



Smartix Privacy Policy

Last Updated: 11th December 2025

1. Introduction

Welcome to Smartix ("we," "our," "us"). We respect your privacy and are committed to protecting your personal data. This Privacy Policy explains how we collect, use, and protect your information when you visit our website www.smartix.uk or use our SaaS platform ("Service"). By using our Service, you agree to the terms of this Privacy Policy.

Smartix acts as:

- a **Data Controller** for personal data we collect directly from you to operate your account, billing, authentication, and support; and
- a **Data Processor** for any data you upload or send to Smartix for the purpose of generating and managing digital wallet passes.

2. Information We Collect

We collect the following types of personal information as **Data Controller**:

- **Account Information:** Your name and email address when you create an account. We may also collect company name, registration number, and further contact details.
- **Payment Information:** Payment details are processed securely by our third-party provider, Stripe. We do not store or access your full payment information.
- **Cookies and Usage Data:** We use cookies to maintain your login session and to analyse basic website usage.

As **Data Processor**, we also store and process information that you choose to upload or transmit for creation or management of wallet passes ("Pass Data"). Pass Data may include:

- Encrypted payloads used to generate wallet passes
- Optional unencrypted metadata fields you define in order to make subsets of data searchable
- Notifications and message content sent to pass holders
- Customer-created pass templates and configuration data

Pass Data is provided entirely by you, and **you remain the Data Controller** for this information.

Where Smartix is connected to third-party platforms such as Shopify, Smartix may also process limited integration data needed to link the Customer's Smartix account to that platform and to operate the relevant integration features. Such integration data does not replace the underlying Smartix account or Pass Data, which remain part of the separate Smartix service.



Smartix Privacy Policy

3. How We Collect Information

We collect data through:

- Signup forms you complete when creating an account or subscribing
- Cookies used to authenticate users
- Payment processing via Stripe
- API calls and dashboard inputs that upload Pass Data to our systems

4. How We Use Your Information

As **Data Controller**, we use your information to:

- Process payments and subscriptions via Stripe
- Communicate important updates, security notices, or support messages
- Provide, maintain, and improve our Service
- Manage your account and authentication
- Comply with legal obligations

As **Data Processor**, we process Pass Data **solely on your documented instructions**, including:

- Creating, updating, or revoking wallet passes
- Sending pass updates and notifications to Apple Wallet, Google Wallet, or supported devices
- Generating analytics or search results using only the metadata you have designated as searchable

We do not determine the purpose or lawful basis for Pass Data and do not use it for our own purposes.

If you use the Smartix Shopify integration, Smartix may also process limited Shopify-related integration data on your instructions, such as linked card identifiers, order settlement references, and other operational data required to apply or reconcile Smartix loyalty, membership, gift, or stamp features within Shopify.

5. Legal Basis for Processing (UK GDPR)

We process your personal data under the following lawful bases:

- **Contractual necessity:** To provide our Service to you
- **Legal obligation:** To comply with applicable laws
- **Legitimate interests:** To improve our Service and maintain security

For Pass Data, the lawful basis is determined by **you**, as the Data Controller.



Smartix Privacy Policy

6. Sharing of Information

We share limited data only when necessary:

- **Stripe** for payment processing (we share your email address and relevant payment details)
- **AWS** for secure data hosting, encryption (KMS), and infrastructure
- **Apple and Google** for the delivery and updating of wallet passes
- **Analytics providers** (if used) to improve performance of the Service

We do not sell or rent personal data to third parties.

7. International Data Transfers

We hold all personal and Pass Data within our AWS VPC based in Ireland (EU region).

Wallet pass delivery and updates rely on Apple and Google services, which may process data outside the UK. These transfers occur as part of the operation of the Wallet ecosystem and use the safeguards provided by Apple and Google.

8. Processing of Pass Data (Smartix as Data Processor)

Pass Data is stored encrypted at rest using AWS KMS. We decrypt this data **only within serverless functions (AWS Lambda)** and only to fulfil your instructions, such as generating or updating a digital wallet pass.

Because Pass Data is strongly encrypted, Smartix cannot meaningfully search it without explicit decryption. This means:

- We cannot perform global searches across encrypted data
- Any search capability relies solely on metadata fields you designate as unencrypted
- You are responsible for ensuring that searchable metadata does **not** contain personal data unless you have a lawful basis to store it unencrypted

You may configure, per pass template, which fields remain encrypted and which (if any) are stored in plain text for searchability.

Smartix does not access or use Pass Data except as required to provide the Service.



Smartix Privacy Policy

9. Data Retention

We retain your personal data only as long as necessary for the purposes stated above or as required by law.

Retention rules include:

- **Account and billing records:** kept while your account is active and for a legally required period afterwards
- **Pass Data:** retained only for as long as your account or pass project remains active, or until you delete it
- **Third-party integration data (for example Shopify integration records):** retained only for as long as needed to operate the integration, support reconciliation or refund workflows, meet compliance obligations, or until deleted under the applicable retention rules
- **Logs and backups:** retained according to our security and compliance requirements

You can request deletion of your account and data at any time (see Section 10).

If you disconnect or uninstall a third-party integration such as Shopify, this does **not** by itself delete your Smartix account, Smartix Pass Data, or Smartix-issued passes. Smartix remains a separate service. Deletion of Smartix account data must be requested through Smartix's own account or support processes.

10. Cookies

We use cookies for:

- Essential functionality (e.g., keeping you logged in)
- Analytics to understand usage and improve performance

You may disable non-essential cookies through your browser settings, although essential cookies are required for the Service to function.



Smartix Privacy Policy

11. Your Rights

Under the UK GDPR, you have the right to:

- Access your personal data
- Request correction or deletion of your data
- Object to or restrict processing
- Request data portability
- Withdraw consent at any time (where processing is based on consent)

To exercise your rights for data where Smartix is **Data Controller**, contact us at www.smartix.uk/contact.

For Pass Data, Smartix is **Data Processor**. Any data subject requests relating to Pass Data (for example, data embedded in passes created by your organisation) should be addressed **directly to you**, the Data Controller. Smartix will assist you in fulfilling such requests where technically feasible.

Where third-party integrations such as Shopify are used, deletion or redaction carried out within that third-party platform may apply only to the data held in, or linked to, that platform. It does not automatically delete the separate Smartix account or Smartix Pass Data unless that deletion is also requested through Smartix.

12. Data Security

We use appropriate technical and organisational measures to protect your personal data from unauthorised access, loss, or misuse.

This includes:

- Encryption of Pass Data, notifications, and logs using AWS KMS
- 12-month rolling encryption keys
- TLS for all data in transit
- Access controls, authentication, and monitoring
- Decryption only within AWS Lambda for operational purposes

Some data may be stored unencrypted if you explicitly choose to make it searchable. You are responsible for ensuring that any unencrypted metadata complies with your legal obligations and does not contain sensitive personal information unless lawfully permitted.

No online service is 100% secure, and we cannot guarantee absolute security.

13. Children's Privacy

Our Service is not directed to individuals under 16. We do not knowingly collect data from minors.



Smartix Privacy Policy

14. Scan App

- Use of camera is required to scan barcodes
- Use of location data is required to record where scans take place
- No photos or videos are taken
- Barcode and location data are sent to Smartix servers and held in encrypted format
- We do not share this data with anyone
- Barcode data is used to validate passes
- Data is used to provide an audit trail for the account holder
 - validating the user who scanned the pass
 - confirming whether the scan took place in an authorised business location
- We do not sell data or use it for advertising
- The Scan App does not display any adverts

15. Changes to This Policy

We may update this Privacy Policy from time to time. Any updates will be posted on this page with the "Last updated" date revised accordingly.

16 [Download PDF](#)

17. Contact Information

If you have questions about this Policy or wish to report a security concern, please contact us at:

www.smartix.uk/contact

[Privacy Policy](#) [PAYG Terms](#) [Contract Terms](#) [Fair Use Policy](#) [SLA](#) [Data security](#)