Securys™

Global Data Privacy Experts

WHITE PAPER

Preparing **Wealth Management** for the new era in data governance

Data Protection risks within UK wealth management and financial advisory organisations

December 2025

Contents

Executive Summary

The UK financial services sector is entering a pivotal phase in its data governance evolution.

With recent sweeping updates to the FCA's data requirements and the introduction of the Data (Use and Access) Act 2025, senior leaders across the sector, including wealth management, investment advisory, and pension administration must now confront a complex landscape of privacy risks and regulatory obligations. The mandated changes are not simply technical adjustments — they represent a strategic imperative. Firms that fail to act risk regulatory censure, reputational damage, and erosion of client trust. Conversely, those that respond decisively will position themselves as leaders in compliance, resilience, and ethical data stewardship.

In this white paper, we consider the data privacy-based risks which are likely to affect many financial service organisations and which are particularly pertinent for wealth management and financial advisory organisations. To set the context more fully, we also reflect on the other key FCA-driven regulatory changes which intersect with these data privacy risks creating what can rightly be perceived as a perfect storm.

The FCA-driven regulatory changes intersect with data privacy risks to **create the perfect storm**.

Sector Risks 4

Issues within the sector are present across all categories of data protection risk but the common themes discovered throughout our research include:

1 Excessive and Unmanaged Data Collection

- Organisations routinely collect large volumes of personal data, often without clear justification or ongoing review.
- Outdated data is commonly retained, undermining the accuracy principle.

2 Extensive Unlawful Records Retention

- Data minimisation principles are frequently overlooked, with little evidence of regular deletion or reduction over time.
- Few firms have robust processes for regular data cleansing or lifecycle management.

3 Rapid Adoption of AI and Data Enrichment Tools

- Tools like **Catchlight** are used to enrich lead profiles using publicly available and third-party data, applying machine learning to score and prioritise prospects.
- Platforms such as **InvestCloud** integrate Generative AI to build dynamic client profiles based on behavioural, transactional, and risk-related data.
- These innovations raise questions about transparency, lawful basis, and fairness in automated decision-making.

4 Inadequate Third-Party Risk Management

- Personal data is frequently shared with brokers, insurers, administrators, and trustees, often without sufficient contractual safeguards.
- Many third-party vendors are based or hosted outside the EU, increasing the risk of non-compliance with international data transfer requirements under GDPR.

Sector Risks *(contd)*

5 Weak Internal Governance and Security Controls

- Some organisations operate with outdated systems, poor encryption standards, and weak internal controls, exposing personal data to cyber threats and fraud.
- Sensitive data (e.g. health, financial, PEP, and children's data) is often processed without appropriate safeguards.

6 Ambiguity in Roles and Responsibilities

- There is widespread confusion over whether independent financial advisors, trustees, or administrators act as data controllers or processors.
- This misclassification leads to gaps in accountability, such as absent contractual clauses or incomplete data protection impact assessment.

7 Deficient Consent and Transparency Mechanisms

- Many firms lack effective consent management systems.
- Privacy and cookie notices are sometimes missing, incomplete, ageing or non-compliant with legal standards.

The industry is at a crossroads as to whether IFAs, trustees or administrators **act as data controllers or processors**.

Regulatory Landscape

The Financial Conduct Authority (FCA) has rolled out a major update to its data governance framework under the FCA Data Requirements 2025 program.

This program introduces enhanced governance standards, mandatory data quality metrics, and real-time reporting capabilities. These updated data requirements for 2025 represent the most significant regulatory change in data governance since MiFID II implementation. These requirements affect all authorised firms, from tier-one banks to boutique investment managers, mandating fundamental changes to data collection, processing, storage, and reporting practices.

At the same time the UK is also undergoing significant changes in its data privacy landscape, primarily driven by the Data (Use and Access) Act 2025 (DUAA). This supplementary legislation has introduced targeted reforms to the existing UK GDPR and the Data Protection Act 2018.

The **FCA Data Requirements 2025 mandate fundamental changes** to data collection, processing, storage, and reporting practices.

Regulatory Landscape *(contd)*

Key Sector Challenges and Regulatory Alignment

1 Excessive Data Collection and Retention

Issue: Firms collect vast amounts of personal data, often without clear purpose or regular review. Data minimisation and deletion practices are weak.

- **FCA alignment:**
  - » **Data Minimisation (Due 30/06/25):** Firms must collect and retain only data strictly necessary for their services.
  - » **Subject Rights:** Enhanced processes for deletion and correction are now mandatory.

2 Inadequate Consent and Transparency

Issue: Many firms lack effective consent management systems. Privacy and cookie notices are often incomplete or non-compliant.

- **FCA alignment:**
  - » **Consent Management (Due 30/06/25):** Firms must implement granular consent mechanisms, enabling users to easily manage their preferences.
  - » **Fair Processing & Transparency (Due 30/09/26):** Clear communication of data use, lawful basis, and client rights is now required.

Regulatory Landscape *(contd)*

3 AI and Data Enrichment Risks

Issue: Tools like Catchlight and InvestCloud use AI and third-party data to profile clients, raising concerns around transparency, fairness, and lawful processing.

- **FCA alignment:**
  - » **Fair Treatment (Due 30/09/26):** Firms must ensure data processing, including AI-driven profiling, is fair, transparent, and in clients' best interests.
  - » **Audit Trails:** All data processing activities, including automated decisions, must be documented.
- **DUAA alignment:**
  - » Organisations must implement safeguards to protect individuals affected by automated decision making. Reforms to expand the lawful bases for processing of this type to legitimate interests which was previously restricted.

4 Weak Third-Party and Cross-Border Data Controls

Issue: Data is frequently shared with brokers, insurers, and administrators — often without adequate contracts or clarity on roles. Cross-border transfers lack robust safeguards.

- **FCA alignment:**
  - » **Operational Resilience (Due 31/03/26):** Emphasis on third-party risk management and data protection in outsourcing arrangements.
  - » **Data Governance (Due 30/09/25):** Clear policies and accountability structures must be in place for all data handling, including third-party relationships.
- **DUAA alignment:**
  - » The aim is to simplify mechanisms for cross-border data flows including streamlined adequacy decisions and support for smart data schemes. Organisations must, however, ensure these schemes and cloud providers meet UK adequacy and safeguard standards.

Regulatory Landscape *(contd)*

5 Poor Internal Governance and Security

Issue: Some firms operate with outdated systems, weak encryption, and insufficient internal controls, increasing exposure to cyber threats.

- **FCA alignment:**
  - » **Cyber Resilience (Due 31/03/26):** Firms must enhance cyber incident response and test backup/recovery systems regularly.
  - » **Mandatory Board Oversight & CDO Appointment (Due 30/09/25):** Senior accountability for data governance is now a regulatory requirement.
- **DUAA alignment:**
  - » The DUAA introduces enhanced expectations for data governance, including clearer documentation of processing activities and decision making logic.

6 Data Quality and Real-Time Reporting Gaps

Issue: Inconsistent data quality and lack of real-time capabilities hinder compliance and decision-making.

- **FCA alignment:**
  - » **Data Accuracy (Due 31/12/25):** Regulatory data must meet a 99.5% accuracy threshold.
  - » **Automated Validation & Real-Time Reporting (Phased from 01/01/26):** Firms must implement automated checks and submit certain reports within 15 minutes of execution.

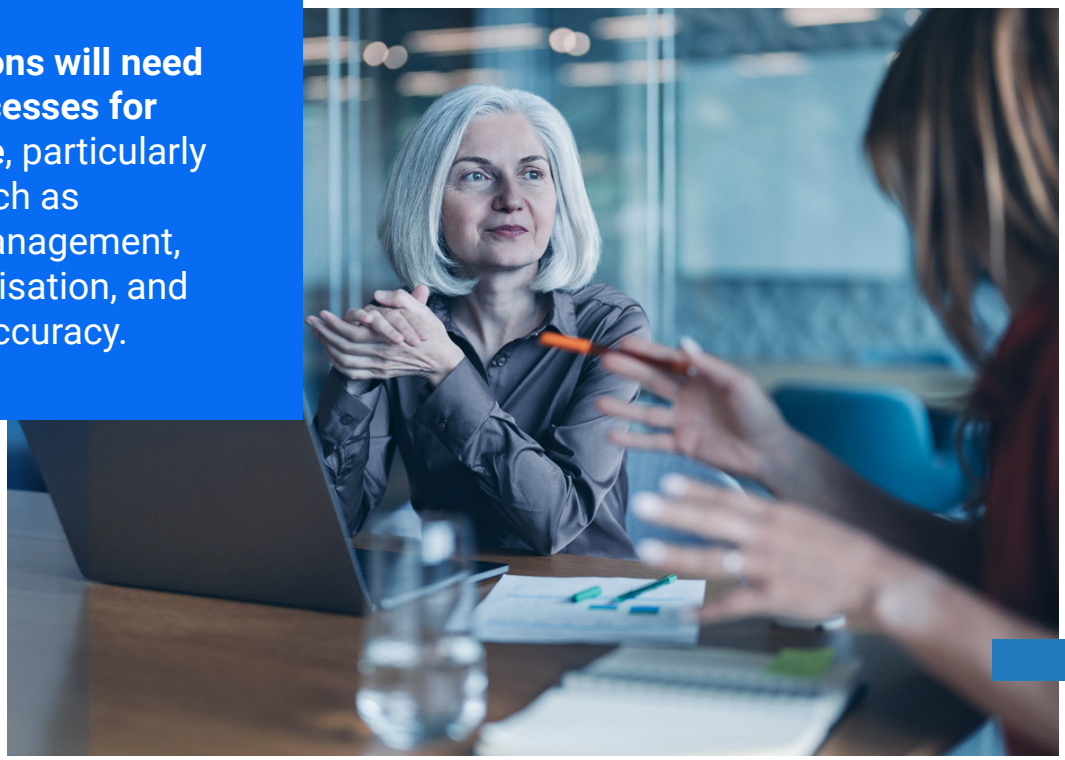
Regulatory Landscape *(contd)*

7 Ambiguity in Data Roles and Responsibilities

Issue: Confusion persists around whether independent financial advisors, trustees, or administrators are acting as controllers or processors, leading to gaps in compliance.

- **FCA alignment:**
  - » **Comprehensive Policies (Due 30/09/25):** Firms must clearly define roles, responsibilities, and data handling procedures across all entities.

Organisations will need to test processes for compliance, particularly in areas such as consent management, data minimisation, and reporting accuracy.



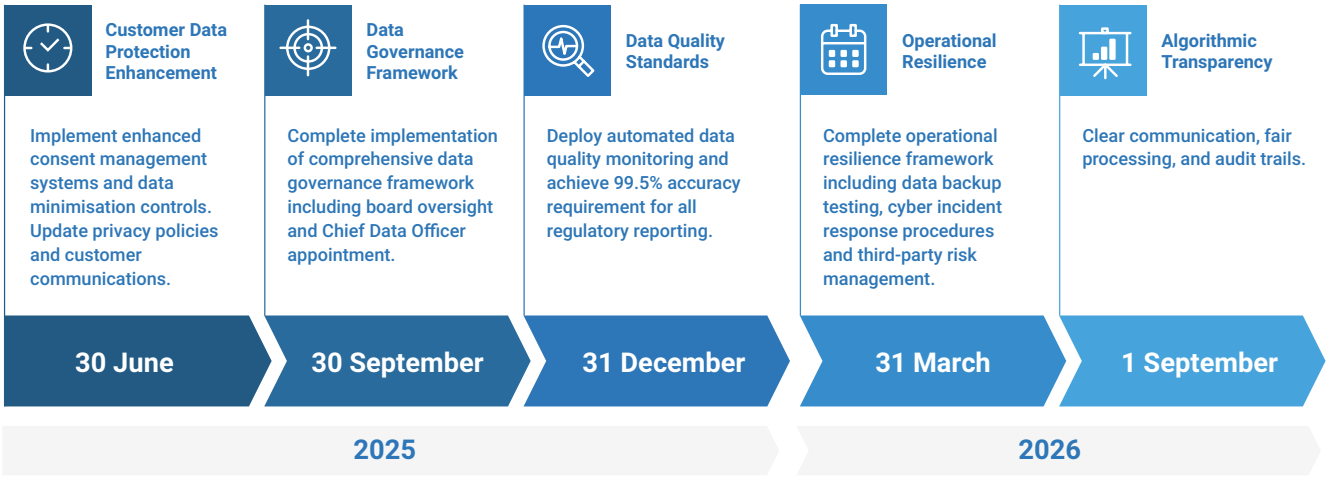
Summary

Overall, there is a strong push to align with broader data protection laws, which means organisations will need to take a series of steps.

This includes revisiting and updating data governance and customer protection policies and managing third-party risks through contractual reviews for both existing and new suppliers. Organisations will need to test processes for compliance, particularly in areas such as consent management, data minimisation, and reporting accuracy. It will be important to develop staff by training them on the new requirements and customer rights. Finally, completing the necessary privacy documentation and assessments will be essential to demonstrate compliance.

Initial provisions of The Data (Use and Access) Act 2025 have commenced with secondary legislation to be rolled out over the coming months. It is a similar story for the FCA Data Requirements (2025) which follow these implementation timelines:

FCA Data Requirement implementation timeline



How we can help

Data protection reforms are not optional. They are imminent, enforceable, and far-reaching. Firms that delay risk falling behind both regulatory expectations and industry standards. Now is the time to act.

With the emphasis on a practical approach, Securys provides expert, actionable insight to help your organisation meet these challenges head-on. Our services are designed to accelerate your compliance journey and embed robust data governance across your operations.

With decades of experience delivering data privacy compliance within the financial services sector, we are well-versed in operating within a highly regulated environment and expert at navigating the complex intersections between financial regulation and data protection law.

We can help you:

1. **Assess your current data governance maturity** and identify priority areas for remediation
2. **Conduct targeted privacy audits** to uncover gaps and ensure alignment with FCA and DUAA requirements
3. **Design and implement compliant frameworks** for consent management, data retention, and minimisation
4. **Review and strengthen third-party contracts** and cross-border data transfer arrangements
5. **Clarify roles and responsibilities** across your data ecosystem to eliminate ambiguity and ensure accountability.

Don’t wait for enforcement to drive change.

Contact us today to begin your compliance transformation, to establish your data governance for the new era and secure your competitive edge.

T 0800 193 8700
E info@securys.co.uk

About Securys

Our approach

We believe privacy matters because people matter. We are a specialist consultancy focused on the human side of data governance.

Securys brings a global view to data privacy, information security and AI ethics, specialising in managing practical approaches to international variance in legislation and regulation. Based on its experience working with enterprise clients in over 60 jurisdictions worldwide, Securys draws on the expertise of an international team of multilingual consultants to engage with key stakeholders at all levels of a business in order to develop a profound understanding of the way clients work.

Our experience

Securys has delivered global information security, privacy, data governance and ethical AI services to clients around the world. We use our wide and deep experience of cyber, data protection, regulation and governance to bring a strongly practical approach to helping organisations of all sizes protect themselves and their stakeholders.

From the Arctic Circle to Australia Securys has supported enterprise and SME clients alike across sectors as diverse as financial services, commodities extraction, healthcare and luxury retail, as well as supporting the non-profit sector in the UK and beyond.

Our team

Collectively our team has a wealth of relevant data protection, information security and AI governance certifications, including CIPP/E, CIPP/A, CIPP/US, CIPT, CIPM, FIP, CISSP, ISSMP, CISA and AIGP. Our privacy and information security management framework is certified by BSI to comply with ISO27001 and ISO27701. We are corporate members of the International Association of Privacy Professionals. More importantly we have decades of collective experience in the management and governance of organisations, so we know how to put the theory into practice.

Securys™
Global Data Privacy Experts

T 0800 193 8700
E info@securys.co.uk
W www.securys.co.uk

securys-limited

UK0046/1225