

CYBER SECURITY

# Customer Data Policy

FUNDS  AXIS

<b>Policy title:</b>	Customer Data Policy
----------------------	----------------------

<b>Issue</b>	2.0
<b>Approved by:</b>	Darren Burrows
<b>Approval Date:</b>	February 2025
<b>Next Review Date:</b>	February 2026

<b>Scope:</b>	The policy applies to Funds-Axis Group and all contractors and other people working on behalf of the company.
<b>Responsibility for Implementation &amp; Training:</b>	<p>Day to day responsibility for implementation: ISO</p> <p>Day to day responsibility for training: ISO</p>

<b>Distribution methods:</b>	<p>Methods used to communicate this policy:</p> <ul style="list-style-type: none"> <li>Information Security Training Module</li> </ul>
------------------------------	--

## CONTENTS

1. Background .....	4
2. Scope .....	4
3. The Customer Data Officer .....	4
4. The Funds-Axis Group .....	4
5. Customer Data Lifecycle.....	4
5.1 Receipt of data .....	4
5.2 Data Access .....	5
5.3 Data Processing .....	5
5.4 Customer data transmission .....	6
5.5 Data Storage - source records and data deletion.....	7
5.6 Client Exit and Data Archiving .....	7
5.7 Regulatory Cooperation .....	8
5.8 Business Continuity and Data Recovery.....	8
6. Personal Data / Investor Data .....	8
7. Incident Management .....	9

## 1. Background

Funds-Axis is a technology-based business which involves the processing, management, and transfer of a large amount of Customer and other data on a daily basis.

The largest volume of data handled by the company relates to Customer Data in respect of the technology solutions provided by Funds-Axis.

In line with our commitment to regulatory compliance, all data processing activities are conducted in accordance with the Digital Operational Resilience Act (DORA), the General Data Protection Regulation (GDPR), and the Data Protection Act 2018 (DPA 2018).

## 2. Scope

This Policy is a supplementary policy detailing certain specific policies in respect of Customer Data, including in respect of data acquisition, data transmission, processing, storage, archive, and destruction.

## 3. The Customer Data Officer

The Customer Data Officer is a team member responsible for ensuring that the Customer's data journey with Funds-Axis, which includes data acquisition, transmission, processing, storage, archiving, and destruction, is compliant with this Customer Data Policy.




## 4. The Funds-Axis Group

The Funds-Axis Group comprises Funds-Axis Limited and our 100% subsidiary, Fundsaxis India Private Limited. When delivering solutions and services to Customers, we may leverage the expertise of the team across the entire Funds-Axis Group. Therefore, all entities within the Funds-Axis Group, including those mentioned above and any other subsidiaries, are subject to this Policy, as well as other business Policies.

## 5. Customer Data Lifecycle

### 5.1 Receipt of data

All data received from clients must be transmitted securely through one of the following methods:

-  Secure download from source system
-  Secure FTP transfer
-  Secure email

Funds-Axis provides secure data processing through:

- \\ **HighWire Platform:** Processes compliance monitoring, regulatory reporting, and risk monitoring data.
- \\ **Learning Management System:** Handles training and progress tracking data.
- \\ **Information Portals:** Manages regulatory obligation data across jurisdictions.

All data processing occurs through our secure AWS infrastructure, with:

- \\ Primary processing in AWS Ireland (eu-west-1).
- \\ Disaster recovery across multiple AWS Ireland availability zones.
- \\ Strict data residency within EU/UK regions.
- \\ Real-time monitoring via AWS CloudWatch.
- \\ Comprehensive security controls through AWS security tools.

Our AWS infrastructure operates within data centers that maintain rigorous security standards and controls. Full details of AWS security certifications and compliance programs are available through AWS's public documentation.

## 5.2 Data Access

Access to Customer Data within the Funds-Axis Group must be in accordance with the Funds-Axis Cyber Security Policy: Internal Organisational Arrangements.

Data access is protected through:

- \\ AES-256 encryption for data at rest.
- \\ TLS 1.2+ encryption for data in transit.
- \\ Role-based access control (RBAC).
- \\ Multi-factor authentication (MFA).
- \\ Regular penetration testing and security audits.
- \\ Strict segregation of client data.
- \\ "Need to know" and "least privilege" principles.
- \\ Compliance with DPA 2018 requirements for data access and control.
- \\ Regular assessment of data protection measures against UK standards.

## 5.3 Data Processing

Customer data will typically require acquisition, transformation, loading into our applications followed by review and potentially correction.

Funds-Axis strives to automate these processes as much as possible to minimize manual downloading, manipulating, or uploading of data. This is done to promote efficiency and reduce the risk of manual errors or data loss.

Depending on the solutions subscribed to or the data formats provided by the Customer, manual activity may still be necessary.

All data processing activities comply with the Data Protection Act 2018, ensuring appropriate technical and organisational measures are in place to protect personal data and maintain records of processing activities.

#### Data Processing Security:

- \\ Automated data integrity checks for accuracy, validity, and completeness.
- \\ Real-time monitoring of data transactions.
- \\ Regular vulnerability assessments.
- \\ Automated alerting systems.
- \\ Clear audit trails of all data processing activities.

#### Data Processing Locations:

- \\ All processing occurs within EU/UK regions.
- \\ Primary processing in AWS Ireland.
- \\ Backup and disaster recovery within AWS Ireland.
- \\ No data transfers outside these regions without prior consent.
- \\ Advance notification of any planned changes to processing locations.

### 5.4 Customer data transmission

Any internal or outward communications involving Customer Data must be sent by:

- \\ Secure FTP data
- \\ Password protected documents sent as attachments to e-mails.
- \\ email transmission is encrypted through opportunistic TLS.

To avoid manual error, outward manual communication of Customer Data is discouraged. Instead, the focus should be on Customers accessing data through secure online applications or automated reports.

The transfer of any Customer data outside of Funds-Axis Group (except to the respective client) is strictly prohibited.

Without the Customer's express prior consent, there must be no communication of Customer Data to other third parties outside of the Funds-Axis Group, including to any third-party system or solution providers, or consultants.

Unless otherwise disclosed to the Customer, where Funds-Axis uses any third-party solutions, these will be within the Funds-Axis controlled cloud computing architecture and the third-party providers will have no access to this. Where third party support is required (new releases, bug fixes etc) this will be obtained securely and without the third party having any access to Customer Data. Where you utilise the Fundpeak factsheets services or the StatPro risk services, this will involve transfer of data to those entities.

Sub-Processing Partners: The following entities may have access to certain data for specific processing purposes:

- \ Amazon Web Services (infrastructure).
- \ Microsoft (software applications).
- \ Acronis (backup services).
- \ Zoho Projects (project management).
- \ Zoho ManageEngine ServiceDesk Plus (service desk).
- \ JIRA (issue tracking).
- \ ChargeOver (billing).
- \ QuickBooks (accounting).
- \ DocuSign (electronic signatures).

These providers:

- \ Only provide infrastructure and software applications.
- \ Have no direct access to personal data.
- \ Receive only encrypted data.
- \ Are bound by strict contractual controls.
- \ Are regularly monitored and audited.

## **5.5 Data Storage - source records and data deletion**

The Funds-Axis solutions are made available based upon source data (primarily holdings and NAV data) which is provided by the Customer and / or its Administrators.

This data is then processed and enriched by Funds-Axis. The Funds-Axis solutions include data integrity checks in respect of accuracy, validity, and completeness of the data.

Funds-Axis do not retain copies of the original source or derived data, except for the data that is stored within our solutions. Other versions of the data will be purged including from our email systems, SFTP data capture, and from our internal Networks. This will be done as soon as possible, but in any case, within 90 days of receipt.

Where required, Customer should maintain its own copies of original source data provided by the Customer (or its delegates) to Funds-Axis for the purposes of the provision of the service, or ensure that original source data can be obtained from Administrators etc.

Data Availability and Recovery:

- \ 99.9% uptime commitment.
- \ Multiple backup versions maintained.
- \ Defined Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
- \ Automated backup systems.
- \ Regular testing of recovery procedures.
- \ Continuous monitoring of backup integrity.

## **5.6 Client Exit and Data Archiving**

On the termination of service, Funds-Axis will continue to support the client during the notice period.

To support the transition, a range of Customer Data and results is available to the client via the application UI. Additionally, where agreed, Funds-Axis will provide the Customer with a data transition strategy on a reasonable time and materials basis.

Unless otherwise agreed, Funds-Axis will have no other responsibilities as regards data transition or archiving. Further, within 90 days of termination of service, Funds-Axis will ensure the deletion of the data from its systems and from the PCCI and any sub-outsourcer.

Enhanced Exit Provisions:

- \ 60-day standard notice period for termination.
- \ Data provided in structured, commonly used formats (e.g., CSV).
- \ Comprehensive data transition support available.
- \ Customer maintains control over termination process.
- \ Access to data maintained throughout transition.
- \ Secure deletion verification after transition.
- \ Support for regulatory compliance during transition.

## **5.7 Regulatory Cooperation**

Funds-Axis commits to:

- \ Full cooperation with customers' regulatory authorities.
- \ Providing access for audits and inspections.
- \ Maintaining transparency in regulatory investigations.
- \ Prompt notification of significant data breaches.
- \ Supporting regulatory reporting requirements.
- \ Providing necessary documentation and records.
- \ Assisting with regulatory compliance verification.

## **5.8 Business Continuity and Data Recovery**

Funds-Axis ensures:

- \ Regular testing of recovery procedures.
- \ Multiple backup locations within EU/UK.
- \ Automated failover capabilities.
- \ Regular disaster recovery drills.
- \ Documented recovery procedures.
- \ Clear escalation paths.
- \ Regular testing of backup integrity.

## **6. Personal Data / Investor Data**

Customers are advised not to transmit any data regarding investors into investment funds to Funds-Axis, as this is not necessary for the solutions/services provided.

## 7. Incident Management

Any exceptions must be managed in compliance with the Funds-Axis Incident Management Policy.



FUNDS  AXIS



## CONTACT US



+44 (0) 28 9032 9736



[info@funds-axis.com](mailto:info@funds-axis.com)



[www.funds-axis.com](http://www.funds-axis.com)



12 Gough Square, London,  
United Kingdom, EC4A 3DW