



Smartix DSAR Workflow

Last Updated: 11th December 2025

1. Introduction

Smartix ("we", "our", "us") is committed to supporting our customers ("Controllers") in fulfilling their obligations under the UK GDPR. This document explains how Smartix handles Data Subject Access Requests ("DSARs") and other data rights requests.

Smartix acts as:

- **Data Controller** for Personal Data we collect directly from customers (e.g., account details, billing information, authentication data).
- **Data Processor** for Pass Data uploaded by customers to generate wallet passes.

Where Smartix is connected to a third-party platform such as Shopify, Smartix may also hold limited integration data needed to operate that connection. This integration data does not replace the separate Smartix account or Pass Data and may need to be handled separately from any deletion or redaction performed within the third-party platform.

This workflow explains how DSARs are handled for both categories of data.

2. Types of DSARs Covered

A data subject may contact either:

- **The Controller** (Smartix customer)
- **Smartix directly**
- **Both parties**

A DSAR may consist of a request to:

- Access personal data
- Correct inaccurate data
- Delete data ("right to erasure")
- Restrict processing
- Object to processing
- Request portability



Smartix DSAR Workflow

3. Scope of Smartix's Responsibilities

3.1. As **Controller**, Smartix responds directly to DSARs relating to:

- Customer account data
- Login and access logs
- Billing information
- Support communications
- Website interaction data

3.2. As **Processor**, Smartix assists Controllers with DSARs relating to:

- Encrypted Pass Data
- Optional unencrypted searchable metadata
- Notifications or messages associated with wallet passes
- Audit logs generated during pass processing

The Controller retains responsibility for responding to data subjects whose data appears in Pass Data.

4. DSAR Workflow for Pass Data (Smartix as Processor)

4.1. If a data subject contacts Smartix directly

Smartix will:

1. Confirm whether the request relates to Pass Data.
2. Inform the data subject that Smartix processes their data **on behalf of a customer**.
3. Provide contact details (if known) or instruct the subject to contact the organisation who issued their pass.
4. Notify the Controller that we have received a DSAR intended for them.

Smartix does **not** respond directly to DSARs for Pass Data.



Smartix DSAR Workflow

4.2. If the Controller submits a DSAR to Smartix for assistance

Smartix will assist the Controller where technically feasible.

Assistance may include:

- Retrieving encrypted Pass Data for specific records
- Deleting or updating specific Pass Data
- Providing extracts of unencrypted metadata fields
- Explaining search limitations due to encryption design

4.3. Requirements from the Controller

The Controller must provide:

- Sufficient identifiers to locate the correct Pass Data
- The specific fields required (if a partial extraction)
- Confirmation of DSAR type (access, erasure, correction, etc.)

5. Technical Considerations for Encrypted Pass Data

Smartix encrypts Pass Data using AWS KMS in a way that prevents global searching across encrypted fields.

This means:

- **Encrypted data cannot be searched directly**
- Smartix cannot locate a record from encrypted content alone
- Searching across encrypted fields would require decrypting every record, which is not feasible and not supported by the system
- Only metadata you designate as unencrypted can be used for searching or filtering DSAR-related data

5.1. Therefore, DSARs affecting encrypted Pass Data require:

- The Controller to provide a unique identifier (e.g., pass ID, reference code, membership or policy number)
- The Controller to define the exact records to retrieve or delete

Smartix cannot identify or extract encrypted Pass Data without such identifiers.



Smartix DSAR Workflow

6. DSAR Workflow for Smartix Account Data (Smartix as Controller)

Smartix will directly respond to DSARs for:

- Account profiles
- Contact details
- Authentication and usage logs
- Emails and support messages
- Billing identifiers (excluding full payment data, which is stored by Stripe)

We will:

1. Verify the identity of the requester.
2. Confirm the scope of the request.
3. Fulfil the request within statutory timeframes (normally 1 month).
4. Notify the requester when the request has been completed.

7. Timeframes

Smartix follows statutory timelines:

- **One month** to fulfil DSAR requests
- Extension of **up to two months** for complex requests

Controllers maintain their own DSAR deadlines for their data subjects.

8. Deletion and Rectification Requests

8.1. For Pass Data

Smartix will delete or update Pass Data **only when instructed by the Controller**, and only where the correct identifiers are provided.

Where a Controller uses Smartix with a third-party platform such as Shopify, a deletion or redaction request carried out in that platform does not automatically instruct Smartix to delete the separate Smartix account or Smartix Pass Data unless the Controller also provides that instruction to Smartix.

8.2. For Smartix-controlled data

We will delete, correct, or anonymise the requester's Personal Data where permitted by law and technically feasible.



Smartix DSAR Workflow

9. Data Subject Requests for Pass Holders

If a pass holder contacts Smartix claiming:

- "I want to see what data you hold about me,"
- "Delete my pass information," or
- "Why did I receive this pass?"

Smartix will:

1. Explain that:
 - The pass was issued by the Controller
 - Smartix only processes the data on the Controller's instruction
 - deletion from a linked third-party platform, if any, may not delete the separate Smartix record unless that deletion has also been requested from Smartix
2. Provide the Controller's contact details (where identifiable)
3. Notify the Controller that the request has been forwarded

Smartix will not action the request unless instructed by the Controller.

10. Breach Notifications

If Smartix becomes aware of a Personal Data breach involving Pass Data:

- Smartix will notify the Controller **without undue delay**
- The Controller is responsible for notifying the ICO and/or affected data subjects unless otherwise agreed

If a breach affects Smartix-controlled data, Smartix handles all legal notifications.



Smartix DSAR Workflow

11. Responsibilities Summary

Data Type	Smartix Role	Who Responds to DSAR?	Smartix Support?
Customer account details	Controller	Smartix	N/A
Billing data (via Stripe)	Controller	Smartix (excluding card data held by Stripe)	N/A
Pass Data	Processor	Customer	Yes. Where technically feasible
Encrypted fields	Processor	Customer	Requires identifier; cannot be searched
Unencrypted metadata	Processor	Customer	Searchable and retrievable
Website analytics data	Controller	Smartix	N/A

For third-party integrations such as Shopify, the relevant platform may also have its own data request, redaction, or deletion processes. Those processes apply to data held in that platform or in the integration layer, but do not automatically delete the separate Smartix account or Smartix Pass Data unless Smartix is also instructed accordingly.

12 [Download PDF](#)

13. Contact Information

If you have questions about DSAR handling, please contact us at:

www.smartix.uk/contact

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