



Tyten Technologies Limited

Company Number 16101444

25 Eccleston Place, London, England, SW1W 9NF

Effective Date: 25 April 2026

Version: 2.0

Previous Version: 1.0 (10 September 2025)

Tyten AI Privacy Policy

1. Who We Are

This Privacy Policy applies to the services provided by Tyten Technologies Limited (“Tyten”, “we”, “us”, “our”), a company registered in England and Wales (Company No. 16101444), with its registered office at 25 Eccleston Place, London, England, SW1W 9NF.

We provide an AI-powered facilities management platform, including an AI helpdesk assistant, technician tools, an admin dashboard, mobile applications and backend integrations used by facilities management providers and their authorised end-users.

For any questions about this Privacy Policy or our processing of personal data, please contact us at privacy@tyten.ai.

2. Scope

This Privacy Policy applies to all users of the Tyten AI solution, including:

- Residents interacting via WhatsApp, mobile apps, or similar interfaces
- Technicians using the Tyten mobile apps and tools
- Facilities managers and admin staff using the dashboard
- FM providers as enterprise clients
- Tyten's internal users supporting or maintaining the platform

3. Data We Collect

We collect and process the following types of information:

Category	Examples
Personal identifiers	Names, phone numbers, emails
Repair request content	Issue descriptions, error codes
Photo/video uploads	Media submitted to describe or verify faults
Work order data	Equipment ID, fix steps, diagnostic results
Device/session metadata	Device type, IP address, WhatsApp metadata
Diagnostic usage data	Timestamps, prompt usage, button clicks
Building and asset data	Equipment lists, floor plans, asset metadata
Location data	GPS data or address info (e.g. for technicians)
Voice data	WhatsApp voice messages or transcripts

3.1. Data Collected via the Tyten Mobile Apps

When you use the Tyten mobile applications distributed on the Apple App Store and Google Play Store, we additionally collect:

- Authentication tokens stored on-device in the iOS Keychain or Android Keystore. These do not leave the device except as the Authorization: Bearer header on requests to our API.
- Photos and videos captured with your device's camera or chosen from your photo library when you attach them to a work order. We request camera, photo-library, and microphone permission only at the moment you tap the relevant control; the app does not access these continuously.
- Device identifiers (a non-resettable device model and operating-system version string) for crash diagnostics and to render the correct UI. We do not collect IDFA, AAID, or any cross-app advertising identifier.
- Push-notification tokens issued by Apple Push Notification service or Firebase Cloud Messaging, used solely to deliver work-order updates to your device.
- Approximate location (city-level) derived from the user's home building, only when the user explicitly attaches a location to a report. We do not continuously track GPS.

4. How We Use This Data

We process the above data to:

- Route and resolve maintenance issues using AI tools
- Assist technicians with diagnostics and task documentation
- Generate work orders and update CAFM systems
- Deliver and monitor service quality for client companies
- Improve system performance and user experience
- Provide support and respond to client inquiries

5. Legal Bases for Processing

We rely on the following legal grounds under UK GDPR and related laws:

- Contract performance – For processing necessary to deliver our services to clients
- Legitimate interests – For platform monitoring, improvement, and internal reporting

- Consent – For opt-in actions, such as WhatsApp messaging permissions

6. Sharing and Sub-Processing

We use selected service providers (sub-processors) to deliver the Tyten AI solution. The current sub-processors and the specific data shared with each are as follows:

Provider	Purpose
OpenAI, Anthropic, Google (Gemini)	AI inference for technician guidance: we send the work-order title, description, and any attached photo. The AI provider returns suggested tools and diagnostic steps. No user account identifier is sent. Data is processed under the provider's API terms (no model training on submitted content).
Meta (WhatsApp), Twilio	Communication interface for residents: phone numbers, message content, and delivery metadata used to send and receive WhatsApp/SMS messages.
AWS, GCP, Microsoft Azure	Hosting, storage, and server infrastructure for the platform and Customer Data.
Microsoft	Internal operations and productivity tooling (email, document storage) used to support the Services.
Folk CRM	Customer relationship management: contact details of client representatives and prospective clients.

These sub-processors are approved by default and do not require individual client approval. A full and up-to-date list is available on request from privacy@tyten.ai.

7. Retention of Data

We retain data only for as long as necessary to:

- Fulfil our service obligations under client contracts
- Meet legal and regulatory requirements
- Comply with internal data retention schedules

7.1 Individual User Deletion Requests

Individual users can request deletion of all personal data Tyten holds about them at any time, by either:

- opening the Tyten app and choosing Settings → Account → Request Account Deletion, or
- emailing privacy@tyten.ai from the address registered on the account.

We delete personal data within thirty (30) calendar days of the request, except where a longer retention period is required by law (e.g. financial-records retention) or to defend legal claims, in which case the data is anonymised. Anonymised aggregate analytics may be retained indefinitely. Backups are overwritten on our standard rolling schedule and are not used to restore deleted personal data.

7.2 Client Company Deletion and Export Requests

Client companies (enterprise customers) may additionally request export or deletion of all data associated with their tenant under their service agreement.

8. Data Security

We implement appropriate technical and organisational measures to protect personal data, including:

- Encryption in transit (TLS) and at rest
- Role-based access controls and least-privilege access
- Multi-factor authentication for administrative access
- Logging and monitoring of system access and security events
- Vulnerability management, patching, and secure development practices
- Incident response procedures and breach escalation
- Secure infrastructure provided by AWS, GCP, and Microsoft Azure
- Staff confidentiality undertakings and security awareness training

9. Your Rights

If your personal data is processed by Tyten, you may have the right to:

- Access your data

- Request correction or deletion
- Object to certain processing
- Request data portability
- Restrict processing in certain circumstances
- Withdraw consent at any time, where processing is based on consent
- Lodge a complaint with the UK Information Commissioner's Office (ICO) if you believe your data has been mishandled. The ICO's contact details are at <https://ico.org.uk/make-a-complaint/>. You may also complain to the supervisory authority of the EU member state where you live.

To exercise your rights, contact us at privacy@tyten.ai.

10. Updates to This Policy

This Privacy Policy may be updated to reflect legal, operational, or functional changes. Clients and affected users will be notified of material updates where applicable. The effective date and version number at the top of this document indicate when the latest version took effect.

11. Children's Data

The Tyten platform and mobile applications are intended for use by professional facilities-management staff and their authorised end-users, all of whom are adults in the course of their employment or residency. We do not knowingly collect personal data from children under 16. If we discover that we have inadvertently collected data from a person under 16, we will delete it within 30 days. Parents or guardians who believe a child has provided personal data should contact privacy@tyten.ai.

12. International Data Transfers

Several of our sub-processors (notably OpenAI, Anthropic, Google, Meta, Twilio, AWS, Microsoft, and Folk) host or process personal data in jurisdictions outside the United Kingdom and the European Economic Area, including the United States.

Where personal data is transferred outside the UK, we rely on one of the following safeguards mandated by UK GDPR Article 46:

- the UK International Data Transfer Agreement (IDTA), or the EU Standard Contractual Clauses with the UK Addendum, executed with each sub-processor that requires it;

- an adequacy decision issued by the UK Secretary of State, where one applies (for example, the UK-US Data Bridge for transfers to certified US recipients);
- explicit user consent, where neither of the above applies and consent is freely given.

A copy of the relevant transfer agreement is available on request from privacy@tyten.ai.

13. Automated Decision-Making and AI

Tyten uses third-party Large Language Models (currently OpenAI's GPT family, Anthropic's Claude family, and Google's Gemini family) to generate suggested tools, probable causes, and diagnostic steps for technicians. These suggestions are decision-support, not automated decisions: a human technician always reviews and applies them. We do not use AI to take decisions that have legal or similarly significant effects on individuals.

When the AI is invoked, we send the relevant work-order text and (where attached) photographs to the AI provider's API. We do not include the user's name, email, or any direct identifier in the prompt unless the user has typed one into the work-order description themselves. AI providers process this content under their own data-processing terms and do not train their public models on it.

Users have the right to obtain human review of any AI-generated guidance by contacting privacy@tyten.ai.

14. Contact

For any questions, concerns, or requests relating to this Privacy Policy or our processing of personal data, please contact:

Email: privacy@tyten.ai

Post: Tyten Technologies Limited, 25 Eccleston Place, London, England, SW1W 9NF

This policy supersedes all prior versions.