GOODWIN

ALERT · AUGUST 9, 2024

EU AI Act: Key Points for Financial Services Businesses

BY Andrew Henderson Gretchen Scott Céline Moille Matthew Dixon-Ward Adelina Popescu

The European Union (EU) Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), came into force on 1 August 2024. As noted in our alert "AI Act Published — What's Next?," there is a two-year implementation period, with most of the obligations under the AI Act coming into force on **2 August 2026**.

In the EU context, the AI Act, which applies to all types of institutions, gives rise to some key questions for any business that is one of the following:

- An EU bank or nonbank lender, broker-dealer, insurer or insurance broker, investment manager, or adviser, especially one that uses innovative technology as a key part of its business (financial services entity)
- A third-party institution, including one located outside the European Union, that is not a financial services entity but provides services to a financial services entity (unregulated service providers)

Although some unregulated service providers, including those outside the European Union, will become directly subject to EU financial services law in the form of the Digital Operational Resilience Act (DORA) — see our most recent alert, ESA Publications on Digital Operational Resilience: A Reminder That DORA is Less Than Six Months Away and Will Apply to US and UK CTPPs," for more — the AI Act is not limited to providers of AI services to EU financial services entities designated as "critical" third-party service providers under DORA.

What Is the AI Act?

We have written more generally on the AI Act, including in our general overview (Series 1 - The World's First AI Regulation Is Here). The AI Act implements a "uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems."

How Will the Obligations in the AI Act Be Enforced Against Financial Services Entities?

As an EU regulation, instead of an EU directive, the EU Act will apply to directly to financial services entities and service

providers without the need for EU member state law to give effect to its provisions.

That said, the AI Act expressly points to existing EU financial services laws, including directives that contain the internal governance and risk management requirements for financial services entities. Noting that governance and risk management are central to AI Act compliance, the existing requirements in EU financial services laws will be expected to apply to financial services entities when they make use of AI systems. In this context, the AI Act states that the current EU authorities that supervise and enforce EU financial services law should be designated to supervise implementation of the AI Act, including for market surveillance activities, and have all the powers under the AI Act with respect to financial services entities.

Enforcement under the AI Act will therefore fall to the financial services authorities of member states and the European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA), collectively known as the European Supervisory Authorities (ESAs). Even before the AI Act, the ESAs had put out guidance on AI matters. See, for example, the EBA's follow-up report on the use of machine learning for internal ratings-based models, EIOPA's artificial intelligence governance principles, and ESMA's public statement on using AI in retail investment services.

Does the AI Act Cover All Financial Services?

The AI Act expressly refers to the EU laws that govern the prudential requirements for credit institutions and investment firms, consumer credit, mortgages, the solvency requirements for insurance companies, and insurance distribution. This leaves the impression that its focus is on the business of banks, lenders, investment banks and broker-dealers, and insurance companies and brokers. However, it does refer to "other types of financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services law." Noting the discussion of the AI Act in ESMA's public statement, it would be surprising if ESMA — charged with regulating investment, fund managers and advisers, and investment banks and broker-dealers — and the competent authorities of EU member states did not impose the same requirements as those under the AI Act, albeit in a proportionate way, on all the firms they regulate. In this respect, the aim stated in Recital 158 of the AI Act, "to ensure consistency and equal treatment in the financial sector," should be noted.

What Is the Territorial Scope of the AI Act?

The AI Act broadly applies to entities to which at least one of the following apply:

- Are located or established in the European Union and use AI systems for business purposes
- Supply AI systems to the EU market (regardless of where they are established)
- Use AI systems for business purposes if the output of the AI system is used within the European Union (even where the entity in question is located or established outside of the European Union)

This gives the AI Act a broad extraterritorial application similar to other general EU laws, such as the General Data Protection Regulation (GDPR) and DORA. This broad application will be especially relevant for unregulated service providers that are located outside the European Union, with the obligations under the AI Act having to be considered alongside those under DORA where the provider of an AI system is considered to be "critical". The AI Act will also have to be considered when a non-EU financial services entity supplies AI systems to an affiliate that is an EU financial services entity.

Non-EU financial services entities will also have to consider how the AI Act applies when providing services to EU customers; they already must do so in the context of the territorial scope of financial services directives and regulations, such as the Credit Requirements Directive and Markets in Financial Instruments Directive. The AI Act's territorial scope provisions, with their broad extraterritorial application, is more closely aligned with that of the GDPR. However, given the AI Act's reference to financial services directives and regulations as "entry points" for financial services entities, the extent to which non-EU financial services entities will have to comply with the AI Act will likely have to be approached on a case-by-case basis.

What Activities Will Be in the Scope of the AI Act?

The AI Act officially defines an AI system as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”

AI systems falling within the above definition will be categorised according to certain risk categories, namely unacceptable, high, limited, or minimal or no risk. In addition to this, the AI Act treats general-purpose AI as its own risk category.

For an AI system designated as minimal or no risk, the AI Act does not provide any mandatory obligations. However, voluntary subscription to relevant codes of conduct are encouraged, and all providers and deployers are required to ensure their staff have adequate levels of AI literacy.

Prohibited AI Systems in Financial Services (Unacceptable Risk)

Article 5 of the AI Act sets out certain prohibited AI systems. Of these, financial services entities should be particularly aware of the prohibition against AI systems that do any of the following:

- Evaluate or classify natural persons based on their social behaviour or personal characteristics to create a “social score” leading to detrimental or unfavourable treatment
- Create or expand facial recognition databases through untargeted scraping of facial images from the internet or closed-circuit TV footage
- Deploy subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques to materially distort the behaviour of a person or group of persons by appreciably impairing their ability to make an informed decision

The prohibition of AI systems deemed to represent an unacceptable risk will come into effect on 1 February 2025.

What About High-Risk AI Systems?

An AI system will be deemed “high risk” if it is either:

- Subject to certain EU-specified product safety legislation listed in Annex I of the act and required to undergo a third-party conformity assessment before being placed on the EU market
- Specified as high risk pursuant to Annex III of the AI Act

The first is not expected to have an effect on financial services entities, but Annex III of the AI Act includes several AI systems that may be relevant to financial institutions and fintech businesses, including AI systems intended to be used for:

- Evaluating the creditworthiness of natural persons or establishing their credit score, with the exception of AI systems used for the purpose of detecting financial fraud
- Risk assessment and pricing in relation to natural persons in the case of life and health insurance
- Recruitment or selection of natural persons, in particular to place targeted job advertisements, analyse and filter job applications, and evaluate candidates
- Making decisions affecting terms of work-related relationships, for the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics, or to monitor and evaluate the performance and behaviour of persons in such relationships

It is possible to rebut the presumption of high risk for any AI system that falls within Annex III by establishing that the AI system

does not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons. This assessment must be documented and provided to national authorities upon request. The provider must still register the AI system in the EU database of high-risk AI systems, even if it has concluded there is no significant risk of harm. The AI Act provides some examples of AI systems that are not considered high risk, such as those that perform narrow procedural tasks, improve previous human activity, detect decision-making patterns or deviations from prior decision-making patterns, or perform preparatory tasks for an assessment relevant for the purposes of the Annex III high-risk use cases (e.g., AI systems used for translation of initial documents). However, the exception cannot be relied on if the AI system performs the profiling of natural persons because profiling by high-risk AI systems is considered to bring significant risk of harm.

For further guidance on whether your AI system will be considered high risk, please see our interactive tool and other AI Act alerts.

What Are the Expectations for Providers of High-Risk AI Systems?

Providers of high-risk AI systems must comply with an extensive list of obligations before, during, and after launching their AI. These requirements are designed to encourage safe and trustworthy AI. They include maintaining comprehensive technical documentation and systems for risk and quality management throughout the AI system's life cycle, using quality datasets, facilitating transparency, and ensuring systems allow for automatic event recording for traceability and monitoring.

High-risk AI systems must pass a conformity assessment before being placed on the EU market, as evidenced by "CE" marking, which indicates that the AI system represents compliance with EU legal standards.

Deployers of high-risk AI systems are subject to obligations that recognise the risks arising from their use of such AI systems and the need to monitor performance as they operate in a live environment. Deployers' obligations include complying with providers' instructions for use and ensuring that the input data are transparent and suitable for the AI system's intended purpose.

All participants in the AI deployment chain are subject to monitoring and reporting obligations with respect to risks presented by high-risk AI systems.

How Does the AI Act Address Specific Obligations for Financial Services Entities?

The AI Act seeks to address the potential overlap between some of its requirements and existing requirements that the EU financial services law imposes on financial services entities. It integrates certain procedural obligations governing risk management, post-marketing monitoring, and documentation for existing obligations under EU financial services laws with existing EU financial services law. To ensure consistency and equal treatment in financial services, financial services entities providing or deploying high-risk AI systems also benefit from limited derogations both for quality management systems and for monitoring obligations to reflect existing rules regarding internal governance arrangements under EU financial services law.

How Will Financial Services Entities Be Expected to Respond to the AI Act?

As noted above, the AI Act points to existing internal governance and risk management requirements for financial services entities. It is through compliance with these requirements, adapted to the use of AI systems, that financial services entities will be expected to comply with the AI Act. The European Commission's consultation document " Targeted Consultation on Artificial Intelligence in the Financial Services" (the consultation) — response window for which closes on 13 September 2024 — serves as a useful list of questions for financial services entities to consider when thinking about AI Act implementation. These are in addition to the broader questions that a financial services entity should consider when looking to implement a new law or regulation, especially those relating to operational resilience, which financial services entities should examine in the context of DORA and are noted in our recent alert "ESA Publications on Digital Operational Resilience: A Reminder That DORA is Less

Than Six Months Away and Will Apply to US and UK CTPPs."

These are some of the questions from the consultation that give an idea of the issues for financial services entities to consider:

- Are you using or planning to use AI systems?
- Will you deploy AI for new or additional processes within your organisation?
- Are you developing or planning to develop in-house AI applications?
- If not, please explain broadly with whom you plan to collaborate for the development of your AI applications (fintech, big tech, etc.) or whether you plan to buy fully developed solutions.
- Which tools are you using to develop your AI applications? Examples include machine learning, neural networks, natural-language processing, large language models, etc.
- Please rank the potential negative impact that widespread use of AI can have on the following risks in your business: operational, market, liquidity, financial stability, market integrity, investor protection, consumer protection, and reputational.

What Is the Timetable for Implementation of the AI Act?

Please see our timeline.

What Is the Timetable for Implementation of the AI Act?

As we have argued before (and most recently in "The FCA's AI Update: Integrating The UK Government's 5 Principles "), it is not clear that AI necessarily creates material new risks for financial services, although this may change. Instead, AI may amplify and accelerate the existing financial services risks — i.e., those connected with financial stability, consumer, and market integrity — which the financial services and markets regime is designed to reduce.

The AI Act represents a significant step in the regulation of AI in Europe, with substantial implications for financial services entities, especially fintechs, and for unregulated service providers.
While the AI Act imposes stringent requirements, it also offers opportunities to build trust, protect consumers, and foster innovation in financial services.

While it is likely that financial services entities will need to invest in resources to ensure compliance with the AI Act, those that succeed can gain a competitive edge and improved access to the European market.

To discuss the contents of this alert, please contact the authors or your usual Goodwin contact.

CONTACTS

Andrew Henderson
Partner

andrewhenderson@goodwinlaw.com
London | +44 (0)20 7667 3628

Gretchen Scott
Partner

gscott@goodwinlaw.com
London | +44 (0)20 7447 4292

GOODWIN

Céline Moille
Counsel

cmoille@goodwinlaw.com
Luxembourg | +352 27 86 67 58
Paris | +33 1 85 65 71 71

Matthew Dixon-Ward
Associate

mdixonward@goodwinlaw.com
London | +44 (0)20 7667 3086

Adelina Popescu
Associate

apopescu@goodwinlaw.com
Luxembourg | +352 27 86 67 56