



2026

HOW TO MANAGE AND REPORT YOUR DATA

A good practice guide by the
Consumer Duty Data Forum

Foreword

Data has become one of the most important assets in our sector. When used well, it shapes how we understand our clients, how we evidence good outcomes, and how we meet the evolving expectations of the regulator. Yet for many advice firms, particularly smaller ones, knowing where to start in terms of a data strategy can feel daunting.

This guide has been created to give firms clear, practical steps to strengthen their data management without unnecessary complexity. It brings together the insights of RegTech, data, and consultancy experts, with one shared aim: to help firms use data confidently, safely and responsibly.

Good data practice isn't about adopting complicated systems and processes – it's about clarity, consistency and embedding simple habits that support better decisions and more meaningful impact for your clients and your business. I hope this guide helps you to take those steps with confidence.

Chris Davies

Chair, Consumer Duty Data Forum



TABLE OF CONTENT

01

SKILLS AND STANDARDS

Improve data skills
Set data standards

02

DATA MANAGEMENT AND CONTROL

Manage data and technology
Formalise data storage
Improve data integrity
Manage distribution chain data flows
Tighten data access and cyber security
Ensure safe and ethical use of AI

03

MEET SPECIFIC FCA REQUIREMENTS

Prepare for FCA Section 165 Information Requests
Map your firm's FCA returns schedule

04

BECOME A DATA-DRIVEN BUSINESS

Treat data as a core business asset

WHY FIRMS OF ALL SIZES NEED A DATA STRATEGY

The Financial Conduct Authority (FCA) now takes a data-driven approach to supervising financial advice and planning firms. The FCA is gathering structured and comparable data from firms, regardless of their size. For example, you will have seen the June 2025 Adviser Survey, which sent to all 5,000 advice and planning firms with 12 weeks to respond.

The FCA aims to use this data to:

- Better understand business models, charging structures, client outcomes
- Spot risks early before complaints or problems arise.

All financial advice and planning firms must now be able to understand and analyse data so that they can properly meet requirements. In line with the FCA's approach to Consumer Duty however, it would expect a firm's data strategy to be proportionate to its size, role and influence over client outcomes.

If your firm is an appointed representative, then you will also need to check your data strategy is aligned with the requirements of your network or principal firm.

Data is the cornerstone of informed decision making, governance, risk and compliance management, and evidences the good outcomes firms achieve for their clients.

In this guide, you'll learn how to put into practice principles about data management and reporting. We have grouped the principles into four themes.

Theme	Principles
Skills and standards	Improve data skills: Ensure all staff understand key data concepts and use data effectively in daily operations. Set data standards: Adopt industry data standards and frameworks for consistency and compliance.
Data management and control	Manage data and technology: Assign clear system ownership, standardise workflows and build operational resilience. Formalise data storage: Understand where you store data in your firm. Improve data integrity: Control and validate critical data, and keep clear records for compliance.

Theme	Principles
	Manage distribution chain data flows: Gather the right information from product providers, assess their strategy, and return the required data. Tighten data access and cyber security: Limit data access, secure systems, and prepare for cyber incidents. Ensure safe and ethical use of AI: Use AI responsibly with high-quality data, ethical oversight, and regular review.
Meet specific FCA requirements	Prepare for FCA Section 165 Information Requests: Respond promptly with accurate data and clear documentation for FCA requests. Map your firm's FCA returns schedule: Track and comply with updated FCA reporting requirements to streamline processes.
Become a data-driven business	Treat data as a core business asset: Data should be key to firms' businesses, and not a byproduct of systems.

SKILLS AND STANDARDS

IMPROVE DATA SKILLS

Here are some steps your firm can take to ensure that all employees understand key data concepts and how to use data effectively in daily operations.

Baseline data literacy across roles:

All staff should share a basic understanding of key data items such as client, product, charges, suitability, vulnerability indicators and outcomes. Your firm should have a glossary for key data terms, which should be used in inductions and ongoing training.

Digital transformation grounded in processes:

Firms should document where data is created, amended and relied on across the advice lifecycle. This helps identify duplication, gaps and manual workarounds that increase risk and reduce capacity.

Here are examples of applied data use in day-to-day operations:

- Comparing datasets to identify breaks and exceptions (for example, data from your CRM, platform provider and finance)
- Monitoring data completeness and timeliness as part of MI
- Segmenting clients consistently to support capacity planning and fair outcomes. Firms should segment clients according to agreed attributes such as life stage, servicing tier, product mix and review frequency.



IMPROVE DATA SKILLS

By adopting industry data standards and frameworks, your firm can ensure consistency in compliance. This includes using recognised templates, structured data principles, and preparing for evolving regulatory requirements.



In the appendix of this guide, you'll find a framework for distribution data reporting standards that can help your firm to identify key data criteria across services, distribution chains (products, platforms, tech) and client activity.

The framework includes:

- **What data** you currently provide
- **Who** you provide that data to
- **The format** you provide it in
- **The channels** you will provide data through
- **The timescales** for providing data requested

Align to recognised industry structures

Where your firm receives or distributes product data, use the [FinDatEx EMT v4.2](#) template to store product, costs, and target market data in a consistent and reusable way.

Use structured data principles from ISO 20022

The [ISO 20022](#) standard gives everyone in finance a common way to organise and share payment data. It replaces older formats like SWIFT MT. This standard makes payments easier to automate, check for fraud, and share between banks. By using clear fields and set values instead of free text, firms can move data smoothly between systems and reduce mistakes.

Adopt UK market data standards where available

Use [Criterion standards and checklists](#) to standardise data requests and responses across platforms, providers and advisers.

Prepare for regulatory data change

The [FCA's Transforming Data Collection programme](#) shows a move toward more structured, granular and reusable firm data. Firms should review what you submit, where it is sourced, and how repeatable your process is.

DATA MANAGEMENT AND CONTROL

MANAGE YOUR DATA AND TECHNOLOGY

This section deals with how to manage your data and technology. Some examples are defining ownership of core systems, standardising workflows, and avoiding unmanaged spreadsheets.

Clear system ownership

Firms should define which system is the source of truth for client status, fees, review dates and advice records. If an individual builds a spreadsheet for their needs first, make sure it is reconciled with core systems. Avoid unmanaged spreadsheets.

Practice management and CRM discipline

In your practice management and CRM, firms should standardise workflows, mandatory fields and templates so advice evidence is consistent. Firms should be able to review advice via automated meeting notes and CRMs automatically updated with relevant and complaint information.

Operational resilience

To make sure that your operations are resilient, firms should:

- Identify important business services
- Map dependencies across internal systems and third parties
- Test realistic disruption scenarios, including data loss and supplier failure.

Integration and access control

For integration and access control, firms should:

- Prefer secure integrations with two-way data flows, over manual rekeying
- Document data flows, access rights and hand-offs between systems and suppliers.
- Put in place a documented off-boarding process that sets out what data a departing employee or third-party partner can access and how this should be reviewed, removed, or secured.

Assessing data trends and themes

Although you do not have to have data scientist expertise in-house, getting skill sets and strategies for assessing your data is good business practice. It's essential to business, client management and regulatory reporting. If your firm can get insights on data relationships and trend analysis, you will better be able to tackle key regulatory risks such as:

- Foreseeable harm
- Vulnerabilities
- Cost benefit analysis



FORMALISE DATA STORAGE

This section deals with how to manage your data and technology. Some examples are defining ownership of core systems, standardising workflows, and avoiding unmanaged spreadsheets.

Data lake

A data lake is a place to keep all your raw data in one spot. For small firms, this can be as simple as using structured OneDrive or SharePoint folders, or automated exports from your CRM or platforms into secure cloud storage.

Data warehouse

A data warehouse is a more organised store of clean, structured data – a “ready-to-use” library. This is typically what supports dashboards, FCA reporting, MI packs and Consumer Duty monitoring. Many firms use tools like Power BI dataflows or managed CRM data warehouses for this purpose.

IMPROVE DATA INTEGRITY



Strong data integrity means a firm's data is accurate, reliable and well-controlled, and supports trust, compliance and confident decision-making.

Here are some practical ways to improve data integrity:

- **Define critical data elements:** identify the small number of fields that materially affect advice quality, fees, reviews and regulatory reporting, and apply stronger controls to them.
- **Validation and reconciliation:** build routine checks between systems (e.g. CRM versus platform valuations) and investigate exceptions promptly.
- **Change control:** log who can amend key client and advice data, when changes are made, and why. This supports audit, complaints handling and regulatory enquiries.
- **Retention and versioning:** ensure historic advice records and data snapshots are preserved and retrievable, particularly where recommendations or client circumstances change.

MANAGE DISTRIBUTION CHAIN DATA FLOWS

The rules make it clear that everyone in the distribution chain has their own responsibility for managing and sharing data properly. This is essential for delivering good outcomes for clients and helping to prevent foreseeable harm.

PRIN 2A.3.16–18 says that advice firms must get enough accurate and reliable information from product providers, check that the provider's distribution strategy is appropriate, and then give providers the information they need in return – including sales data and details from regular reviews of how products are being distributed. In the appendices, we've included two data-flow templates to show the types of information involved and how firms can use them for reporting.

TIGHTEN DATA AND CYBER SECURITY

Protecting your firm's data is about more than just technology. It's about building trust, meeting regulatory requirements, and ensuring your business can keep running smoothly even when faced with cyber threats. By taking a proactive approach to data and cyber security, firms can safeguard sensitive information, reduce risks and respond effectively to incidents.

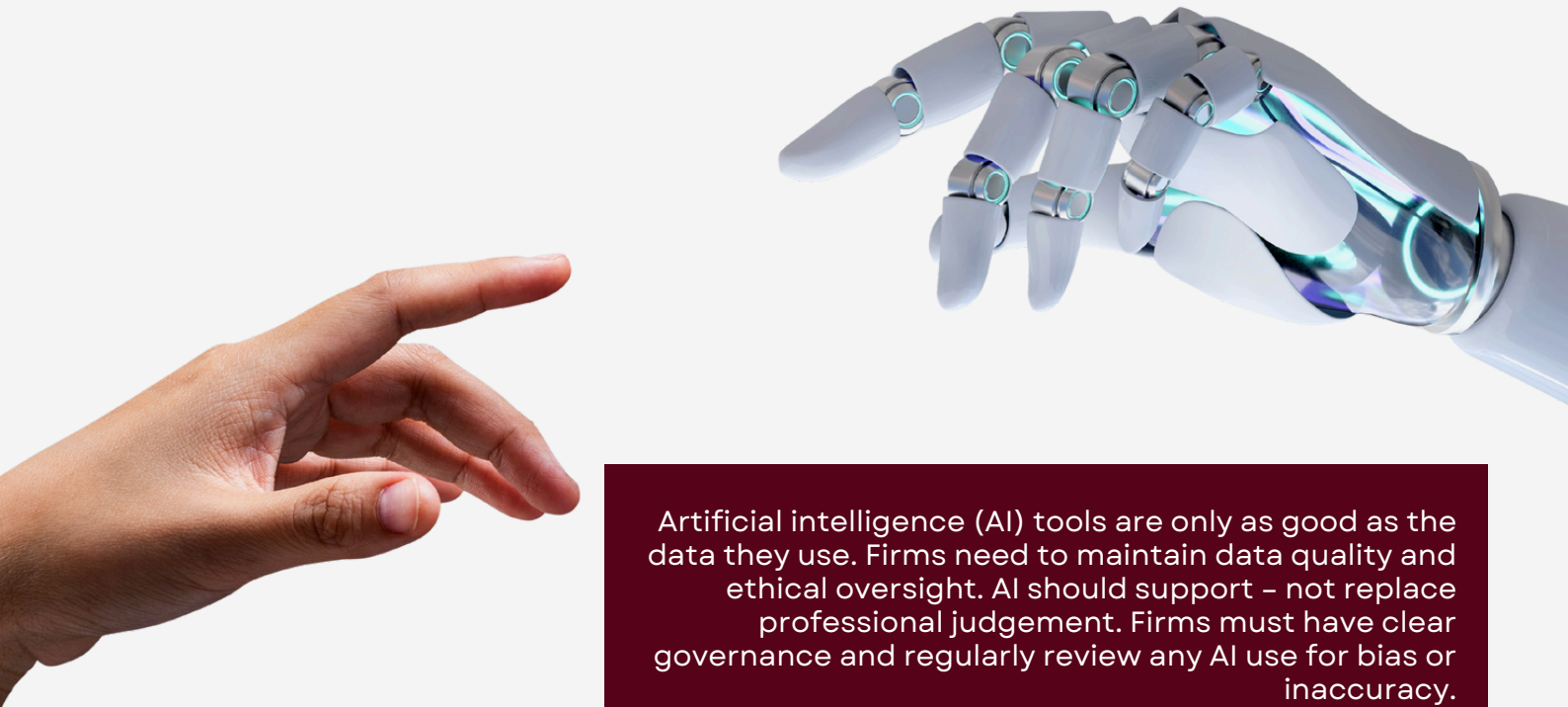
Consider taking these five steps:

1. **Access control:** ensure staff access only the data and systems required for their role, with regular reviews as roles change. This is referred to as the principle of least privilege.
2. **Third-party risk management:** assess cyber and data security controls for platforms, CRMs, IT providers and outsourced services, not only for internal systems.
3. **Data protection:** encrypt sensitive data, secure backups, and test recovery processes regularly to reduce operational and client impact.
4. **Adopt password management software:** helps keep accounts secure.
5. **Incident readiness:** maintain a clear incident response plan covering data breaches, system outages and ransomware, with defined escalation and FCA reporting processes.
6. **Cyber security resource library:** Make sure your firm has a library for cyber resources. Here are some examples of useful documents:

- [FCA Cyber Coordination group insights 2024](#)
- [FCA Cyber security insights](#)
- [ICO security including Cyber Security](#)
- [Nation Cyber Security Centre \(NCSC\) advice for SMEs](#)



ENSURE SAFE AND ETHICAL USE OF AI



Artificial intelligence (AI) tools are only as good as the data they use. Firms need to maintain data quality and ethical oversight. AI should support – not replace professional judgement. Firms must have clear governance and regularly review any AI use for bias or inaccuracy.

Meeting business and client needs

AI is now built into many financial services tools, such as CRM systems and client analysis software. For advice firms, the main benefit of AI is to improve everyday work, not to do complex modelling. The focus should be on using AI to help with tasks and integrating it into workflows, supported by good quality underlying data to meet real business and client needs.

Data quality and AI

Before deploying AI-enabled tools, firms should assess whether their data is complete, current, consistent and suitable for the intended use. This includes:

- Checking data quality, for example, identifying missing fields, outdated client information and inconsistent classifications. Poor data quality can lead to misleading outputs, inappropriate prioritisation or unsupported conclusions.
- Understanding where data originates and how often it is refreshed.
- Understanding whether data reflects real client circumstances.

Ethical use

AI should support – not replace – professional knowledge and judgement, and outputs need to be assessed in terms of being explainable and fair.

Bias and risk

AI models can sometimes treat certain groups unfairly if the data they use reflects old habits or missing information. Firms should regularly check AI results for unexpected

patterns and make sure they don't use protected characteristics unless there's a clear legal reason. This helps prevent unfair treatment and outcomes.

Governance is critical

Firms must document:

- What AI tools are in use (including those embedded in third-party systems)
- What data they access and how it is used (e.g. whether it is used to train public language models such as Open AI or Claude)
- If large language models (LLMs) access data, document if this data is protected, how your use of AI complies with data protection laws, reviews of data segmentation, and retention and deletion policies.
- Which jurisdiction the data is housed under.
- Any decisions the AI tools influence
- AI controls and oversight, for example, when and how humans will check any output.
- Good practice is to adopt a due diligence questionnaire and a structured process for ongoing supplier reviews.

Change management processes

These processes should cover model updates, system upgrades and vendor changes, with testing before deployment. Staff using AI-enabled tools need training not only on functionality, but also on limitations and appropriate challenge to AI outcomes as necessary.

Align with Consumer Duty expectations

Firms should be able to show how AI tools support good client outcomes, fair treatment and effective monitoring, rather than only efficiency gains. If AI is used for monitoring, triage or MI, firms should ensure that special cases, such as execution only and vulnerable clients, are not overlooked because they do not fit standard patterns.

In short, AI can be helpful for advice firms, but only where data quality, governance and ethics are treated as core operational responsibilities rather than technical add-ons.



COMPLIANCE WITH SPECIFIC FCA REQUIREMENTS

MAP YOUR FIRM'S FCA RETURNS SCHEDULE



It's important to map your FCA data reporting and regulatory returns schedule by due date, type and frequency and estimated time to complete. Appointed representative firms should liaise with their network or principal firm to understand their requirements.

The FCA's [Transforming Data Collection programme](#) has already removed data returns across a number of areas and further decommissioning is planned:

- **FSA039** – Client money and client assets
- **RMA-F** – Section of the **Retail Mediation Activities Return (RMAR)**
- **RMAR** reporting across certain sections moves from **2x to 1x per annum**
- **Form G** – an event driven adviser complaints notification
- Decommission REP022 (General Insurance Pricing Attestation) and retail investment advisers (RIA) complaints.
- Reduce the frequency of reporting for **REP009 (Consumer Buy-To-Let Mortgage Aggregated Data)**.
- Remove the requirement to submit nil returns for **REP008 (Notification of Disciplinary Action relating to conduct rules staff – other than senior manager functions)**.

PREPARE FOR FCA SECTION 165 INFORMATION REQUESTS

The FCA uses Section 165 requests to collect structured and comparable data from advice and planning firms. Treat any requests as urgent and mandatory. Pay attention to your data when you prepare your response.

Section 165 requests help the FCA to assess business models, charging structures, client outcomes and sector risks under the Consumer Duty. By gathering this data, the FCA can identify risks early, and support a more proactive and data-led approach to supervision.

If you receive a Section 165 request from the FCA or your principal firm, treat it as urgent and mandatory. Double-check your data for consistency, involve key teams across compliance, operations, finance, and IT, and provide clear explanations of how you meet Consumer Duty standards. Always keep a record of what you submit, including raw data, calculations, and approvals, in case the FCA asks for more details later.

What firms must do to prepare:



Keep your data accurate and easy to access. Make sure your records match FCA definitions for things like clients, products, fees, complaints, and more.



Set up strong data governance and ownership. Document who owns what data, keep track of changes, and maintain clear audit trails.



Make your systems FCA-friendly. Ensure your core platforms can export data in formats the FCA expects, like structured CSV or Excel files.



Be transparent about your methods. Clearly explain how you segment clients, assess value, categorise advice, and select products.



Strengthen your controls. Protect your data with robust systems, backups, access management, and incident response plans.

BECOME A DATA-DRIVEN BUSINESS



What is a data-driven business?

Being data-driven means treating data as a core business asset that underpins client service, internal processes, and regulatory reporting.

This starts with clear data ownership, consistent definitions, and documented data flows across advice, suitability, fees, products, and client outcomes.

Core systems like CRM, platforms, AI, cashflow tools, and compliance are integrated so staff can access accurate, timely data for advice delivery. Sensitive information remains protected in line with data protection rules.

Ongoing monitoring, validation, and audit trails support reliable FCA reporting and early identification of risks. Embedding cyber security and resilience testing into your data framework helps keep data secure and available, even during disruptions.

In summary

Becoming a data-driven business with a clear data strategy empowers firms to deliver better client service, streamline internal processes, and meet regulatory requirements with confidence.

By treating data as a valuable asset and integrating systems, firms can ensure information is accurate, accessible, and secure. With ongoing monitoring and strong data practices, firms are perfectly positioned to respond to evolving regulatory requirements and support positive outcomes for clients and the business.

APPENDICES

SKILLS AND STANDARDS

- Introduce a documented Data Governance framework: named Data Owners, Data Stewards and defined Critical Data Elements (CDEs). Find more information [here](#).
- Maintain a central data glossary and taxonomy register aligned to FCA definitions – example: [Data and Tech taxonomy](#).
- Use this framework to help your firm to identify key data criteria across services, distribution chains (products, platforms, tech) and client activity – [Distribution Data Reporting Standards Framework](#)
- Considering aligning cyber controls to [Cyber Essentials Plus](#) or [ISO 27001](#).
- [FinDatEx EMT v4.2 template](#)
used to store product, costs, and target market data in a consistent and reusable way.
- [Criterion standards and checklists](#)
used to standardise data requests and responses across platforms, providers and advisers.
- [ISO 42001](#)
The world's first international standard for managing AI responsibly
- [ISO 20022](#)
A global standard for how financial institutions structure and share payment and transaction data.

MEET SPECIFIC FCA REQUIREMENTS

- Maintain a controlled Regulatory Reporting Calendar with named owners –example of [FCA returns schedule](#).
- Keep up-to-date with [the FCA's Transforming Data Collection programme](#).