Data Protection Policy

Policy Summary

As an FCA-regulated firm, we are required to manage operational risks effectively, including those related to personal data. This policy outlines how we protect personal data in line with the UK GDPR, the Data Protection Act 2018, PECR, and ICO guidance.

We implement robust access controls, employee training, and secure data management practices to meet our obligations and safeguard data.

Background

The UK Data Protection Act 1998 established individuals' control over personal data. On 25 May 2018, the GDPR came into force, strengthening data rights and obligations for organisations. After Brexit, the UK GDPR replaced the EU GDPR in the UK on 31 December 2020.

Purpose

To ensure compliance with applicable data protection laws by setting out how we lawfully process, store, access, and protect personal data.

Scope

This policy applies to all employees, contractors, directors, and Introducer Appointed representatives (IAR's), Appointed Representatives (ARs). It covers all personal and special category data processed by the business.

Key Definitions

- **Personal Data:** Information that identifies a living person (e.g., name, ID number, location, IP address).
- **Special Category Data:** Sensitive information, including health, religion, sexual orientation, political views, biometric and genetic data.
- **Data Subject:** The individual whose personal data is being processed.
- **Processing:** Any activity involving personal data (collection, storage, sharing, deletion).
- **Controller / Processor:** The party deciding how and why data is used / processes data on behalf of a controller.

Data Protection Principles

We adhere to the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

Lawful Basis for Processing

Processing must be based on one of the six lawful grounds:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Data Subject Rights

Under UK GDPR, individuals have the right to:

- Access their data
- Request rectification
- Request erasure
- Restrict processing
- Data portability
- Object to processing
- Be informed of and object to automated decision-making and profiling

All requests are logged and managed within the required timeframes.

Governance and Accountability

Although not legally required to appoint a DPO, we operate a GDPR Committee (comprising senior leadership) responsible for:

- Overseeing compliance and reporting to the Board
- Reviewing policies and training staff
- The process for handling subject access requests
- Approving third-party data processors
- Ensuring marketing and IT systems comply with GDPR

Employee Responsibilities

All staff must handle personal data properly. Directors, managers, and employees may be personally liable for breaches. Misuse or negligent handling of data may lead to disciplinary action and reporting to the ICO or police.

Responsibilities:

- Access data only when necessary
- Keep data secure (e.g., password protection, locked screens)
- Follow IT and data handling policies
- Report any concerns to managers or the GDPR Committee

Transparency

We communicate data processing via:

- Privacy Notices
- Contracts
- Terms & Conditions

These documents outline data categories, purposes, sharing practices, rights, and contact information.

Data Processing Obligations

We maintain records of:

- Lawful basis for processing
- Data locations and access points
- Users of the data
- Retention periods

Data Storage & Security

Data must be:

- Stored securely (physical and digital)
- Password protected
- Not stored on personal devices
- Regularly backed up
- Disposed of securely when no longer needed

Data Accuracy

We ensure data is:

- Up to date
- Reviewed regularly
- Corrected or deleted when necessary

Data Protection Impact Assessments (DPIAs)

We conduct DPIAs when processing may pose high risks, such as:

- Large-scale processing of special category data
- Systematic monitoring
- Automated profiling with significant effects

Data Breach Management

We follow a formal process for handling breaches:

- Logging and assessing all incidents
- Reporting to ICO within 72 hours where required
- Informing affected individuals if high risk
- Maintaining a breach register
- Escalating serious incidents internally and, where necessary, to the FCA

Review & Monitoring

This policy is reviewed annually or upon regulatory updates. Breaches of this policy may lead to disciplinary action and regulatory reporting.