Privacy Policy

Privacy notice for the website, SaaS platform, admin users and Mobile App users

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. Introduction

This Privacy Policy explains how Managezy Limited, trading as OperatEzy, collects, uses, stores, shares and protects personal data in connection with the OperatEzy website, SaaS admin platform, Mobile App (Field App) and related services.

We process personal data in accordance with the General Data Protection Regulation (GDPR), applicable Irish data protection law and, where relevant, equivalent UK data protection rules.

This Privacy Policy should be read together with the Website Terms and Conditions, SaaS Services Agreement, Mobile App Terms of Use, Cookie Policy, Subprocessor List, Data Subject Rights & Account Deletion Procedure and Complaints Procedure.

2. Who we are

The provider is Managezy Limited, an Irish limited company registered with the CRO under number 812735, with registered office at 46 Enterprise Centre, Lavery Avenue, Park West Business Park, Dublin 12, D12 PP48, Ireland.

- **Registered Business Name:** OperatEzy.
- **Website:** www.operatezy.com.
- **Contact e-mail:** help@operatezy.com.

For privacy questions, requests or complaints, please contact us at help@operatezy.com.

3. Controller and processor roles

For most personal data processed through the OperatEzy platform on behalf of a business client, the client company is the controller and Managezy Limited is the processor.

This includes staff data, scheduling data, task tracking, multi-site attendance logs, compliance documents, proof of work data, operational logs, and field worker information entered into or generated through the Services. The business client decides why and how this data is processed. If you are a field technician, team member, supervisor, or staff member of a business using OperatEzy, you should normally contact your employer or contracting organisation first to exercise your data protection rights.

Managezy Limited acts as controller for its own business data, including website enquiries, customer account administration, billing, technical support, platform security, fraud prevention, product analytics based on anonymous or aggregated data, and business-to-business communications with prospective or current corporate clients.

4. Personal data we collect

4.1 Website visitors and business contacts

We may collect contact details, corporate information, enquiry notes, technical system logs, IP address, browser metadata and communications submitted through our website forms or via corporate email channels.

4.2 Corporate customers and administrative users

We may process names, job titles, business email addresses, professional telephone numbers, account credentials, granular role permissions, customer organisation structures, SaaS subscription information, billing details, invoices, support tickets, operational audit logs, and security logs.

4.3 Field staff and mobile workers using the Mobile App

Depending on the corporate customer's system configuration, we may process name, email address, telephone number, account credentials, shift assignments, scheduling dependencies, task statuses, uploaded proof of work data (such as signatures, photos, or operational logs), task checklists, compliance declarations, and active attendance check-ins.

4.4 Multi-site supervisors and operations personnel

Where the business customer uses the respective operational modules, we may process name, mother's name, date of birth, address, tax number, payroll identifier, corporate

bank details, emergency contacts, telephone number, email address, shift logs, overtime records, site access histories, and specific multi-site maintenance or service assignments.

4.5 Location data

Where location-based features are explicitly enabled by the business client (such as for automated site check-in verification, mileage verification, or proximity-based proof of work), geographical location data may be processed to support field accountability, operational security, and fraud prevention. Proximity/iBeacon tracking is not deployed by default.

4.6 Data we do not intentionally collect

The Services are not designed to collect or store health metrics, medical condition data, fitness assessments, biometric physical data, minors' data, or parental consent records.

5. Purposes and legal bases

Where we act as **controller**, we process personal data for the following purposes and on the following legal bases:

- **Website enquiries:** Legitimate interests or pre-contractual steps.
- **Customer contracts:** Performance of a contract.
- **Support workflows:** Performance of a contract and legitimate business interests.
- **Security and fraud prevention:** Legitimate interests to safeguard the infrastructure.
- **Legal compliance:** Compliance with a legal obligation.
- **Product analytics:** Legitimate interests based purely on anonymised or heavily aggregated technical data.

Where we act as **processor**, the corporate business customer determines the relevant legal basis. This may include performance of an employment or service contract, legitimate business operational interests, legal compliance obligations, or direct consent, depending entirely on the customer’s regulatory use case and applicable employment/labour law.

6. Corporate communications and internal notifications

OperatEzy does not provide external B2C marketing SMS services or email newsletters to consumer end-users as part of its standard service.

The platform allows business managers to send operational push notifications and in-app system messages to field personnel. These messages include shift updates, urgent task reminders, safety alerts, compliance submission prompts, and internal operational status updates configured by the corporate customer.

The business client is solely responsible for establishing the legal basis for such internal workplace communications, managing opt-outs where legally appropriate, and maintaining required compliance records. Managezy Limited does not issue its own marketing to our clients' field personnel unless separately authorized and legally permissible.

7. AI analytics and predictive metrics

The built-in AI operational analytics and optimization functionality is engineered to evaluate aggregate, macro-level business operational trends, such as historical task completion rates, scheduling compliance patterns, and workforce productivity metrics across sites.

The AI module is explicitly not designed to process unmasked, identifiable personal data, does not build intrusive personal consumer profiles, and does not execute automated decisions that yield adverse legal or similarly significant effects for natural persons. Where an AI infrastructure provider such as the Anthropic Claude API is engaged, the strict architectural protocol dictates that only anonymised, structured, or aggregated metadata is transmitted rather than raw personal identifiers.

8. Sharing personal data

We may share personal data with the following recipients only where necessary and strictly lawful:

- The specific **corporate business client** that controls and manages the relevant staff, technician, supervisor, or operations data;
- **Work Mit Uns Kft.**, which provides the underlying core cloud hosting, databases, email (SMTP) relays, and push notification infrastructure in Hungary;
- **Stripe Payments Europe Ltd**, where corporate SaaS B2B billing or related financial functionality is active;
- **Anthropic (Claude API)**, strictly for processing anonymous or aggregated technical operational analytics data where configured;
- **Professional advisers**, including legal counsel, corporate auditors, accountants, and commercial insurers;
- **Courts, regulatory bodies, public authorities, and law enforcement agencies** where explicitly compelled by binding law;
- **Successors or prospective corporate purchasers** in connection with a verified merger, acquisition, corporate restructuring, or sale of business assets.

A comprehensive, current register of approved subprocessors is maintained in the *OperatEzy Subprocessor List*, available online at www.operatezy.com/legal or via request to help@operatezy.com. **We do not sell personal data.**

9. International transfers

Core infrastructure hosting is physically located in Hungary, inside the European Economic Area (EEA). The current architectural design of the service does not require the intentional, persistent transfer of primary field service personal data outside the EEA for core system hosting.

Where specific enterprise optimization configurations route data through the Anthropic Claude API and involve paths outside the EEA, only fully anonymised or aggregated system data is transferred, relying upon Standard Contractual Clauses (SCCs) or alternative approved lawful transfer frameworks. If any other international data transfer outside the EEA or the UK becomes operationally necessary, we will ensure rigorous legal compliance via adequacy decisions, Standard Contractual Clauses, or appropriate statutory legal mechanisms.

10. Data retention

We retain personal data only for the duration necessary to satisfy the specific operational purposes for which it was gathered, unless a prolonged retention window is mandated by statutory regulation. Standard corporate retention rules include:

- **Business lead data:** Up to 3 months if the enterprise prospect does not convert into an active customer;
- **Terminated corporate accounts:** 30 days post-termination, subject to finalized client data export and deletion procedures;
- **Field staff/user app data:** Retained throughout active account utilization and, if rendered inactive, up to 90 days unless the corporate controller or the individual requests expedited deletion, and provided no conflicting statutory preservation order applies;
- **Multi-site attendance and security access logs:** Maintained for the duration of platform use, unless distinct customized retention thresholds are set within the software by the business client, or required by law;
- **Financial billing, transaction, and invoice data:** Maintained for the duration of the commercial relationship and subsequent mandatory fiscal archiving timelines (typically 6 to 8 years under Irish corporate accounting law);
- **System backups:** Preserved within automated daily and monthly operational backup cycles, and securely overwritten via normal backup rotation protocols.

Where the corporate business client acts as the data controller, they possess the system ability to set custom data retention metrics within the outer limits of applicable law.

11. Security and breach notification

We implement robust technical and organisational safeguards engineered to protect platform data. These safeguards encompass strict role-based access controls (RBAC), mandatory administrator multi-factor authentication (MFA), comprehensive encryption of databases at rest and backups in transit, granular operational audit logs, daily and

monthly secure snapshots, disaster recovery protocols to geographically isolated secure nodes, and highly restricted payment visibility.

However, no cloud transmission vector or digital storage medium can be guaranteed as entirely infallible. In the event we become aware of an unauthorized data breach affecting Customer Data, we will formally alert the impacted corporate business client without undue delay and, where feasible, within 72 hours of initial discovery. Where we operate as the data controller for our primary commercial data, we will formally notify the Data Protection Commission (DPC) within 72 hours where mandated by Article 33 GDPR, alongside any impacted individuals as required by Article 34 GDPR.

12. Your rights

Subject to territorial data protection legislation and specific qualifying legal contexts, you may maintain the following data protection rights:

- The right of **access** to your structured personal data records;
- The right to **rectification** of faulty, incomplete, or outdated information;
- The right to **erasure** ("the right to be forgotten");
- The right to **restriction** of ongoing data processing;
- The right to structural **data portability**;
- The right to **object** to processing based upon legitimate corporate interests;
- The right to **withdraw consent** at any point where consent serves as the primary legal gateway;
- The right to not be subjected to automated profiling or individual decisions carrying legal or equivalent material consequence.

If your data is processed within the system on behalf of an employer or corporate partner, we may be required to formally route your query to that specific business client in their capacity as the data controller. We stand ready to comprehensively assist our business clients in fulfilling data subject rights requests under GDPR.

We strive to formally address all direct controller requests within one calendar month of receipt, which may be extended by up to two additional months for multi-layered or technically complex requests as authorized by Article 12(3) GDPR. Specific, granular workflow steps are outlined in our *Data Subject Rights & Account Deletion Procedure*.

13. Complaints

You are invited to contact our privacy desk directly at help@operatezy.com if you have any questions or procedural concerns regarding our corporate data workflows. Our formal internal escalation matrix is detailed in the *OperatEzy Complaints Procedure*.

You also maintain the fundamental legal right to submit an official grievance to an approved data protection supervisory authority.

- In **Ireland**, this is the **Data Protection Commission** (www.dataprotection.ie).
- In **Hungary**, this is the **Nemzeti Adatvédelmi és Információszabadság Hatóság** (NAIH, www.naih.hu).

You may also coordinate directly with your localized national supervisory body depending on your primary operational location.

14. Children

The OperatEzy field service management platform is strictly a business-to-business (B2B) enterprise service and is not intended for or directed towards minors. We do not intentionally process personal data belonging to children through the Mobile App and do not provide an explicit parental authorization workflow.

15. Cookies

Granular parameters surrounding cookie architectures and local browser storage are detailed in our standalone Cookie Policy. At operational launch, the public website and SaaS backend limit usage strictly to essential technical session variables, intentionally avoiding tracking pixels, commercial profiling arrays, or third-party behavioral analytics packages.

16. Changes to this Privacy Policy

We reserve the right to modify or refresh this Privacy Policy document over time. The updated copy will be deemed active immediately upon its digital publication on the website, unless a future enforcement date is expressly specified. In the event of material structural modifications to this policy, we will execute reasonable technical steps to alert active enterprise accounts where required by law.

17. Contact

Privacy-related queries, formal legal requests, or statutory notices may be directed to **help@operatezy.com** or dispatched via post to: Managezy Limited, 46 Enterprise Centre, Lavery Avenue, Park West Business Park, Dublin 12, D12 PP48, Ireland.