SaaS Services Agreement

Admin platform agreement for field service management and business customers

Last updated: 7 June 2026

- **Provider:** Managezy Limited
- **Registered Business Name:** OperatEzy
- **CRO registration number:** 812735
- **Registered office:** 46 Enterprise Centre, Lavery Avenue, Park West Business Park, Dublin 12, D12 PP48, Ireland
- **Website:** www.operatezy.com
- **Contact:** help@operatezy.com
- **VAT number:** not yet issued; will be provided once registered.

This document is intended to apply to the English-language version of the OperatEzy 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 OperatEzy, 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 corporate business entity, field service provider, utility company, multi-site operator, or other commercial organisation. The OperatEzy SaaS platform is not sold directly to private individuals as a retail consumer subscription.

This Agreement applies together with any accepted order form, commercial pricing plan, data processing terms and alternative schedules expressly incorporated by reference. If a direct conflict arises, a signed custom order form takes priority, followed by this Agreement, followed by any online web policy.

2. Key definitions

- **"Admin Platform":** The OperatEzy web-based backend administration environment utilized by Customer owners, operations managers, dispatchers, supervisors, and administrative personnel.
- **"Mobile App" (also referred to as "Field App"):** The OperatEzy mobile application made available to field workers, remote staff, and site technicians of the Customer.

- **"Services":** The unified SaaS platform, Mobile App, maintenance updates, customer technical support, underlying hosting, and related system functionality provided by the Provider.
- **"Customer Data":** All data, content, digital records, task configurations, photos, signatures, and operational information submitted to, stored in, or generated by the Services on behalf of the Customer.
- **"Personal Data":** Has the meaning assigned to it in the General Data Protection Regulation (GDPR) and includes any equivalent legal concept under applicable local data protection law.
- **"Order Form":** Any written, electronic, or online digital order accepted formally by both parties or otherwise completed through the Provider's digital sign-up interface.

3. Scope of the Services

The standard Services include the following primary modules and digital system functionality, subject to the customer's selected commercial plan and system configuration:

- Mobile App / Field App;
- Workforce management and dispatcher scheduling administration;
- Real-time executive owner and operations dashboards;
- Task assignment and checklist modules;
- Compliance and multi-site maintenance tracking modules;
- Automated internal workflow notifications (push alerts and in-app system messages);
- AI operational analytics and optimization metrics based on aggregated or anonymised trends;
- Digital QR code and PIN-based site check-in functionality (operating independently without direct physical gate-control hardware modules);
- Field staff shift logging and overtime tracking features; and
- Optional integrated corporate platform payment collection through Stripe.

The standard Services explicitly do not include general commercial SMS services, external SMS marketing, customer email newsletter engines, physical entry gate control hardware, physical facility gate hardware integration, direct remote gate actuation, field worker direct payout or earnings payroll execution reporting, unless a separate written bespoke schedule states otherwise. Proximity/iBeacon tracking functionality is an optional add-on and is not part of the standard core software launch scope. The Services may include geographic location tracking where explicitly enabled by the Customer and authorized by the respective end-user, but do not include proximity/iBeacon tracking arrays by default.

4. Subscription term, renewal and cancellation

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

The Provider will send a automated renewal confirmation reminder to the Customer at least one (1) month prior to the upcoming renewal date, summarising the upcoming renewal transaction, the applicable fee tier, and structural cancellation options. Receipt of the reminder is not a strict legal condition for renewal enforcement.

There is no complimentary free trial unless explicitly executed in a written Order Form. There is no minimum fixed lock-in term unless explicitly agreed in writing between the corporate parties. Either party may terminate the active subscription for convenience by serving at least 30 days' formal written notice. All fees paid are non-refundable, including instances where the Customer elects to terminate midway through a paid subscription month, except where mandatory territorial law requires otherwise.

5. Fees, invoicing and payment

The Customer must pay the specific fees outlined in the applicable Order Form or active digital pricing plan. All fees are exclusive of VAT and equivalent local taxes unless explicitly stated otherwise. The Provider's VAT number is not yet officially issued and will be formally provided to the Customer once registration is finalized.

All automated payment processing is securely handled via Stripe where credit card or electronic payment functionality is utilized. The Provider does not store full credit card account numbers or card security codes (CVVs) on its own infrastructure.

If any undisputed financial invoice remains overdue, the Provider reserves the right to suspend corporate access to the Services after giving reasonable formal notice. If non-payment continues, the Provider may terminate the software subscription and handle remaining Customer Data in strict accordance with clause 17. The Provider may adjust active pricing by giving at least 30 days' prior written notice. The adjusted pricing will take effect from the next renewal period following the notice timeline, unless otherwise negotiated.

6. Customer responsibilities

The Customer maintains sole responsibility for its overall use of the Services, the accuracy, propriety, and legality of all submitted Customer Data, the internal configuration of granular user role permissions, and the professional conduct of its owners, managers, staff, supervisors, maintenance technicians, and field workers.

The Customer must guarantee that it possesses a valid, legal basis for collecting and processing any Personal Data submitted into the Services, including field worker profiles, supervisor logs, tax details, and attendance tracking information.

The Customer remains fully responsible for its own employment or service terms, task rules, health and safety protocols, refunds or payouts to field workers, physical site access decisions, independent pricing models to its client base, and all workplace communications sent to field workers through the platform.

The Customer must not use the Services to store employee health records, occupational injury data, medical condition files, clinical fitness assessment information, biometric physical datasets, minor children's data, or equivalent special category data unless a specific written addendum and compliant configuration have been reviewed and approved by the Provider.

7. User accounts and access control

The Services utilize strict role-based access control (RBAC). The Customer is responsible for assigning appropriate operational roles to its users and for promptly removing system access privileges when a user no longer requires them for their job duties.

Only authorized manager-level and owner-level administrative accounts may access billing, payment, or corporate subscription information within the platform. Field staff and site technicians can access only the specific task data, checklists, or compliance files associated with their own schedules or assigned locations, according to the configuration selected by the Customer.

Administrator multi-factor authentication (MFA) is fully supported and must be actively utilized where mandated by the Provider's security configuration or the Customer's internal data governance policies. The Customer must keep all account login credentials highly confidential and must notify the Provider immediately if it suspects a system account compromise or unauthorized platform access.

8. Workflow notifications and field communications

The Services provide functionality enabling the Customer to dispatch operational push notifications and in-app system messages to remote personnel. Standard consumer SMS marketing services and public email newsletters are not included in the standard core Services.

Examples of supported system messages include shift updates, urgent task reminders, safety warnings, inactive user flags, compliance submission prompts, and operational field notices configured by the Customer.

The Customer is solely responsible for determining whether a message constitutes a routine internal service message, an operational transactional notice, or an external marketing communication under local telecommunication laws, and for obtaining, recording, and retaining any required consents or explicit opt-out records. The Provider

does not dispatch its own direct marketing communications to the Customer's field personnel unless separately agreed and lawfully authorized.

9. AI operational analytics and metrics

The integrated AI optimization and analysis feature is engineered to generate high-level commercial trend insights, such as aggregate historical task completion metrics, general multi-site attendance frequencies, and scheduling compliance patterns across different regions.

The AI feature is explicitly not designed to process identifiable Personal Data, does not assemble intrusive consumer-style profiles, and does not execute automated workforce decisions that yield adverse legal or similarly significant effects for individual natural persons. The Customer maintains total discretion over whether to enable the AI optimization module. The AI module may be toggled off by the Customer where the selected plan tier and software configuration permit.

Where an AI subprocessor infrastructure provider such as the Anthropic Claude API is engaged, the strict architectural design dictates that only fully anonymised, structured data or aggregated metadata is submitted, completely excluding identifiable personal identifiers.

10. Hosting, infrastructure and subcontractors

The core Services are physically hosted in Hungary on secure 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 underlying transactional email (SMTP) relays and push notification infrastructure utilized by the platform.

The Provider may utilize third-party subcontractors and cloud service providers to deliver hosting, database operations, email delivery, mobile notification frameworks, payment processing, information security, customer support, and AI analytical processing.

The current key infrastructure subprocessors include Work Mit Uns Kft., Stripe Payments Europe Ltd, and Anthropic (Claude API), subject to the strict architectural limitations described in this Agreement, the Privacy Policy, and the formal Subprocessor List. No commercial consumer SMS gateway provider or external live customer support chat tools are integrated into the standard core Services.

The Provider guarantees that all subcontractors processing Personal Data on behalf of the Customer are legally bound by written data protection obligations that are substantially equivalent to, or more rigorous than, those required by applicable European data protection law.

11. Security

The Provider will deploy and maintain robust technical and organisational security controls engineered to safeguard Customer Data against unauthorized access, accidental loss, structural destruction, physical damage, and unlawful processing.

The active security measures encompass strict role-based access control (RBAC), mandatory administrator multi-factor authentication (MFA), comprehensive encryption of databases at rest, encrypted transit of system backups, operational audit logging, daily and monthly automated backups, and isolated disaster recovery backups mirrored to a separate secure server node.

The dedicated information security and incident response desk is accessible via help@operatezy.com. The Provider will formally notify the Customer without undue delay and, where feasible, within 72 hours of becoming aware of a verified Personal Data breach impacting Customer Data.

12. Support and service levels

The Provider will deliver customer technical support during standard business hours of 9:00 to 17:00 on official business days, with 24/7 technical engineering availability reserved exclusively for critical server-down incidents where operationally required.

The Provider targets an initial response window of less than one hour for standard support requests. Initial response time metrics constitute a target and do not provide a legally binding guarantee of final technical resolution time.

The Provider targets a 99.5% software platform availability rate measured over an annualized cycle, explicitly excluding planned maintenance downtime, emergency security maintenance, Customer-side network failures, third-party global outages outside the Provider's direct infrastructure control, public internet routing failures, and force majeure occurrences. Planned maintenance windows will be announced to the Customer at least one week in advance where reasonably practicable.

13. Intellectual property rights

All rights, title, and interest in and to the cloud Services, software applications, underlying source code, compiled object code, administrative user interfaces, databases, product documentation, trade marks, and operational know-how belong exclusively to the Provider or its corporate licensors.

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

The Customer retains absolute ownership of all Customer Data. The Customer grants the Provider the non-exclusive right necessary to host, process, transmit, parse, display, and

otherwise utilize Customer Data solely to provide, secure, maintain, troubleshoot, and improve the operational performance of the Services in accordance with this Agreement.

14. Confidentiality

Each party must preserve the absolute confidentiality of all non-public information disclosed by the other party that is marked confidential or would reasonably be understood to be of a confidential nature, including corporate business strategies, proprietary source code, commercial pricing tables, financial metrics, and infrastructure security details.

Confidential information may be used only for the express purpose of executing rights or obligations under this Agreement and may be disclosed only to internal personnel, corporate professional advisers, and approved subcontractors who maintain a strict need-to-know basis and are legally bound by appropriate, equivalent non-disclosure confidentiality obligations.

Confidentiality restrictions do not apply to information that becomes publicly available through no fault of the receiving party, is independently developed without reference to the disclosure, is lawfully received from a third party without restriction, or is explicitly required to be disclosed by formal operation of law or a binding court order.

15. Data protection

For all field worker, technician, supervisor, and staff data processed through the Services, the Customer acts as the legal Data Controller and the Provider acts as the Data Processor, except where the Provider handles corporate information for its own independent business purposes as detailed in the Privacy Policy.

The *Data Processing Terms* detailed in Schedule 2 form an inseparable part of this Agreement and comprehensively govern the processing of Personal Data by the Provider on behalf of the Customer. The Customer explicitly authorizes the Provider to process Personal Data to provide core platform services, maintain infrastructure security, deliver technical support, generate automated snapshots and backups, perform system troubleshooting, comply with lawful judicial instructions, and delete or return corporate data following subscription termination.

16. Suspension

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

- The Customer fails to settle undisputed financial fees when they fall due;
- The Customer or its authorized users execute a material breach of this Agreement;
- Suspension is deemed critical to protect the overall security, systemic integrity, or operational availability of the infrastructure;

- The Customer's specific system usage pattern creates an imminent legal or regulatory liability risk for the Provider; or
- Suspension is mandated by formal operation of law or a competent government authority.

The Provider will employ reasonable efforts to provide prior notice of suspension where operationally practicable, unless immediate technical suspension is required for emergency security, statutory legal, or critical operational reasons.

17. Termination and data export

Either party may terminate this Agreement for material breach if the underlying breach is not remedied within 14 days following receipt of detailed written notice, or immediately where the material breach is legally incapable of remedy or creates an imminent security, legal, or financial liability risk.

Upon subscription termination or natural contract expiry, the Customer may formally request the extraction and export of its raw Customer Data. The Customer has a window of 30 days to explicitly specify where the data export package or system backup should be securely transmitted. If the Customer fails to provide clear destination instructions within that 30-day timeline, the Provider is authorized to permanently delete the data from all production arrays.

Following the finalization of the applicable technical retention period, the Provider will permanently delete or thoroughly anonymise Customer Data unless explicit legal retention obligations mandate continued corporate storage.

18. Warranties and disclaimers

The Provider warrants that it will deliver the cloud Services with reasonable professional skill and care, and in substantial alignment with this Agreement. The Provider does not warrant that the software platform will be entirely uninterrupted, completely error-free, compatible with every localized Customer network system, or capable of meeting every single idiosyncratic business optimization requirement of the Customer.

The Customer maintains sole business responsibility for independently verifying that the cloud Services are structurally suitable for its commercial field operations, regulatory compliance obligations, and internal workforce management model.

19. Liability

Neither party excludes or limits its liability for fraud, fraudulent misrepresentation, wilful misconduct, death or personal injury caused directly by negligence, or any other category of liability that cannot lawfully be excluded or limited under Irish law.

Subject to the preceding sentence, the Provider will not be held liable under any circumstances for indirect, incidental, special, punitive, or consequential losses, loss of commercial profit, loss of business revenue, loss of corporate opportunity, loss of brand goodwill, loss of anticipated fiscal savings, workplace business interruption, reputational damage, or data losses arising from third-party hardware or routing services.

Subject to the exclusions outlined above, the Provider's maximum total aggregate liability arising out of or in connection with this Agreement, whether in contract, tort (including negligence), or otherwise, is strictly limited to the cumulative fees paid by the Customer to the Provider during the 12 months immediately preceding the specific event giving rise to the legal claim.

For instances of unexpected data loss, the Provider's absolute obligation is strictly limited to restoring data records from the most recent available automated system backup, where such backup is physically available and technically recoverable. Unless explicitly executed in a written 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 operate to expand the financial liability caps established in this Agreement.

20. Force majeure

Neither party will be liable for an operational delay or failure to perform obligations under this agreement caused by events entirely beyond its reasonable control, including natural disasters, acts of war, civil unrest, labor disputes, emergency acts of government, regional power grid failures, public internet routing failures, third-party hosting outages, cyberattacks not caused by the affected party's negligence, and systemic failures of public utility providers.

21. Notices

Formal legal notices directed to the Provider must be sent via email to **help@operatezy.com** or delivered via post to: 46 Enterprise Centre, Lavery Avenue, Park West Business Park, Dublin 12, D12 PP48, Ireland.

Notices directed to the Customer may be sent directly to the email address associated with the Customer's primary administrative account or stated explicitly in the baseline Order Form. Email notices are deemed received on the next consecutive business day after transmission, provided the sender does not receive an automated delivery failure metadata bounce.

22. Governing law and jurisdiction

This Agreement and any dispute or claim arising out of or in connection with it, its subject matter, or its formation (including non-contractual disputes or claims) are governed exclusively by, and construed in accordance with, the laws of Ireland.

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

Schedule 1 - Service level summary

- **Availability target:** 99.5% measured annually.
- **Support hours:** 9:00 to 17:00 on business days, with 24/7 emergency infrastructure coverage for critical platform-down incidents.
- **Response target:** Less than one hour for initial technical response tracking.
- **Planned maintenance notice:** At least one week in advance where reasonably practicable.
- **Backups:** Daily and monthly encrypted database backups, with isolated disaster recovery backups stored on a separate server node.
- **Renewal reminder:** Dispatched at least one month prior to the upcoming renewal cycle.

Schedule 2 - Data Processing Terms

1. Subject matter and duration

The Provider processes Personal Data on behalf of the Customer for the active duration of the commercial subscription and any post-termination window required for data export, final deletion, backup restoration cycles, legal compliance archiving, or dispute handling.

2. Nature and purpose of processing

The data processing consists of secure cloud hosting, storage, indexing, display formatting, transmission routing, cryptographic securing, automated backing up, final deleting, and otherwise processing Personal Data as structurally necessary to provide the field service management platform features.

3. Categories of data subjects

- Customer employees, field workers, technicians, remote staff, and contractors;
- Customer owners, regional managers, dispatchers, supervisors, and platform administrators;
- Multi-site maintenance workers and third-party service personnel;
- Customer contacts and software support contacts.

4. Categories of Personal Data

Field worker and staff data records may include name, email address, telephone number, account login credentials, assigned schedules, task histories, check-in timestamps,

attendance logs, site checklists, uploaded operational signatures or photos, and payment status references where payment modules are active.

Supervisor, dispatcher, and maintenance worker data may include name, mother's name, date of birth, home address, tax identifier number, payroll identifier, corporate bank account details, emergency contacts, telephone numbers, and email addresses.

The Services are explicitly not engineered to collect health data, injury logs, medical records, clinical fitness metrics, biometric identifiers, minor children's data, or parental consent records.

5. Processor obligations

The Provider will process Personal Data strictly on documented instructions from the Customer, unless compelled to do otherwise by applicable EU or Irish law. The Provider will guarantee that all internal personnel authorized to process Personal Data are bound by binding confidentiality agreements.

The Provider will implement appropriate technical and organisational security measures, assist the Customer with data subject rights requests where technically feasible, assist with Personal Data breach notifications where required by law, and systematically delete or return Personal Data after termination in accordance with this Agreement.

6. Subprocessors

The Customer provides generalized authorization to the Provider to engage subprocessors necessary to deliver the Services, including hosting providers, database operators, electronic payment gateways, email relays, mobile notification engines, and AI analytics infrastructure. The active subprocessors are publicly registered in the *OperatEzy Subprocessor List*. The Provider remains fully liable for the data processing performance of its subprocessors to the extent required by applicable data protection law.

7. International transfers

Core cloud infrastructure hosting is physically located within Hungary (EEA). The Provider does not intentionally transfer field worker Personal Data outside the EEA as part of its core hosting environment. If an international transfer outside the EEA becomes required for enterprise expansion integrations, the Provider will guarantee that appropriate safeguards are implemented in strict accordance with Chapter V of the GDPR.

8. Audit

The Provider will make reasonable information available to the Customer to demonstrate compliance with these Data Processing Terms. Any audit request must be reasonable, proportionate, subject to strict confidentiality, limited to once per calendar year unless

required by law or following a serious security incident, and must never compromise the data security of other platform tenants or the integrity of the core Services.

Schedule 3 - Security measures

- Multi-tenant data segregation with role-based access control (RBAC);
- Mandatory administrator multi-factor authentication (MFA);
- Comprehensive backend system audit logs and access histories;
- Full cryptographic encryption of databases at rest;
- Encrypted daily and monthly data backups;
- System backups mirrored securely to a separate physical server node for disaster recovery;
- Restricted payment and billing data visibility limited exclusively to manager and owner roles;
- Incident response desk contact available at help@operatezy.com;
- Administrative data export controls restricted by default, with comprehensive export tools available only through authorized Customer credentials; and
- Prompt Customer notification of verified Personal Data breaches affecting Customer Data, where feasible within 72 hours of initial discovery.