



Smartix Data Processing Agreement

Last Updated: 11th December 2025

1. Introduction

This Data Processing Agreement ("DPA") forms part of the Terms of Service or other written agreement ("Agreement") between the Customer ("Controller", "you") and Smartix Ltd ("Processor", "Smartix", "we", "us") for the provision of the Smartix wallet pass generation and management platform ("Service").

This DPA reflects the parties' agreement with respect to the processing of personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

By using the Service, you agree to this DPA.

2. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person.

"Processing" means any operation performed on Personal Data (e.g. storage, transmission, deletion).

"Controller" means the entity that determines the purpose and means of processing Personal Data.

"Processor" means the entity that processes Personal Data on behalf of the Controller.

"Pass Data" means any data you upload or transmit to Smartix for the purpose of generating and managing digital wallet passes.

"Data Protection Laws" means the UK GDPR, the Data Protection Act 2018, and any applicable data protection legislation.

3. Roles of the Parties

1. Smartix acts as **Processor** for all Pass Data you upload or submit to the Service.
2. You, the Customer, act as **Controller** for Pass Data and are responsible for determining the lawful basis and purpose of processing.
3. Smartix acts as **Controller** only for Personal Data we collect directly from you (e.g., account data, billing information).

Where you choose to connect Smartix to a third-party platform such as Shopify, Smartix processes the relevant integration data only to provide that integration. The existence or deletion of the third-party platform integration does not by itself create, transfer, or delete the underlying Smartix account or Smartix Pass Data.



Smartix Data Processing Agreement

4. Subject Matter and Duration of Processing

Smartix will process Personal Data solely for:

- creating, updating, and managing digital wallet passes
- sending notifications and updates to pass holders
- providing the Service according to your configuration
- maintaining security, logging, and operational functionality

Processing continues for the duration of your use of the Service and until all data is deleted in accordance with this DPA.

5. Nature and Purpose of Processing

Smartix processes Pass Data:

- **to generate and update wallet passes** in Apple Wallet, Google Wallet, or other supported platforms
- **to send pass notifications**
- **to store encrypted pass payloads** required for Service functionality
- **to enable optional search and filtering**, where the Controller designates specific metadata fields as unencrypted

Smartix does not process Pass Data for its own purposes and does not determine what Personal Data you choose to include.

Where Smartix is connected to Shopify or another third-party platform, Smartix may also process limited integration data required to synchronise identifiers, apply Smartix features within the third-party platform, settle transactions, and maintain records needed for operational or compliance purposes.



Smartix Data Processing Agreement

6. Types of Personal Data and Data Subjects

6.1. Personal Data processed as Processor

Depending on your configuration, Pass Data may include:

- Identifiers (e.g., membership numbers, policy numbers, booking references)
- Customer-specific attributes (expiry dates, statuses, metadata fields)
- Information required to personalise wallet passes

Smartix does not require Personal Data in Pass Data. Any inclusion is determined solely by the Controller.

6.2. Categories of Data Subjects

- Your customers
- Your employees or representatives
- Individuals who receive or redeem wallet passes created by you

7. Controller Responsibilities

The Controller is responsible for:

- ensuring a valid lawful basis for Pass Data
- obtaining any necessary consents from data subjects
- ensuring the Pass Data provided to Smartix is accurate and lawful
- configuring which metadata fields are stored unencrypted (if any)
- responding to data subject access requests (DSARs) relating to Pass Data
- determining whether deletion or redaction requested in a third-party platform (such as Shopify) should also be requested separately within Smartix where the underlying Smartix account or Pass Data is to be removed

Smartix is not responsible for determining what data is appropriate for inclusion in wallet passes.



Smartix Data Processing Agreement

8. Processor Obligations

Smartix shall:

1. **Process Pass Data only on documented instructions** from the Controller.
2. **Maintain confidentiality** and ensure all personnel are bound by obligations of confidentiality.
3. **Implement appropriate technical and organisational measures** as described in Section 9.
4. **Assist the Controller** with DSARs, erasure requests, and regulatory obligations where technically feasible.
5. **Notify the Controller of a Personal Data breach** without undue delay.
6. **Delete or return all Pass Data** at the end of the contract, unless otherwise required by law.
7. **Not engage subprocessors** without meeting the requirements in Section 7.

9. Subprocessors

Smartix uses reputable third-party subprocessors to support the Service:

9.1. Approved Subprocessors

- **Amazon Web Services (AWS):** Hosting, encryption (KMS), storage, serverless compute
- **Stripe:** Payment processing (Controller data only)
- **Apple:** Wallet pass delivery and updates
- **Google:** Wallet pass delivery and updates
- **Optional analytics providers** (listed in our Privacy Policy, if enabled)

Smartix will ensure that subprocessors are bound by data protection terms that offer the same level of protection as this DPA.

9.2. Changes to Subprocessors

Smartix will notify Customers of material changes to subprocessors via website update or email.



Smartix Data Processing Agreement

10. International Data Transfers

Smartix stores all data in AWS Ireland.

Transfers to Apple and Google may occur outside the UK when delivering wallet passes.

Smartix relies on:

- platform safeguards provided by Apple and Google
- AWS compliance with UK GDPR transfer mechanisms

No other international data transfers occur unless expressly agreed.

11. Security Measures

Smartix implements industry-standard security measures including:

- Encryption at rest using **AWS KMS** with 12-month rolling keys
- Encryption in transit using TLS
- Decryption **only inside AWS Lambda** functions
- Role-based access control and least-privilege architecture
- Audit logging via CloudWatch
- Segregated per-customer data stores within AWS RDS
- Restricted access to production systems

11.1. Encrypted vs Unencrypted Fields

- By default, Pass Data is fully encrypted.
- The Controller may designate specific metadata fields as unencrypted for searchability.
- The Controller is responsible for ensuring such metadata does not contain personal data unless lawfully permitted.

12. Data Subject Requests (DSARs)

Smartix will:

- Forward any DSARs received directly from data subjects to the Controller
- Assist the Controller with retrieving or deleting Pass Data, where technically feasible
- Provide clarification on any technical constraints (e.g., encrypted data cannot be globally searched)

The Controller remains responsible for responding to data subjects.



Smartix Data Processing Agreement

13. Personal Data Breach Notification

Smartix will notify the Controller **without undue delay** after becoming aware of a breach affecting Pass Data.

The notification will include:

- the nature of the breach
- the likely consequences
- measures taken to mitigate or address the breach

Smartix will provide reasonable assistance to the Controller for regulatory notifications.

14. Return and Deletion of Data

Upon termination of the Agreement:

- Smartix will delete or return all Pass Data to the Controller, at its discretion or upon request
- Backups containing encrypted Pass Data will be deleted automatically during normal rotation cycles
- Smartix may retain Controller-operated account records as required by law (e.g., financial records)

For clarity, removal of a third-party integration, or deletion of data within that third-party platform, does not by itself require Smartix to delete the separate Smartix account or Smartix Pass Data unless that instruction is also provided to Smartix.

15. Audits

The Controller may request information demonstrating Smartix's compliance with this DPA.

On-site audits may be permitted where required by law, subject to reasonable notice, confidentiality, and operational restrictions.

16. Liability

This DPA does not alter the liability limitations set out in the Agreement between the parties.

17. Changes to This DPA

Smartix may update this DPA to reflect changes in law, subprocessors, or functionality. Notice will be provided where required.

18 [Download PDF](#)



Smartix Data Processing Agreement

19. Contact

If you have questions about this DPA or how your data is processed, please contact us at:

www.smartix.uk/contact

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