



Smartix Data Deletion & Retention Policy

Last Updated: 11th December 2025

1. Introduction

This Data Deletion & Retention Policy explains how Smartix ("we", "our", "us") deletes, retains, and manages customer data, Pass Data, and system logs in accordance with our Privacy Policy, Data Processing Agreement (DPA), and applicable data protection laws, including the UK GDPR.

This policy applies to all data stored or processed as part of the Smartix Service.

Where Smartix is connected to a third-party platform such as Shopify, this policy also applies to Smartix-held integration records created to operate that connection. However, deletion within the third-party platform does not by itself delete the separate Smartix account, Smartix Pass Data, or Smartix-issued passes unless that deletion is also requested through Smartix.



Smartix Data Deletion & Retention Policy

2. Pass Deletion

2.1. Automatic Deletion After Expiry

If a pass has an expiry date, Smartix automatically deletes the pass and all associated Pass Data (other than logs) after a configurable period defined by the Customer.

- Each Customer may configure the retention window (e.g., 7, 30, 90 days).
- After this window, the pass and its non-log data are permanently deleted.

2.2. Manual Deletion by Customer

Customers can delete a pass at any time.

Deleting a pass removes:

- Pass Data
- Pass metadata
- Notification data
- Any other related stored fields

Deleted passes cannot be recovered.

Deleting a pass in Smartix is separate from deleting any linked customer, order, or integration record in a third-party platform such as Shopify.

2.3. Billing Considerations

Smartix charges customers based on the **number of active passes** present in the system each month.

Customers are encouraged to delete passes that are no longer required to avoid unnecessary billing charges.



Smartix Data Deletion & Retention Policy

3. Account Deletion

3.1. Customer-Initiated Account Deletion

A Customer may request deletion of their Smartix account at any time.

- The deletion will occur at the **end of the current billing period**.
- Until that time, the deletion request may be cancelled.

Removing or uninstalling a third-party integration such as Shopify is **not** the same as deleting a Smartix account.

3.2. Data Removed Upon Account Deletion

When an account is deleted, Smartix permanently deletes:

- All Customer data
- Customer user profiles
- API keys
- Pass templates
- Passes and all associated Pass Data
- Stored notification content
- Session and authentication data
- Customer settings and configuration
- Payment and customer records held in Stripe
- Smartix-held third-party integration records associated with the account, except where temporary retention is required for audit, compliance, dispute handling, or backup rotation

3.3. Data That Cannot Be Deleted

Google Wallet templates ("Class files") cannot be deleted once registered with Google.

This is a technical limitation of the Google Wallet ecosystem, not of Smartix.

These templates simply become inactive and cannot be updated.

3.4. Passes Installed on End User Devices

Passes already installed on Apple or Google Wallet by end users **cannot be deleted by Smartix**.



Smartix Data Deletion & Retention Policy

- This is a technical limitation of mobile wallet platforms.
- Smartix does not force expiry or removal of installed passes.
- Customers may choose to update passes or send notifications, but cannot remove installed passes remotely.

4. Payment Data (Stripe)

4.1. Deletion on Account Cancellation

When a Customer account is deleted, Smartix deletes:

- The Stripe customer object
- All associated payment methods
- Subscription and billing history (to the extent allowed by Stripe and accounting requirements)

4.2. Deletion When a Customer Downgrades to the Free Tier

If a Customer upgrades to a paid plan and later returns to the free tier:

- Smartix deletes their Stripe customer profile
- All stored payment methods are removed
- No payment data remains linked to the account



Smartix Data Deletion & Retention Policy

5. Log Retention

5.1. Application Logs Stored in the Database

Smartix stores certain operational logs in its database for security, debugging, and audit purposes.

- These logs are **retained for 90 days**.
- This retention period may change in the future, and any updates will be reflected in this policy.

Logs may include:

- Pass generation events
- Scan events
- Notification events
- System errors and access logs

5.2. CloudWatch Logs

Smartix also uses AWS CloudWatch for runtime and function execution logging.

- CloudWatch logs are retained for **1 month**.
- Logs may contain metadata but not decrypted Pass Data.

5.3. Logs Are Not Deleted During Pass or Account Deletion

Due to audit and security requirements:

- Logs related to passes
- Logs related to Customer operations
- System events and API access logs

are **not deleted** when passes or accounts are deleted.

These logs continue to age out according to their retention periods.

Logs do not contain raw decrypted Pass Data.

Where Smartix stores limited third-party integration records for operational, reconciliation, refund-support, or compliance purposes, those records may also remain until their applicable retention period expires or until the related Smartix account data is deleted in accordance with this policy.



Smartix Data Deletion & Retention Policy

6. Backups and Disaster Recovery

6.1. Backup Retention

Smartix uses AWS backup mechanisms such as:

- RDS automated snapshots
- Point-in-time recovery

Backups containing encrypted Pass Data remain encrypted and inaccessible without the proper KMS keys.

6.2. Backup Lifecycle

- Backups are retained according to our operational configuration.
- Backups containing Customer data are overwritten or deleted during normal backup rotation cycles.
- Deleted Customer data will be removed automatically once old backups expire.

7. Data That Smartix Cannot Delete

Due to platform limitations outside Smartix's control, Smartix cannot delete:

- Google Wallet Class templates once registered with Google
- Passes stored on end-user mobile devices
- CloudWatch logs or system logs before their retention period expires
- Backups created before a deletion request (these are purged automatically according to rotation schedules)

8. Customer Responsibilities

Customers are responsible for:

- Configuring pass expiry and retention windows appropriately
- Deleting passes no longer required (to avoid billing charges)
- Deleting unneeded metadata fields
- Ensuring Pass Data complies with legal obligations
- Responding to DSARs from their pass holders
- deciding whether a deletion request made in a third-party platform such as Shopify should also be submitted separately to Smartix
- Requesting account deletion when required

9 [Download PDF](#)



Smartix Data Deletion & Retention Policy

10. Contact Us

If you have any questions regarding data deletion or retention, please contact us at:

www.smartix.uk/contact

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