The Provider does not warrant that the Services will be uninterrupted, error-free, compatible with all Customer systems, or capable of meeting every business requirement of the Customer.

The Customer is responsible for verifying that the Services are suitable for its business operations, regulatory obligations and member management model.

19. Liability

Neither party excludes or limits liability for fraud, fraudulent misrepresentation, wilful misconduct, death or personal injury caused by negligence, or any liability that cannot lawfully be excluded or limited.

Subject to the previous sentence, the Provider will not be liable for indirect, incidental, special, punitive or consequential loss, loss of profit, loss of revenue, loss of business opportunity, loss of goodwill, loss of anticipated savings, business interruption, reputational damage or loss arising from third-party services.

Subject to the exclusions above, the Provider's total aggregate liability arising out of or in connection with this Agreement is limited to the fees paid by the Customer to the Provider during the 12 months immediately preceding the event giving rise to the claim.

For data loss, the Provider's obligation is limited to restoring data from the most recent available backup, where such backup is available and technically recoverable.

Unless expressly stated in an Order Form, the Provider does not represent that any specific professional indemnity or cyber insurance policy is maintained, and any insurance held by the Provider does not increase the liability limits in this Agreement.

20. Force majeure

Neither party will be liable for delay or failure to perform caused by events beyond its reasonable control, including natural disasters, war, civil unrest, labour disputes, acts of government, power failures, internet failures, hosting outages, cyberattacks not caused by the affected party's negligence, and failures of third-party providers.

21. Notices

Notices to the Provider must be sent to help@gymezy.eu or by post to 46 Enterprise Centre, Lavery Avenue, Park West Business Park, Dublin 12, D12 PP48, Ireland. Notices to the Customer may be sent to the e-mail address associated with the Customer's account or stated in the Order Form.

E-mail notices are deemed received on the next business day after sending, unless the sender receives an automated delivery failure notice.

22. Governing law and jurisdiction

This Agreement and any dispute or claim arising out of or in connection with it, including non-contractual disputes or claims, are governed by the laws of Ireland.

The Irish courts have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement.

Schedule 1 - Service level summary

- Availability target: 99.5% annually.
- Support hours: 9:00 to 17:00 business days, with 24/7 availability for critical incidents.
- Response target: less than one hour for initial response.
- Planned maintenance notice: at least one week where reasonably practicable.
- Backups: daily and monthly encrypted backups, with disaster recovery backups stored on a separate server.
- Renewal reminder: at least one month before the next renewal date.

Schedule 2 - Data Processing Terms

1. Subject matter and duration

The Provider processes Personal Data on behalf of the Customer for the duration of the subscription and any post-termination period required for export, deletion, backup restoration, legal compliance or dispute handling.

2. Nature and purpose of processing

The processing consists of hosting, storing, organising, displaying, transmitting, securing, backing up, deleting and otherwise processing Personal Data as necessary to provide the Services.

3. Categories of data subjects

- Gym members;
- Customer owners, managers, reception staff and administrators;
- trainers;
- maintenance workers;
- Customer contacts and support contacts.

4. Categories of Personal Data

Gym member data may include name, e-mail address, telephone number, date of birth, gender, optional profile photograph, membership data, payment status or transaction references where payment features are enabled, check-in history, attendance logs, class bookings, trainer-member communications and workout history depending on the membership package.

Staff, trainer and maintenance worker data may include name, mother's name, date of birth, address, tax number, payroll identifier, bank details, emergency contact, telephone number and e-mail address.

The Services are not designed to collect health data, injury data, medical condition data, fitness assessments, body weight, body fat, heart rate data, minor children's data or parental consent records.

5. Processor obligations

The Provider will process Personal Data only on documented instructions from the Customer, unless required to do otherwise by law. The Provider will ensure that persons authorised to process Personal Data are bound by confidentiality obligations.

The Provider will implement appropriate technical and organisational measures, assist the Customer with data subject requests where reasonably possible, assist with Personal Data

breach notifications where required, and delete or return Personal Data after termination in accordance with this Agreement.

6. Subprocessors

The Customer authorises the Provider to use subprocessors necessary to provide the Services, including hosting, database, payment, e-mail, push notification and AI analytics providers. The current subprocessors are listed in the GymEzy Subprocessor List. The Provider remains responsible for subprocessors to the extent required by applicable data protection law.

7. International transfers

Core hosting is located in Hungary. The Provider does not intentionally transfer gym member Personal Data outside the EEA as part of core hosting. If a transfer outside the EEA becomes necessary, the Provider will ensure that appropriate safeguards are implemented in accordance with applicable data protection law.

8. Audit

The Provider will make reasonable information available to demonstrate compliance with these Data Processing Terms. Any audit must be reasonable, proportionate, subject to confidentiality, limited to once per calendar year unless required by law or following a serious incident, and must not compromise the security of other customers or the Services.

Schedule 3 - Security measures

- role-based access control;
- administrator MFA;
- audit logs;
- encrypted databases;
- encrypted daily and monthly backups;
- backup copies on a separate server for disaster recovery;
- restricted payment data visibility to manager and owner roles;
- incident response contact at help@gymezy.eu;
- member data export restricted by default, with full export available through authorised Customer request; and
- prompt Customer notification of Personal Data breaches affecting Customer Data, where feasible within 72 hours of becoming aware.