

PRIVACY POLICY

Last Updated: 01/06/2026

1. INTRODUCTION

This Privacy Policy explains how **Syntari LTD**, a company incorporated in England and Wales (“Syntari”, “we”, “us”, or “our”), processes personal data in connection with:

- our websites
- our applications
- our SaaS platform(s)
- our Visitor Management and Site Access Logging Services (the “Services”)

This Privacy Policy applies where Syntari acts as a Data Controller. Where Syntari processes personal data on behalf of a Customer, Syntari acts as a Data Processor, and such processing is governed by the applicable Data Processing Agreement (DPA).

2. DATA CONTROLLER AND DATA PROCESSOR ROLES

2.1 DATA CONTROLLER ROLE

Syntari acts as a Data Controller in relation to:

- Website visitors
- Sales and marketing communications
- Business enquiries
- Account administration
- Platform usage telemetry (where applicable as controller data)

2.2 DATA PROCESSOR ROLE

When providing the Services to Customers, Syntari acts as a Data Processor and processes Customer Data strictly:

- on documented instructions of the Customer; and
- for the purpose of providing the Services only

Syntari does not determine the purposes or means of processing Customer Data.

3. SCOPE OF THIS POLICY

This Privacy Policy applies to:

- All users of Syntari websites and Services
- All SaaS products operated by Syntari

- All associated digital platforms, APIs, and systems

This Policy does not override any applicable Data Processing Agreement between Syntari and its Customers.

4. PERSONAL DATA WE COLLECT

We may collect and process the following categories of personal data:

4.1 IDENTITY AND ACCOUNT DATA

- Full name
- Email address
- Job title (if provided)
- Organisation name
- Authentication credentials (processed via third-party identity providers)

4.2 OPERATIONAL DATA (SERVICE USAGE DATA)

Depending on how the Services are used, we may process:

- Visitor registration records
- Site entry and exit logs
- Time-stamped access events (including late arrival / early departure where configured)
- User roles and permissions
- Location or site identifiers assigned by Customers

4.3 TECHNICAL AND SECURITY DATA

- IP address
- Device and browser information
- Session identifiers
- Authentication logs
- Audit logs and security events
- Failed login attempts and anomaly detection data

4.4 SUPPORT AND COMMUNICATIONS DATA

- Customer support communications
- Technical support requests
- Metadata relating to support interactions

4.5 PAYMENT AND BILLING DATA

Payments are processed by third-party providers.

We do not store full payment card details. We may receive:

- Billing status information
- Transaction metadata
- Billing contact details

4.6 SPECIAL CATEGORY DATA

Syntari does not intentionally process Special Category Data unless explicitly configured by the Customer in connection with the Services.

5. PURPOSES OF PROCESSING

We process personal data for the following purposes:

- Provision and operation of the Services
- Account creation and authentication
- Visitor management and site access logging
- Security monitoring and fraud prevention
- Customer support and service communication
- Service improvement and analytics
- Compliance with legal obligations

6. LAWFUL BASIS FOR PROCESSING (UK GDPR / EU GDPR)

We process personal data under the following lawful bases:

- **Contract:** where processing is necessary to provide the Services
- **Legitimate Interests:** for security, service improvement, and operational stability
- **Legal Obligation:** where required by law or regulatory requirements
- **Consent:** where required for optional processing activities

7. DISCLOSURE OF PERSONAL DATA

We do not sell personal data.

We may disclose personal data to trusted third-party service providers acting as data processors, including:

- Stripe — payment processing
- Amazon Web Services (AWS) — cloud hosting
- Vercel Inc. — deployment infrastructure
- PostHog — product analytics
- Resend — transactional email delivery

- Betterauth — authentication services

All processors are bound by contractual obligations consistent with UK GDPR Article 28.

We may also disclose data where required by law or to enforce legal rights.

8. INTERNATIONAL DATA TRANSFERS

Personal data may be transferred outside the United Kingdom and/or European Economic Area (EEA).

Where this occurs, we ensure appropriate safeguards, including:

- UK International Data Transfer Agreement (IDTA), and/or
- EU Standard Contractual Clauses (SCCs)
- Supplementary technical and organisational measures where required

9. DATA RETENTION

Personal data is retained only for as long as necessary for:

- Provision of the Services
- Legal and regulatory compliance
- Dispute resolution
- Contract enforcement

Data is then securely deleted or anonymised.

10. DATA SECURITY

We implement appropriate technical and organisational measures including:

- Encryption in transit
- Access controls and role-based permissions
- Authentication mechanisms
- Audit logging and monitoring
- Secure cloud infrastructure

These measures are designed in accordance with Article 32 UK GDPR.

11. COOKIES AND ANALYTICS

We use cookies and similar technologies to:

- Enable core functionality
- Maintain user sessions
- Improve performance

- Analyse usage patterns

Analytics providers (such as PostHog) may be used to improve Services.

Users may control cookies via browser settings, subject to functional limitations.

12. DATA SUBJECT RIGHTS

Where applicable under UK GDPR and EU GDPR, individuals may exercise:

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction
- Right to data portability
- Right to object
- Right to withdraw consent

13. CHILDREN'S DATA

Syntari Services are not directed at children as end users.

However, certain Services (including Visitor Management and Site Access Logging) may involve processing personal data relating to individuals under 16 (such as pupils or students), where recorded by authorised users acting on behalf of an educational institution or Customer organisation.

In such cases:

- Syntari acts as Data Processor
- The Customer acts as Data Controller
- The Customer is responsible for lawful basis and transparency obligations

We do not determine the purposes or means of processing such data.

We apply appropriate safeguards including:

- Encryption
- Access controls
- Role-based permissions
- Audit logging

14. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time.

Where material changes occur:

- The revision date will be updated
- Users may be notified where appropriate

Continued use of the Services constitutes acceptance.

15. CONTACT DETAILS

Syntari LTD

Email: legal@syntari.co.uk