Date informal advice provided: 14 January 2025

This advice represents the position as at the date the advice provided. Businesses should consult relevant information and guidance on regulators' websites to keep up to date with the latest developments

CASE STUDY:

FCA Authorisation and Data Protection Considerations for Firms using AI to Assist Financial Advisors

Response from the FCA and ICO

This is an anonymised version of a query submitted to the DRCF AI and Digital Hub ('the Hub').

The query in this case study has been responded to by the following DRCF regulators ('we', 'us', 'our'):

- Financial Conduct Authority ('FCA'); and,
- Information Commissioner's Office ('ICO').

This informal advice is provided in line with the Conditions for Participation.

Our informal advice is provided to a business based on our current understanding of the legal and regulatory frameworks within our remits and how they apply to the business's service. This informal advice should not be treated as an exhaustive account of the issues linked to a business's service or represent an endorsement of their proposed innovation.

Our informal advice is specific to a business's circumstances as described by them in the information they provided to the Hub.

Our informal advice is provided without prejudice to any future regulatory intervention by any DRCF or non-DRCF regulator and nor is it a substitute for independent legal advice which a business may wish to seek in advance of the launch their service.

It is ultimately a business's responsibility to assess their position under the law and regulatory regime, with the benefit of independent legal advice as necessary. Recognising that some regulatory regimes are still developing and could change over time, businesses have a responsibility to keep up to date with the latest position.

A non-confidential version of the informal advice provided to the applicant is attached to this case study. This informal advice was provided on 14 January 2025 and represents the position as at 14 January 2025. Businesses should consult

relevant information and guidance on regulators' websites to keep up to date with the latest developments.

Summary of query and response

- Business A sought clarification on whether their product required FCA authorisation, including the type of authorisation, the timing, and the application process. Business A also requested guidance on complying with data protection law.
- Business A's software product is designed to assist financial advisors in streamlining workflows and is currently capable of:
    - Note-taking: AI captures meetings and client interactions in real-time, reducing the need for manual notes.
    - Document creation: AI automatically drafts documents such as suitability letters, client reports, and follow-up communications, thereby reducing time spent on administrative tasks.
    - CRM updates: A tool that automatically updates the CRM system with key client information after meetings.
- The response lays out FCA's perimeter guidance, how to get authorised and some key data protection considerations as the firm further develops the business proposition.

Introduction to the regulators

This query has been responded to by the FCA and ICO. A brief introduction to each regulator has been included below.

Each regulator is responsible for separate legal regimes with different requirements that may be applicable to the same set of facts, and it will be necessary to take steps to comply with each regime as set out.

FCA

The Financial Conduct Authority (FCA) is the UK's financial services regulator with focus on reducing and preventing serious harm, setting higher standards and promoting competition and positive change.

The FCA regulates the conduct of around 42,000 businesses and prudentially supervises around 41,000 firms.

The FCA oversees the following regulations which are relevant to this informal advice:

- Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO)

ICO

The Information Commissioner's Office (ICO) is the UK's independent public authority set up to uphold information rights. The ICO oversees the UK General Data Protection Regulation (UK GDPR), which is relevant to this informal advice.

Regulator Response References

In the below table, we have set out the relevant regulator and the respective responses that they have input on. Each regulator is only responsible for the responses within their regulatory remit as noted in this table.

Regulator	Relevant Responses
FCA	1, 2
ICO	3

Response

1. Perimeter Activities (requiring authorisation)

1.1. The FCA's perimeter is set through legislation, primarily the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO), which sets out activities regulated by the FCA. Within the FCA Handbook, which contains (among other things) rules and guidance set by the FCA, the Perimeter Guidance Manual (PERG) provides guidance on the perimeter to assist firms in determining for themselves whether they need to be authorised by the FCA to carry out their activities.

1.2. It is the firm's responsibility to ensure it has determined, based on the progressive stages of your business development, whether and at what stage its business activity falls within the perimeter. Based on the information provided in your query and in response to questions asked, the FCA believe there is a possibility that the firm's (current and proposed) activities could fall under one or both of the following:

- *arranging (bringing about) deals in investments* which are *securities*, *relevant investments*, *structured deposits* or the *underwriting capacity of a Lloyd's syndicate* or *membership of a Lloyd's syndicate* (article 25(1)) RAO;
- *making arrangements with a view to transactions in investments* which are *securities*, *relevant investments*, *structured deposits* or the *underwriting capacity of a Lloyd's syndicate* or *membership of a Lloyd's syndicate* (article 25(2)) RAO.

1.3. FCA guidance on these activities is contained at PERG 2.7.7. For example, PERG 2.7.7B states that "The activity of *arranging (bringing about) deals in investments* is aimed at arrangements that would have the direct effect that a particular transaction is concluded (that is, *arrangements* that bring it about). The activity of *making arrangements with a view to transactions in investments* is concerned with arrangements of an ongoing nature whose purpose is to facilitate the entering into of transactions by other parties."

1.4. PERG 2.7.7BA goes on to state that "the *regulated activity* of *making arrangements with a view to transactions in investments* is not limited to arrangements that are participated in by investors. It is also not necessary that both the buyer and the seller under the transaction that is being arranged should participate in the arrangements. So, arrangements may come within the activity if they are participated in only by product companies with a view to their issuing investments." In other words, there does not necessarily need to be direct

interaction with the consumer for the activities of a firm to fall within the regulated activity.

1.5. There is further guidance on these activities at PERG 8.32 (although this guidance relates to the activities of publishers, broadcasters, website operators and telephone marketing services, the firm may wish to consider whether any of the principles therein may apply to the firm's activities). As noted in PERG 8.32.2, "Article 25(1) applies only where the arrangements bring about or would bring about the particular transaction in question", which is only if the "involvement in the chain of events leading to the transaction is of enough importance that without that involvement it would not take place." Whereas the scope of Article 25(2) "is potentially much wider as it does not require that the arrangements would bring about particular transactions."

1.6. In PERG 8.32.3, for the services listed to fall within Article 25(2), the FCA's guidance states that it considers they must be made "with a view to the *authorised* or *exempt* (or overseas) *person* or that *person*'s customers or counter parties or any or all of them *buying* or *selling investments*. This means that a *person* making arrangements must take account of the purpose for which he makes them."

1.7. These are the factors which the FCA invites the firm to contemplate. That being said, it is the firm's responsibility to ensure it has considered whether their activities fall within the FCA's perimeter and if so to obtain the necessary authorisations. This consideration should not necessarily be limited to the factors mentioned above.

1.8. It would also be beneficial to consider whether your proposed activities might fall under Article 53 (1) RAO (advising on investments). As set out in Article 53(1), your services would fall within this activity if:

- is given to a *person* in his capacity as an investor or potential investor, or in his capacity as agent for an investor or a potential investor; and
- is advice on the merits of his (whether as principal or agent):
  - *buying*, *selling*, subscribing for, exchanging, redeeming, holding or underwriting a particular investment which is a security, a structured deposit or a relevant investment; or
  - exercising or not exercising any right conferred by such an *investment* to *buy*, *sell*, subscribe for, exchange or redeem such an *investment*.

1.9. The FCA points you towards the perimeter guidance on this activity from PERG 8.24 onwards. For example, from PERG 8.27.2: "Art 53(1) does not apply where

the advice is given to persons who receive it as (1) an adviser who may use it to inform advice given by him to persons for whom he does not act as agent."

1.10. The FCA also refers you to PERG 8.30.5: "Some software services involve the generation of specific *buy*, *sell* or hold signals relating to particular *investments*. These signals are liable, as a general rule, to be advice for the purposes of article 53(1) (as well as *financial promotions*) given by the *person* responsible for the provision of the software. The exception to this is where the user of the software is required to use enough control over the setting of parameters and inputting of information for the signals to be regarded as having been generated by him rather than by the software itself."

1.11. Again, the firm should consider for itself whether there are any other potentially applicable regulated activities to which the services intended to be provided by the firm may apply and consider on that basis whether it requires authorisation.

2. Authorisation

2.1. It is ultimately your responsibility to determine if your business requires authorisation and what type of authorisation you would require. The resources below provide guidance on the process.

- PERG 2 Annex 1 contains a flowchart to help firms identify whether they need to be authorised.
- FCA Authorisation Process.
- You may also be interested in guidance for regulated firms on their use of third-party providers and operational resilience.
- The FCA and Bank of England (BoE) recently released information (on 12/11/2024) on its expectations for critical third parties.

3. Data Protection Considerations

3.1. If you process personal data, then you will need to comply with the UK General Data Protection Regulation (UK GDPR). As you have advised, personal data may be processed when your AI tool helps to draft suitability letters. Personal data includes an individual's name, contact details, and income, as well as anything derived or attributed to them by your AI tool, such as potential financial vulnerabilities or risk appetite. In practice, this means you will need to consider a number of your obligations. Below is a non-exhaustive list of some areas to consider.

Controllership

3.2. One of first aspects to consider is your controllership role in relation to the financial organisations you serve. Your role may be a joint controller, independent controller, or processor, depending on the specific processing activities. It is important to note that organisations are not by their nature either a controller or a processor. Instead, the nature of the personal data processing and how each party uses it must be assessed on a case-by-case basis.

- Controller: The organisation that decides why and how personal data is processed.
- Joint Controller: Two or more organisations that jointly decide why and how personal data is processed.
- Processor: The organisation that processes personal data on behalf of the controller, following its instructions.

3.3. The relationship between your organisation and your financial clients could come under any of these roles, depending on the circumstances. Each client relationship must be assessed individually.

3.4. From the information provided, it seems your AI tool is used by financial organisations to support tasks, such as note taking or drafting suitability letters. If your role is limited to following their instructions without determining why or how personal data is processed, you are likely acting as a processor. This may be the case if your financial clients retain control over the purpose of the processing (e.g., to provide its customers with financial advice) while using your AI tool (the 'how') to achieve that purpose. Even if your organisation determines certain technical elements, the financial organisation's control over the purpose likely qualifies your role as a processor.

3.5. However, it is crucial to ensure this reflects your actual role. If your organisation has influence or control over the why and how of processing, you could be an independent controller or a joint controller. For example, fine-tuning your AI tool based on the personal data of your financial clients could indicate joint controllership, particularly if your financial clients contribute to or benefit from your AI tool's development.

3.6. Given these complexities, it is essential to evaluate each client relationship individually to determine whether you act as a processor, independent controller, or joint controller. Once you are satisfied with your role, you should enter into an agreement with your financial clients. For example, if you determine that you are a processor, you must put in place with the controller an Article 28 UK GDPR

controller/processor contract. Reviewing the ICO's guidance on controllers and processors can help clarify your role and the associated responsibilities.

Automated Decision-Making

3.7. Data protection law applies to all automated individual decision-making and profiling. Article 22 UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

3.8. One of your key considerations will be whether the suitability letters generated by your AI tool amount to financial advice and, if so, whether they constitute a significant effect. If your AI system leads to automated decisions such as refusing customers access to financial products without human review, Article 22 will apply. Article 22 is particularly relevant when organisations use AI. Under Article 22, you can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract;
- authorised by law that applies to you; or
- based on the individual's explicit consent.

3.9. If Article 22 applies, you must:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision; and
- carry out regular checks to make sure your systems are working as intended.

3.10. Mere human involvement in the AI lifecycle does not necessarily qualify as meaningful human review. The sequencing and substance of human involvement are critical. For example, if a human inputs personal data into the AI tool and the tool then makes recommendations or classifications that lead to decisions with significant effects, this remains a solely automated decision under Article 22. The human's role in this instance does not constitute meaningful review.

3.11. For human review to be meaningful, it should occur after the automated decision has been made and involve an assessment of the actual outcome. For example, if your chatbot identifies a recommendation that appears unsuitable, meaningful

human review might involve querying the recommendation with a qualified financial advisor to ensure accuracy. This active review process would likely constitute meaningful human review.

3.12. The ICO recommends you consider the possible implications of Article 22 in your AI product and document any risks and measures you take to mitigate those risks in your Data Protection Impact Assessment (DPIA), as outlined in further detail below.

3.13. For further guidance, please refer to:

- Automated decision-making and profiling;
- Guidance on AI and data protection; and
- AI and data protection risk toolkit.

Transparency

3.14. You must provide individuals with clear and accessible transparency information, particularly if Article 22 applies to your processing activities. This includes updating your privacy notice to explain what decisions your AI tool makes, the reasoning behind those decisions, and the potential impact on individuals. Just-in-time notifications at the point of personal data collection are also recommended to ensure individuals understand how their personal data will be used.

3.15. Your financial clients must also inform their customers about the risks and benefits of your product. This will help to build trust and ensure individuals are confident their personal data will be protected by all parties.

3.16. For further information, please refer to:

- Transparency; and
- The right to be informed.

Data Protection Impact Assessment (DPIA)

3.17. It is likely that, due to the type of information you will be processing, you will need to complete a DPIA.

3.18. Article 35(3) UK GDPR lists three examples of types of processing that automatically require a DPIA. One which may apply to you is Article 35(3)(a) – Systematic and extensive profiling with significant effects:

- "(a) *any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*."

3.19. In addition, the ICO is required by Article 35(4) to publish a list of processing operations that require a DPIA. Two of these may be relevant to your processing:

- ***Innovative technology***: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI).
- ***Denial of service***: decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.

3.20. In the vast majority of cases, the use of AI will involve a type of processing likely to result in a high risk to individuals' rights and freedoms, and will therefore trigger the requirement for you to undertake a DPIA.

3.21. DPIAs are a key part of data protection law's focus on accountability and data protection by design. You should not see DPIAs as simply a box ticking compliance exercise. They can effectively act as roadmaps for you to identify and control the risks to rights and freedoms that using AI can pose. They are also an ideal opportunity for you to consider and demonstrate your accountability for the decisions you make in the design of AI systems. They can additionally help to explain to the public and potential clients how you have mitigated certain risks, which can help to build trust in your product and organisation.

3.22. If, during your risk assessment, you identify a risk that indicates a residual high risk to individuals that you cannot sufficiently reduce, you must consult with the ICO prior to starting the processing.

3.23. For more information on DPIAs, please see the guidance below:

- Data protection impact assessments;
- When do we need to do a DPIA?; and
- Examples of processing 'likely to result in high risk'.

Data Minimisation, Purpose Limitation, and 'Data Protection By Design and Default'

3.24. When processing personal data through your AI tool, it is crucial to adhere to the principles outlined in the UK GDPR, particularly Articles 5(1)(c) (data minimisation) and Article 5(1)(b) (purpose limitation).

3.25. Given that your tool supports financial advisors by streamlining workflows like note-taking, document generation, and CRM updates, it must be configured to capture only essential information necessary for these tasks, in line with Article 5(1)(c). For example, during real-time meeting note-taking, the tool should focus on capturing relevant discussions, while avoiding unnecessary or sensitive personal details. Similarly, when drafting suitability letters or updating CRM systems, the tool should only process the specific client data needed to achieve these purposes, ensuring no irrelevant or excessive data is collected.

3.26. Under Article 5(1)(b) of the UK GDPR, the principle of purpose limitation requires that personal data be collected for specified, explicit, and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. For your AI tool, this means that any personal data collected — such as client names, contact details, income, and derived information like financial vulnerabilities or risk appetite — must be used solely for its intended purposes, such as note-taking, drafting suitability letters, and updating CRM systems to support financial advisors. These purposes should be clearly defined and communicated to your financial organisation clients to ensure transparency.

3.27. It is critical to ensure that data processed for these specific tasks is not repurposed for unrelated activities. Further processing may only occur if it is compatible with the original purpose, as outlined under Article 6(4) of the UK GDPR, which considers factors such as the relationship between the original and new purpose, the context of data collection, and the safeguards in place.

3.28. For example, if the AI tool generates meeting notes to produce suitability letters, this data cannot be later reused to perform unrelated profiling without clear justification.

3.29. Under Article 25 of the UK GDPR, data protection by design and default requires that data protection is embedded into your AI tool's development and operation from the outset, ensuring that only necessary personal data is processed and appropriate safeguards are in place.

3.30. In the context of your AI tool, this means proactively designing features to protect personal data, for example, implementing role-based access controls, encrypting data in transit and at rest, and enabling financial advisors to review and edit AI-generated outputs before storage or sharing. By default, the tool should limit data collection to only what is strictly required for its core tasks – such as generating suitability letters, taking meeting notes, or updating CRM systems – while excluding unnecessary or sensitive details unless explicitly needed.

3.31. For more information, please see the guidance below on:

- Data minimisation;
- Purpose limitation; and
- Data protection by design and by default.

Data Retention

3.32. Under Article 5(1)(e) of the UK GDPR, personal data should not be kept for longer than necessary. Since your AI tool processes personal data for note-taking, document generation, and CRM updates, it is important to have clear rules about how long the data is stored. For example, meeting notes or drafts of suitability letters should only be kept as long as they are needed to complete their purpose. After that, the data should be securely deleted or made anonymous. CRM updates should be regularly checked to ensure outdated or incorrect information is removed or updated. Your tool could include features like automated deletion or anonymisation after a set period to make this process easier.

3.33. For more information about storage limitation please see the guidance below on:

- Storage limitation; and
- Self-assessment toolkit – records management checklist.

Data Accuracy

3.34. Under Article 5(1)(d) of the UK GDPR, organisations must ensure that personal data is accurate, up to date, and corrected without delay when inaccuracies are identified. Given that your AI tool generates notes, drafts documents such as suitability letters, and updates CRM systems, maintaining data accuracy is critical to avoid errors that could impact financial advice or client records. For example, real-time note-taking may inadvertently capture incorrect or irrelevant information, which, if transferred to the CRM or included in client reports, could lead to inaccurate financial recommendations or decisions. To mitigate this, the tool may include validation mechanisms and allow financial advisors to review, edit, and confirm AI outputs before they are finalised or stored.

3.35. Additionally, implementing audit trails may help track changes and ensure transparency in the data update process. Please refer to the ICO's guidance on accuracy for more information.

Data Security

3.36. To ensure compliance with Article 32 of the UK GDPR, your AI tool must implement robust technical and organisational measures to protect personal data processed for note-taking, document generation, and CRM updates.

3.37. Options to consider may include: 1) end-to-end encryption for data both in transit and at rest to ensure client information remains secure against unauthorised access; 2) implementing role-based access controls to restrict data access to authorised personnel and multi-factor authentication to enhance user verification; 3) maintaining audit trails and logging to monitor access and changes to personal data. Please refer to the ICO's guidance on data security for more information.