Privacy Policy

Organisation: Tyten Technologies Limited (trading as TYTEN; company number 16101444)
Version: 1.2
Effective Date: 2026-11-16
Last Updated: 2026-11-15

1. Data Controller

Tyten Technologies Limited ("we", "us", "our") is the data controller for the personal data of visitors to our website, users of their TYTEN accounts, our sales prospects, and the suppliers and others we correspond with on our own behalf. For the data our clients put into the TYTEN platform (their work orders, documents and emails, including details of their staff, suppliers and residents), we act as a processor on our clients' instructions under our agreement with each client; the client is the controller.

Detail	Information
Registered name	Tyten Technologies Limited (trading as TYTEN)
Product	TYTEN: Facilities Management SaaS Platform
Registered address	25 Eccleston Place, London, England, SW1W 9NF
Company number	16101444 (England and Wales)
Data Protection Officer	Not appointed: Tyten does not carry out the large-scale monitoring or special-category processing that makes a DPO mandatory under UK GDPR Article 37. Privacy enquiries go to the privacy lead, Serge Nasonov
Contact email	privacy@tyten.ai
ICO registration number	ZC021425 (registered 22 October 2025, renewal due 21 October 2027)

2. About This Policy

This Privacy Policy explains how we collect, use, store, share, and protect personal data when you use the TYTEN platform or interact with our services. It applies to:

- Clients and their employees who use the TYTEN platform
- Suppliers and subcontractors whose data is processed through TYTEN
- Residents whose personal data appears in work orders or building management records
- Visitors to our website
- Anyone who contacts us by email, phone, or other means

This policy is written in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

3. Types of Data We Collect

We collect and process the following categories of personal data:

3.1 User and Staff Data

Data	Purpose	Legal Basis
Name, email address, phone number	Account creation and management; user authentication	Contract performance
Username and password (hashed)	Platform access and authentication	Contract performance
Login history and IP addresses	Security monitoring; fraud detection; access auditing	Legitimate interest (security)
Session data	Maintaining authenticated sessions	Contract performance

3.2 Client and Tenant Data

Data	Purpose	Legal Basis
Client organisation name and contact details	Service delivery; account management	Contract performance
Site and building addresses	Work order management; asset tracking	Contract performance
Email domains	Automatic email routing and document classification	Contract performance

3.3 Supplier Data

Data	Purpose	Legal Basis
Supplier company name	Invoice processing; work order assignment	Contract performance
Supplier contact names, email addresses, phone numbers	Communication regarding invoices, work orders, and quotes	Legitimate interest (business operations)
Bank details (where provided via invoices)	Invoice processing and payment facilitation	Contract performance

3.4 Resident Data

Data	Purpose	Legal Basis
Resident name, phone number, email	Work order coordination; maintenance communication	Legitimate interest (property management)
Apartment/unit assignment	Work order routing; asset management	Legitimate interest (property management)

3.5 Financial Data

Data	Purpose	Legal Basis
Invoice amounts, numbers, and line items	Automated bill processing and accounting sync	Contract performance
Quote amounts and details	Quote management and approval workflows	Contract performance
Chart of accounts data	Accounting integration with Xero	Contract performance

3.6 Email Content

Data	Purpose	Legal Basis
Email subjects, body text, sender/recipient addresses	Document ingestion and classification; supplier communication	Contract performance; legitimate interest (service delivery)
Email attachments (invoices, job sheets, quotes)	Document processing; audit trail	Contract performance

3.7 Sales Prospects

Data	Purpose	Legal Basis
Business contact details of people at companies we may sell to, and where a sales representative requests it their mobile or direct line: name, job title, work email, phone numbers, LinkedIn profile	Business-to-business sales outreach by email and phone	Legitimate interest (B2B marketing). UK numbers are checked against the Telephone Preference Service and Corporate TPS, and a number on either register is flagged to the caller (calls are not blocked automatically). Anyone can opt out at any time
Sales call recordings and transcripts	Call quality, follow-up and training	Legitimate interest

This data comes from commercial data providers and public sources.

3.8 Technical Data

Data	Purpose	Legal Basis
Browser type, operating system, device information	Platform optimisation; troubleshooting	Legitimate interest (service improvement)
Error logs and diagnostic data	System reliability and debugging	Legitimate interest (service quality)

---

4. How We Use Your Data

We process personal data for the following purposes:

1. **Service delivery**: Operating the TYTEN platform, processing documents, managing work orders, generating quotes, and synchronising accounting data
2. **Communication**: Sending service-related notifications, supplier chasing emails, and work order updates
3. **Security**: Monitoring access, detecting fraud, preventing unauthorised use, and maintaining audit logs
4. **Compliance**: Meeting legal and regulatory obligations, including financial record-keeping
5. **Improvement**: Analysing usage patterns (aggregated and anonymised) to improve the platform

We use business contact data for business-to-business marketing as described in section 3.7. We do **not** use personal data for profiling or automated decision-making that produces legal effects.

5. Legal Basis for Processing

Legal Basis	Application
Contract performance (Article 6(1)(b) UK GDPR)	Processing necessary to deliver the TYTEN platform services under our agreements with clients
Legitimate interest (Article 6(1)(f) UK GDPR)	Security monitoring, fraud prevention, system improvement, and supplier communication where these interests are not overridden by data subject rights
Legal obligation (Article 6(1)(c) UK GDPR)	Financial record retention (7 years for accounting records); regulatory compliance
Consent (Article 6(1)(a) UK GDPR)	Only where specifically required (e.g., optional communications); consent may be withdrawn at any time

6. Data Sharing with Third Parties

We share personal data only with the following categories of processors, and only to the extent necessary for service delivery:

Processor	Data Shared	Purpose	Location	DPA in Place
Amazon Web Services (AWS)	All data (hosting)	Infrastructure: compute, storage, database hosting	United Kingdom (London, eu-west-2)	AWS Data Processing Addendum
Google (Gemini)	Document and email content, which can include names and contact details	AI document classification and data extraction; transcription of sales calls	United States / EU	Google Cloud data processing terms (coverage being confirmed)
Anthropic	Document and email content, which can include names and contact details	AI document analysis	United States	Anthropic commercial terms (DPA acceptance being confirmed)
OpenAI	Document and email content, which can include names and contact details	AI document classification and data extraction (secondary provider)	United States	OpenAI DPA (acceptance being confirmed)
Microsoft	Email content, sender/recipient addresses	Email processing via Exchange/Graph API	EU / United States	Microsoft DPA
Xero	Financial records and supplier data (on a client's instruction); our own clients' billing contacts and invoices	Accounting integration for clients; TYTEN's own invoicing	Australia, New Zealand, United States	Xero's terms

Processor	Data Shared	Purpose	Location	DPA in Place
Twilio	Prospects' phone numbers, call recordings	Sales calls	United States	Twilio DPA (being confirmed)
Apollo; folk; Instantly	Prospects' business contact details	Sales prospecting and outreach	United States / EU	Each provider's DPA (being confirmed)
TPS screening service	Prospects' phone numbers	Telephone Preference Service checks	United Kingdom	Provider's terms
Google Analytics	Website usage data (only with your consent)	Website analytics	United States	Google's data processing terms

Client-owned systems we connect to on a client's behalf (for example their CRM, CAFM or accounting system) are covered by the client's own agreement with that provider.

We do not sell personal data to any third party.

We are putting data processing terms in place with each processor, requiring them to process data only on our instructions, protect it, and tell us of a breach. The status of each, including those still being confirmed, is kept in our vendor register.

---

7. International Data Transfers

Some of our processors operate outside the UK:

Transfer	Destination	Safeguard
AI provider API calls (Google Gemini, Anthropic, OpenAI)	United States (and EU for Google)	The UK Extension to the EU-US Data Privacy Framework where the provider is certified; otherwise the UK International Data Transfer Addendum to the Standard Contractual Clauses in the provider's DPA. Only the content needed for the task is sent
Xero data sync	Australia / New Zealand / United States	Safeguards in Xero's terms
Microsoft 365	EU / United States	SCCs; Microsoft DPA
Sales tools (Twilio, Apollo, folk, Instantly) and Google Analytics	United States / EU	The UK Extension to the Data Privacy Framework or the transfer clauses in each provider's terms
AWS (primary)	United Kingdom (eu-west-2)	No transfer: data remains in UK

Where data is transferred outside the UK, we ensure appropriate safeguards are in place as required by Chapter 5 of the UK GDPR.

---

8. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law:

Data Category	Retention Period	Disposal Method
Security audit logs, email activity logs, AI usage logs, document processing logs	Kept as the record of what the platform sent, received and decided, from the date our nightly deletion job is switched off (planned November 2026). Until then, email activity logs are deleted after 6 months, security audit and AI usage logs after 1 year, and failed document-processing logs after 3 months	Not deleted after that date; reviewed if a legal or contractual reason requires it
Failed login attempts	Until the next successful login from the same username and address (used for account lockout); others are deleted after 6 months until the nightly deletion job is switched off	Cleared automatically
Business records (bills, quotes, invoices)	7 years	Manual review and secure deletion
User accounts (inactive)	Staff accounts with no login for 90 days are listed in our quarterly access review and deactivated unless there is a reason to keep them	Manual review
Database backups	Encrypted nightly backups 7 years; volume snapshots and the transaction log archive 400 days	Automatic expiry. Data deleted from the live database remains in backups until they expire
Sales prospect data	Contact details until the prospect opts out or is no longer relevant; call recordings and transcripts 12 months	Recordings and transcripts deleted automatically after 12 months; contact details on opt-out

When data reaches the end of its retention period it is deleted, or anonymised where we must keep a record that something happened.

---

9. Data Subject Rights

Under the UK GDPR, you have the following rights regarding your personal data:

Right	Description	How to Exercise
Access (Article 15)	Request a copy of the personal data we hold about you	Email privacy@tyten.ai
Rectification (Article 16)	Request correction of inaccurate or incomplete data	Email privacy@tyten.ai or update via the TYTEN platform
Erasure (Article 17)	Request deletion of your data where there is no compelling reason for continued processing	Email privacy@tyten.ai
Restriction (Article 18)	Request restriction of processing in certain circumstances	Email privacy@tyten.ai
Portability (Article 20)	Receive your data in a structured, commonly used, machine-readable format	Email privacy@tyten.ai
Objection (Article 21)	Object to processing based on legitimate interest	Email privacy@tyten.ai

Right	Description	How to Exercise
Withdraw consent	Withdraw consent at any time where processing is based on consent	Email privacy@tyten.ai

We will respond to all data subject requests within **30 days** of receipt. If a request is complex or we receive a high volume of requests, we may extend the response period by a further 60 days, and we will inform you of the extension within the initial 30-day period.

We will verify your identity before processing any request. We do not charge a fee for requests unless they are manifestly unfounded or excessive.

---

10. Security Measures

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

10.1 Technical Measures

Measure	Implementation
Encryption in transit	TLS 1.2+ for web traffic, API calls and email; database connections inside our cloud network are being moved to full certificate verification
Encryption at rest	AES-256 for document storage; database backups encrypted before upload; disk encryption on servers, except the root volumes of two older hosts (protected by compensating controls) and two volumes on stopped legacy hosts that are due for removal; Fernet encryption for API tokens and credentials
Access control	Role-based access with least-privilege principle; multi-factor authentication for administrative access
Multi-tenant isolation	Each client's data is kept separate from every other client's
Authentication	Minimum 12-character passwords; account lockout after 5 failed attempts; multi-factor authentication for staff; sessions end after 8 hours of inactivity (7 days if you choose "Remember me")
Logging and monitoring	Security audit logging; alerts on sensitive cloud account activity; brute-force protection on servers; file-integrity monitoring on our newest database server
Vulnerability management	Dependency scanning; security testing; timely patching

10.2 Organisational Measures

Measure	Implementation
Security policies	An information security policy framework aligned with SOC 2 and ISO 27001:2022 (preparing for both)
Staff training	A security awareness briefing within 30 days of joining and once a year; the first briefings are due by 31 December 2026

Measure	Implementation
Access reviews	A quarterly review of staff access rights, the first completing in Q4 2026; inactive staff accounts are deactivated unless the reviewer records a reason
Incident response	Documented incident response plan with defined severity levels and response procedures
Vendor management	Due diligence and ongoing monitoring of all third-party processors

11. Cookies

The TYTEN platform (app.tyten-services.com) uses only strictly necessary cookies:

Cookie	Type	Purpose	Duration
sessionid	Essential (first-party)	Maintains your authenticated session	8 hours, renewed while you are active; 30 days if you choose "Remember me" (you are still signed out after 7 days without activity)
csrftoken	Essential (first-party)	Protects against cross-site request forgery attacks	1 year

Our website (tyten.ai) uses essential cookies, Ahrefs analytics (which sets no cookies), and Google Analytics cookies (*ga, _ga**) only if you agree through the cookie banner. You can change your choice at any time from the banner.

12. Data Breach Notification

In the event of a personal data breach:

1. We will assess the breach within **24 hours** of becoming aware of it
2. If the breach is likely to result in a risk to your rights and freedoms, we will notify the **Information Commissioner's Office (ICO)** within **72 hours** as required by Article 33 of the UK GDPR
3. If the breach is likely to result in a **high risk** to your rights and freedoms, we will notify affected individuals **without undue delay** as required by Article 34 of the UK GDPR
4. We will document all breaches, including those that do not meet the notification threshold, in our incident register

Our full incident response procedures are documented in our Incident Response Plan.

13. Children's Data

The TYTEN platform is a business-to-business service and is not directed at children. We do not knowingly collect personal data from anyone under the age of 18. If we become aware that we have collected data from a child, we will delete it promptly.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. When we make material changes:

- We will update the "Last Updated" date at the top of this document
- For significant changes affecting how we process personal data, we will notify clients via email or an in-platform notification
- Previous versions of this policy are retained for reference

---

15. Complaints

If you are not satisfied with how we handle your personal data or your data subject request, you have the right to lodge a complaint with the Information Commissioner's Office:

Detail	Information
Organisation	Information Commissioner's Office (ICO)
Website	https://ico.org.uk
Telephone	0303 123 1113
Address	Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We encourage you to contact us first at privacy@tyten.ai so we can attempt to resolve your concern directly.

---

16. Applicable Law

This Privacy Policy and any disputes arising from it are governed by the laws of **England and Wales**. The courts of England and Wales have exclusive jurisdiction.

---

17. Contact Us

For any questions about this Privacy Policy or to exercise your data subject rights:

Channel	Details
Email	privacy@tyten.ai
Post	Privacy lead, Tyten Technologies Limited, 25 Eccleston Place, London, England, SW1W 9NF
Response time	Within 30 days for data subject requests; within 5 business days for general enquiries