LK SHIELDS
YOUR LEGAL COUNSEL

DATA PROTECTION, PRIVACY AND SECURITY

AI and MiFID

by **David Naughton, Jane O'Grady, Katrina Smyth**

AI and MiFID

14th October 2024 | by David Naughton, Jane O'Grady, Katrina Smyth

Change is rapidly afoot in the financial services tech sector. How is AI transforming the landscape?

With the Artificial Intelligence Act and the widespread adoption of Artificial Intelligence, particularly Generative Artificial Intelligence, it is certainly having an impact.

Generative AI (Gen AI) tools use input training data and natural language processes to create and generate new data in the form of text, code, language or images and can provide insights such as risk scores or alerts, gaps or inconsistencies and future patterns. It can assist in mandatory reporting and compliance with the ever-increasing array of financial services laws and regulations and, for example, is being deployed by many firms to integrate sustainability preferences into investment and risk management processes.

This article examines ESMA's recent Public Statement, of 30 May 2024, on the use of Artificial Intelligence (AI) in the provision of retail investment services by MiFID investment firms (and credit institutions that provide investment services).

Background

While acknowledging the opportunities presented by the use of AI in terms of efficiency, innovation and improved decision-making, ESMA's Public Statement focuses on the adoption of AI in the provision of MiFID investment services and flags the widespread and currently divergent adoption of AI by firms across the EU and the resultant risks to retail investor protection.

The Statement outlines a number of potential use cases for AI by firms, including:

- customer service and support;
- provision of investment advice and portfolio management services;
- compliance with laws and regulations;
- risk management;
- fraud detection;
- and operational efficiency (including the use of third-party AI tools).

It aims to remind firms to comply with their MiFID II client safeguarding duties and to implement an appropriate governance framework around the use of AI tools (whether deployed with or without the direct knowledge and approval of senior management).

Inherent Risks

The Statement highlights the following key potential risks that may be inherent in the use of an AI tool: lack of oversight or human judgement; lack of transparency and explainability around the AI tool's decision-making processes; data privacy or security; and data input training bias or "hallucinations" leading to misleading advice or portfolio management.

Compliance with MiFID II

ESMA's guiding principles, in the use of AI tools by firms in the provision of MiFID investment services to

clients, can be summarised as follows:

1. There is an overarching requirement to act in clients' best interests and to provide information to clients on the firm's use(s) of AI in a clear, fair and not misleading way.
2. Oversight by the firm's management body is required to ensure alignment of the AI tool with its strategy, risk profile and compliance framework, including robust governance structures; monitoring and reporting procedures; and a clearly documented culture of risk ownership, transparency and accountability.
3. An effective risk management framework specific to AI (including regular testing) must be implemented to enable the firm to identify, assess and manage risks associated with AI investment decision-making, such as bias and data security.
4. Inputted data must be "relevant, sufficient and representative" and the training of algorithms must use accurate, comprehensive and sufficiently broad datasets, when used in investment decision-making (including where provided by third parties). Rigorous oversight of the creation, training, testing, validation and continuous analysis of data is required. Robust controls must ensure that accurate (ex-ante and post-ante) information is used by AI tools to avoid the distribution of inaccurate or misleading investment advice, with stringent oversight and comprehensive staff training.
5. Robust controls must align AI tools with product governance and suitability requirements, with rigorous quality assurance processes and testing of algorithms and their outcomes for accuracy, fairness and reliability in differing scenarios (including periodic stress testing).
6. Adequate due diligence must be conducted in the selection of third parties to provide critical and important functions; and sufficient outsourcing controls implemented.
7. Data protection requirements must be adhered to.
8. Thorough record-keeping on the use of AI (such as decision-making, data sources, algorithms, adjustments) and on client complaints is required.

The AI Act

The Statement has much in common with the requirements of the AI Act -- Regulation (EU) 2024/1689, which was signed into law on 13 June 2024, and entered into force on 1 August 2024.

The AI Act lays down harmonised rules on AI by following a risk-based approach. There are four risk categories:

1. unacceptable AI;
2. high risk;
3. limited risk; and
4. minimal risk.

The AI Act sets out specific requirements and obligations for relevant market actors that are placing AI systems and tools on the market or putting them into service or use in the European Union. The Act creates different legal obligations for AI providers and deployers.

AI providers are responsible for the market placement or service provision of a high-risk AI system or a Gen AI model, irrespective of whether the provider designed or developed the AI system. Deployers by contrast are individuals and entities that use AI in a professional context. As with the GDPR's definitions of "controller" and "processor", the classification of an entity as a "provider" or "deployer" for AI regulation will be determined by factual circumstances; parties will not be free to agree their status by contract. Under the AI Act, both providers and deployers are subject to clear requirements and obligations regarding specific uses of AI, including requirements around transparency, technical documentation and record-keeping of AI systems, as well as adherence to the principles of transparency, privacy and data governance. Key obligations arising under the AI Act will be implemented from February 2025 over 24 months, with all obligations to be fully phased in over a 36-month period. Initially, unacceptable AI will be prohibited and thereafter, from August 2025, rules on Gen AI will start to apply as will provisions around the legislation's governance framework and Member State penalties.

Utilising AI – Thoughts

The adoption of Gen AI undoubtedly has the capacity to produce many benefits, such as more efficient and

higher-quality portfolio construction; better management of risk; safeguarding of investors; innovation in asset classes; democratisation of access to data; diversification in talent/skills acquisition within firms; and augmented cyber security.

But AI providers and deployers must be aware of the potential risks and how to mitigate those risks. The ability to move quickly to adapt in the rapidly changing sphere of AI and its regulation is essential. While off-the-shelf AI models may be very good, responsibility for ultimate decision-making and judgement must remain with humans, as a principle of the AI Act is that AI use in the EU must be human-centric, trustworthy and protect fundamental rights. Firms should focus on their governance and risk management frameworks; explainability and transparency around how and why AI systems are used, including decision-making using AI; staff training; the identification and removal of bias or hallucinations; and future-proofing any contracts for the provision of AI tools.

The AI Act expressly states that it does not seek to regulate the application of data protection law. As AI systems and models often involve processing large volumes of personal data, it is important to remain complaint with data protection obligations when using personal information, including establishing a clear legal basis to process personal data. Additionally, a data protection assessment should include the rationale for the use of AI and the identification and mitigation of any risks to data subjects.

Next Steps

If you require our assistance in implementing any of these measures, please contact David Naughton dnaughton@lkshields.ie or Katrina Smyth ksmyth@lkshields.ie (in our Financial Services team) or Jane O'Grady jogrady@lkshields.ie (in our Technology and Innovation team).

About the Authors

David Naughton
Partner

David Naughton is Head of Financial Services.
T: +353 1 637 1585 **E:** dnaughton@lkshields.ie

Jane O'Grady
Partner

Jane is dual qualified as a solicitor and a trade mark and design attorney, with many years' experience advising on commercial contracts, intellectual property, commercial agency and all aspects of technology law.
T: +353 1 637 1554 **E:** jogrady@lkshields.ie

Katrina Smyth
Senior Associate

Katrina is an experienced financial services solicitor specialising in Investment Funds and Asset Management.
T: +353 16371548 **E:** ksmyth@lkshields.ie