Smartix Security Overview

Last Updated: 11th December 2025

1. Introduction

Smartix (“we”, “our”, “us”) is committed to maintaining industry-standard security for the processing of Personal Data and Pass Data. This Security Overview describes the technical and organisational measures Smartix implements to protect data in accordance with Article 32 of the UK GDPR and the AWS Well-Architected Security Model.

These measures apply to all environments where Pass Data or Smartix-controlled Personal Data is processed, stored, or transmitted.

2. Infrastructure Security

2.1. Hosting Environment

Smartix is hosted exclusively on **Amazon Web Services (AWS)** within an **isolated Virtual Private Cloud (VPC)** located in the EU (Ireland) region.

AWS provides:

- ISO 27001, SOC 1/2/3 compliance
- Physical security, environmental controls, and resilient data centres
- Infrastructure redundancy and high availability

Smartix does not maintain any on-premise infrastructure.

2.2. Network Security

Smartix employs the following network controls:

- Isolated VPC with private subnets
- Security groups enforcing least-privilege inbound/outbound rules
- No direct public access to databases
- TLS 1.2+ enforced for all data in transit
- AWS-managed certificates for secure endpoints
- WAF-level protections where applicable

All traffic between system components is encrypted.

Smartix Security Overview

3. Data Security

3.1. Encryption at Rest

All potentially sensitive data is encrypted using **AWS Key Management Service (KMS)** with:

- AES-256 encryption
- 12-month rolling key policy
- Automated key rotation and audit logging
- Customer data segregated at application level

Pass Data is encrypted at the field or payload level to minimise exposure even in internal environments.

3.2. Encryption in Transit

All communications use HTTPS/TLS. This includes:

- Dashboard and API interactions
- Internal service-to-service communication
- Pass updates sent to Apple and Google services
- Data transmissions from the Scan App

Smartix disables weak protocols and ciphers.

3.3. Data Isolation

Customer data is logically isolated using:

- Tenant-aware access layers
- Application-level segmentation
- Row-level association controls within RDS

Cross-customer access is technically prevented.

3.4. Searchable Metadata and Encrypted Payloads

Pass Data is encrypted in a way that **cannot be full-text searched**. Smartix supports customer-defined **unencrypted metadata fields** strictly for:

- Search
- Filtering
- Pass management automation

Customers are responsible for ensuring unencrypted metadata does not contain sensitive or unlawful personal data.

Smartix Security Overview

3.5. Key Management

Smartix does not access raw private encryption keys.

AWS KMS provides:

- Fully managed keys
- Access control policies
- Detailed audit logs
- Envelope encryption
- Strict IAM controls

Smartix applications use KMS only to perform envelope decryptions at runtime inside AWS Lambda.

4. Application Security

4.1. Serverless Execution Environment

Smartix executes sensitive operations inside **AWS Lambda**, which provides:

- Ephemeral execution environments
- Automatic scaling
- No long-lived servers
- Strong runtime isolation
- Immutable deployment artefacts

Pass Data is decrypted **only** within Lambda during pass creation or update workflows.

4.2. Dependency and Build Security

Smartix follows:

- Automated dependency scanning
- Regular patch updates
- Locked package manifests
- Build-time integrity checks
- Principle of minimal dependencies

Smartix Security Overview

4.3. Authentication & Access Control

- Multi-factor authentication (MFA) is enforced for internal staff
- Least-privilege IAM roles
- Role-based access to production environments
- No direct database logins via password; IAM-authentication or IAM-managed secrets only
- Strong password requirements for customer accounts

5. Operational Security

5.1. Logging and Monitoring

Smartix uses AWS CloudWatch and other monitoring tools to collect:

- API access logs
- Security events
- Pass generation events
- Lambda execution logs
- Authentication attempts

Logs containing potentially sensitive data are encrypted via KMS.

5.2. Incident Detection & Response

Smartix maintains an internal incident response plan including:

- Immediate triage and severity assessment
- Isolation of affected components
- Restoration steps
- Communications with Controllers (per the DPA)
- Review and remediation actions

Security events are escalated to senior engineering staff.

5.3. Backup and Disaster Recovery

- Automated daily RDS snapshots
- Point-in-time recovery
- Encrypted backups
- Backups stored only within the AWS Ireland region
- Infrastructure-as-code defines consistent environment rebuilds

Smartix Security Overview

6. Subprocessors

Smartix uses carefully selected subprocessors:

- **AWS** (hosting, storage, encryption, serverless compute)
- **Stripe** (Controller data only)
- **Apple** (wallet pass distribution)
- **Google** (wallet pass distribution)
- **Optional analytics providers** (see Privacy Policy)

All subprocessors offer GDPR-aligned protections.

7. Access to Personal Data

Access to production systems is restricted to a minimal number of authorised Smartix personnel.

Controls include:

- MFA-protected IAM accounts
- Strict least-privilege and just-in-time access
- Access logging and audit trails
- Background checks for employees (where legally appropriate)

Smartix employees do not access Pass Data unless explicitly required for troubleshooting and authorised by the Controller.

8. Data Deletion and Termination

Upon account closure or customer request:

- Pass Data is deleted from active databases
- Cached and temporary data is purged
- Backups containing encrypted Pass Data are removed during their regular rotation window
- Controller data is retained only as required by law

Smartix provides deletion confirmation on request.

Smartix Security Overview

9. Vulnerability Management

Smartix maintains:

- Regular vulnerability scanning
- Patch cycle for application dependencies
- Automated alerts for known CVEs
- Code review for security-sensitive components
- Secure software development lifecycle (SSDLC) practices

10. Customer Responsibilities

Customers must:

- Ensure a lawful basis for Pass Data
- Configure metadata fields responsibly
- Protect API keys and dashboard credentials
- Use supported authentication methods
- Respond to DSARs from their pass holders

Smartix supports customers in meeting their obligations (see DSAR Workflow).

11 Download PDF

12. Contact

If you have questions about security or require additional documentation, please contact us:

www.smartix.uk/contact