SQUIRE PATTON BOGGS

The EU AI Act and Respective Regulation of Financial Services

EU – March 2025

The EU Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689, came into force on 1 August 2024. As outlined in my previous article headlined EU AI Act Proposal and Regulation of Financial Services, the AI Act has a two-year implementation period, while most of the rules and obligations under the AI Act will be enacted after 2 August 2026.

Since the AI Act is an EU regulation, it will directly apply to EU seated financial service entities and service providers without requiring any implementation through national laws of the EU member states. Ultimately, the AI Act will restrict the deployment of certain classes of artificial intelligence systems (AI Systems) and will regulate their use, provision, import and distribution. The definition of AI Systems can be found in Article 3(1) of the AI Act;

"'AI system' means 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."

The list of AI techniques and approaches provided in the Annex of the AI Act includes machine learning methods, logic- and knowledge-based methods, statistical methods and estimations, as well as search and optimisation techniques. The EU Commission will have the authority to revise the attached list of methods and techniques to align it with developments in technology and the market. However, users, as well as importers and distributors of third-party software, and companies that commission or modify third-party software, may lack adequate information to ascertain whether the software was created using the techniques or approaches mentioned. Regardless, it appears probable that new software will make greater use of methods and strategies linked to acknowledged AI technologies. Consequently, companies might need to consider whether their software could potentially be included in the definition, and therefore routinely study the provisions of the AI Act to determine whether software is prohibited or might be subject to regulation.

Impact of the AI Act

The AI Act applies to all instances of introducing AI systems to the EU market, deploying these systems and utilising them, irrespective of the industry. As a result, the AI Act is not aimed specifically at the financial services sector; nevertheless, it will apply to AI systems introduced into the financial market or utilised there.

Financial institutions will have an obligation as a "user" of an AI system when the software is integrated into the institution's own systems (regardless of whether the software is proprietary or licensed from a third-party). Financial institutions must also consider whether they have duties as a user if they depend on or utilise the systems of third-parties, including affiliated companies, clients, vendors or market infrastructure. The AI Act does not specify how to ascertain when third-party software is utilised under an institution's authority, leading to the firm being classified as a user.

Financial institutions might also have responsibilities as a "provider" of an AI system utilised by the financial institutions. This can arise from various factors, including: the software being developed internally; the financial institutions commissioning it from an external provider; the financial institutions altering or adapting a third-party software; or the financial institution using third-party software, while operating under its own name or trademark. Further, the financial institution can be seen as a provider of an AI system utilised by other group companies or third-parties, for instance, if the company created the software or commissioned it through external parties. A financial institution may find it challenging to meet all the legal obligations placed on it as a provider. As a result, it will need to evaluate how much it can depend on contractual agreements with developers or other third-parties to ensure compliance with the AI Act.

Moreover, financial institutions based in the EU could have responsibilities as "importers" of a high-risk AI system they utilise when they deploy the software under the name or trademark of a non-EU firm or individual. When the financial institution provides a high-risk AI system, further obligations may come into effect if external parties use the software, as the financial institution may then be regarded as a "distributor" of the system.

Therefore, as users, suppliers, importers or distributors of a single AI system, several institutions in a financial sector group may be liable under the AI Act. Under inter-affiliate service agreements or other contracts, numerous group companies may take part in the software purchase, development, management and use. Where appropriate, they may also make the software available to other group companies, clients or suppliers (possibly under a common group brand name or trademark). Given the AI Act's extraterritorial application, this could make it challenging to determine which group companies are subject to obligations under the act.

Notably, there are cases where the AI Act imposes specific obligations for providers or deployers in the financial services sector:

- According to EU financial services law, financial institutions that offer AI systems are already bound by rules pertaining to their internal governance, arrangements or procedures when it comes to the quality management system. Therefore, they can adhere to the rules on internal governance arrangements, or processes in accordance with the applicable EU financial services law (Article 17(4) of the AI Act) and meet the requirement to adopt a quality management system. The regulations pertaining to credit institutions and investment firms, consumer credit (including mortgages), insurance and reinsurance, as well as insurance distribution are all included in EU financial services law for the purposes of this framework. However, they are still required to implement the risk management system referred to in Article 9 of the AI Act, a post-market monitoring system in accordance with Article 72 of the AI Act, and a serious incident reporting procedure pursuant to Article 73 of the AI Act (see also Recitals 65, 81 and 155).
- Financial institutions may preserve technical documentation as part of the documentation maintained in accordance with the applicable EU financial services law (Article 18(3) of the AI Act) according to the same principle. The same reasoning holds true for automatically generated logs, which financial institutions may keep as part of the records required by the applicable financial services law (Article 19(2) of the AI Act) and produced by their high-risk AI systems (see also Recital 81).
- When financial institutions act as deployers, they can fulfil the monitoring obligation by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service law (Article 26(5) of the AI Act), as well as maintain their logs as part of the documentation kept pursuant to the relevant Union financial service law (Article 26(6) of the AI Act) (see also Recitals 91 et seqq.).

Territorial Scope of the AI Act

The AI Act has a wide territorial scope and applies to entities that meet at least one of the following conditions:

- The financial institution is a deployer who is established or located within the EU, and utilise AI systems for business purposes.
- The financial institution is a provider who makes AI systems available on the EU market, irrespective of their location.
- The financial institution is a provider or deployer who employs AI systems for business purposes, provided that the system's output is used within the EU even if the organisation itself is based outside the EU.

Due to these criteria, the AI Act has significant extraterritorial reach, like overarching EU regulations such as the General Data Protection Regulation (GDPR) and the Digital Operational Resilience Act (DORA). This broad applicability is particularly relevant for non-EU AI service providers that are not otherwise regulated, as they must ensure compliance with the AI Act alongside DORA when an AI system is classified as "critical."

Additionally, financial service providers based outside the EU that supply AI systems to affiliated companies within the EU will also need to consider the implications of the AI Act. Furthermore, non-EU financial institutions offering services to EU customers must assess how the AI Act applies to their operations. This mirrors the approach taken in financial regulations such as the Capital Requirements Directive (CRD) and the Markets in Financial Instruments Directive (MiFID).

However, since the AI Act identifies financial directives and regulations as key "entry points" for financial institutions, the extent to which non-EU financial service providers must adhere to it will likely require case-by-case analysis.

Overall, financial groups with headquarters in the EU may be especially affected by the AI Act's extraterritorial application. The results of risk-management, or regulatory capital processes and credit assessment software implemented by the group's non-EU subsidiaries, are probably going to be used in the EU head office. As a result, the AI Act may apply to those non-EU subsidiaries and to non-EU group, as well as non-group companies that are treated as providing that software, at least if any of the individuals affected by the use are in the EU. Groups not headquartered in the EU may be able to restrict the use of software output from outside the EU within the EU, but the AI Act will still apply to non-EU entities within those groups if they are considered to provide software for their EU subsidiaries. Even if some other nations were to eventually adopt the EU's strategy of regulating software in this manner the AI Act does not provide any relief about software supplied or utilised by non-EU entities subject to comparable third-country regulatory requirements. Although there are some US legislative initiatives on automated decision-making and facial recognition, as well as numerous initiatives offering guidance, principles or voluntary international technical standards that the private sector may apply, the Commission impact assessment points out that no other nation has implemented a comparable regulatory framework for AI. Notably, the AI Act will provide a uniform set of legally binding regulations that all types of financial institutions including those outside the EU must follow, regardless of whether they adhere to other laws or norms.

General Scope of the AI Act

AI systems that meet the definition as set out in Article 3(1) of the AI Act (see also Recital 12) will be categorised based on their implied risk level. The categories include prohibited, high-risk, limited risk or minimal/no risk. Moreover, the AI Act designates general-purpose AI as a separate risk category. The AI Act does not impose any mandatory regulatory requirements on AI systems categorised as minimal or no risk. It is recommended that providers and deployers voluntarily subscribe to applicable codes of conduct, and they must guarantee that their employees possess sufficient knowledge and understanding of AI.

In the context of the financial sector, AI systems that evaluate a customer's credit score or creditworthiness should be classified as high-risk AI systems, as stated in Recital 58 of the AI Act. The reason for this is that they determine whether those clients can access financial resources or essential services such as housing, electricity and telecommunications. Furthermore, AI systems that are meant to be used for risk assessment and pricing in relation to clients for health and life insurance can also have a big impact on people's lives. If they are not properly designed, developed and used, they can violate people's fundamental rights and have major negative effects on people's lives and health, such as discrimination and financial exclusion. Thus, these AI systems are also regarded as high-risk.

However, AI systems that are allowed under EU law to identify fraud in financial services, and to prudently establish the capital requirements for credit institutions and insurance undertakings should not be classified as high-risk.

Prohibited AI Practices in the Financial Service Market

The AI Act will prohibit financial service entities from placing on the market, putting into service or using an AI system pursuant to Article 5(1)(a) of the AI Act:

"the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;"

The prohibition of AI systems deemed to represent an unacceptable risk and officially came into force on 1 February 2025.

While these prohibitions are relatively limited in scope, there are already calls to broaden some of them to include private sector firms, such as the restrictions on specific applications of facial recognition techniques in public spaces that currently apply only to public authorities and law enforcement bodies. Certain AI systems that are prohibited are specified in Article 5 of the AI Act (see also Recitals 29 et seqq.). Among these, financial services entities should pay special attention to the ban on AI systems that perform any of the following actions:

- Evaluate or classify natural persons based on their social behaviour, or known, inferred or predicted personal, or personality characteristics to create a social score that leads to detrimental or unfavourable treatment.
- Create facial recognition databases by untargeted scraping of facial images from the internet or television.

High-risk AI Systems

In principle, the AI Act will primarily regulate the use, provision, importation or distribution of high-risk AI systems. This covers certain software used as safety components in physical products, or by operators of critical infrastructure, as well as educational or vocational training institutions, public authorities and law enforcement. Article 6(1) of the AI Act (see also Recitals 46 et seqq., 50 et seqq.) defines what such high-risk AI systems are:

"Irrespective of whether an AI system is placed on the market, or put into service independently of the products referred to in points (a) and (b), that AI system shall be high-risk where both of the following conditions are fulfilled:

(a) The AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the EU harmonisation legislation listed in Annex I;

(b) The product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the EU harmonisation legislation listed in Annex I"

While Annex I is not expected to have an impact on financial services entities, Annex III of the AI Act identifies several AI systems that may be particularly relevant to financial institutions and FinTech companies. Such high-risk AI systems pursuant to Article 6(2) of the AI Act are the AI systems listed in any of the following areas:

"4. Employment workers' management and access to self-employment:

(a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates

(b) AI systems intended to be used to make decisions affecting terms of work-related relationships, 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

5. Access to and enjoyment of essential private services and essential public services and benefits:

[…]

(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud;

(c) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance; […]."

It has to be noted that according to Art. 6(3) of the AI Act, an AI system referred to in Annex III shall not be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including but not materially influencing the outcome of decision making. The AI Act specifies use cases where no significant risk of harm is assumed. These include narrow procedural tasks, enhancing human-generated results, identifying decision patterns or deviations without altering prior human assessments, and performing preparatory tasks for Annex III use cases. Documentation of this assessment is required, and it must be provided to national authorities when requested. Even if the provider determines that there is no significant risk of harm, they must still register the AI system in the EU database of high-risk AI systems. Furthermore, for the exemption to apply, at least one of the following conditions must be met:

- The AI system is designed to carry out a narrow procedural task.
- The AI system aims to enhance the outcome of an activity performed by a human in advance.
- The AI system aims to identify patterns or anomalies in decision-making compared to previous patterns, and is not intended to replace or affect the human evaluation that has been conducted previously, without appropriate human review.
- The AI system is designed to execute a preparatory action related to an assessment pertinent to the use cases described in Annex III.

Nevertheless, the AI Act clarifies that the exceptions are not appliable, if the AI system performs the profiling of natural persons because that shall always be high-risk. Providers or deployers of those high-risk AI systems in the financial sector are therefore subject to the stricter rules imposed on such high-risk AI systems.

The EU Commission will be empowered to broaden the definitions of these classes to include additional types of software. Biometric identification software classified as high-risk may be restricted to those that involve remote biometric identification, which is defined as "the identification of natural persons at a distance by comparing an individual's biometric information with the biometric information in a reference database, without prior knowledge whether the targeted individual will be present and can be identified". It remains uncertain whether biometric authentication software, including fingerprint or facial recognition tools used for verifying customer identity and granting account access, as well as allowing staff entry to company premises or computer systems, will be treated as falling within this class.

Given the current definition of AI systems, it may be challenging to ascertain when software utilised for human capital management or individual credit assessment is classified as high-risk. This class could encompass nearly any software (such as spreadsheets or databases) utilised for managing recruitment, recording and retrieving employee data, conducting appraisals, reviewing salaries and bonuses or promotions, allocating holidays, tracking time or assigning tasks as part of work management. The category of credit assessment software is restricted to those used to evaluate access to "essential private services". However, this encompasses tools utilised for assessing access to financial resources, including banking, insurance and other financial services. It might also be challenging to define the range of software that regulations will apply to, for example, where software used for credit assessment of individuals is integrated with the firm's pricing or risk management systems.

Providers of High-risk AI Systems

Before, during and after the launch of AI systems, providers of high-risk AI systems must adhere to a comprehensive set of obligations. The purpose of these requirements is to promote safe and reliable AI systems. Providers must maintain comprehensive technical documentation, implement effective risk and quality management systems during the AI system's life cycle, utilise quality datasets, promote transparency and guaranteeing that systems enable automatic event recording for traceability and monitoring purposes.

Therefore, before being introduced to the EU market, high-risk AI systems must undergo a conformity assessment. The presence of the "CE" marking will confirm that the system complies with EU legal requirements.

Deployers of high-risk AI systems must recognise the potential risks associated with their use and monitor the systems while they operate in real-world conditions. They are also obligated to adhere to the provider's instructions for use, ensuring that the input data is both transparent and suitable for the intended purpose of the AI system.

Ultimately, all parties must monitor and report obligations to address the risks posed by high-risk AI systems.

Application of the AI Act

The AI Act will not apply to high-risk AI systems that are placed on the market, or put into service before the date of application of the AI Act unless they are subsequently subject to significant changes in their design or intended purpose. However, users and providers may need to comply with the transparency obligations under the AI Act in relation to existing software, and the prohibitions on the deployment of existing prohibited AI systems that will apply from the date of the application of the AI Act.

Unless it is already evident, providers of an AI system meant to engage with natural persons must ensure that the system is designed or developed in a way that makes natural persons aware that they are interacting with an AI system. This encompasses chatbots, as well as a variety of other software applications where natural persons engage with the software in any manner (for example by entering data or retrieving content).
Users of AI systems designed for emotion recognition or biometric categorisation must notify natural persons exposed to these systems about their functioning. People who use AI systems to create or alter "deep fakes" must reveal that the content is not genuine and has been artificially created or modified. These duties will also apply to high-risk AI systems that have the described characteristics.

Therefore, the AI Act aims to resolve any potential overlap between some of its requirements and existing requirements set out by the EU financial services law for financial services entities. It incorporates certain obligations, such as risk management, monitoring and documentation for existing obligations under EU financial services laws. To guarantee uniformity and equal treatment in the EU financial services industry, entities that offer or utilise high-risk AI systems are afforded limited exceptions concerning quality management and monitoring obligations in line with the current regulations on internal governance arrangements according to EU financial services law. These exceptions are aligned with the current regulations on internal governance requirements set by EU financial services law.

Ultimately, financial service entities need to comply with the AI Act and firms should start to apply the rules internally. This may involve a preliminary assessment to determine where the AI Act might impose obligations on the financial institution and other members of its group, as well as how compliance might be achieved. Overall, any financial institution will also have to consider how the new regulations will relate to other current and planned sectoral and cross-sectoral regulatory obligations, including those under MiCAR, DORA and GDPR.

The AI Act also addresses the existing internal governance and risk management requirements for financial services entities, and they will be expected to comply with the AI Act. These are supplementary to the wider issues a financial services entity should contemplate when aiming to apply a new law or regulation, particularly those concerning operational resilience – these should be reviewed by financial services entities within the framework of DORA and other national rules and regulations.

For instance, the following questions need to be considered:

- Are you developing or planning to develop in-house AI applications?
- Are you planning to collaborate for the development of your AI applications with third-parties, or buying fully developed solutions?
- Which tools do you utilise for the development of your new AI applications?
- Are you using external AI systems?
- Do you evaluate the potential adverse effects of the AI use on the risks associated with your business?

Regardless of the circumstances, the magnitude of the possible sanctions indicates that it should be a top priority for boards to establish AI governance and ensure compliance.

Enforcement under the AI Act

The European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA), together known as the European Supervisory Authorities (ESAs), will thus be responsible for enforcing the AI Act in conjunction with the financial services authorities of the EU member states. The ESAs had issued guidance on AI issues even prior to the AI Act. Take, for instance, ESMA's public statement on the use of AI in retail investment services, EIOPA's AI governance principles and the EBA's follow-up report on the use of machine learning for internal ratings-based models.

The AI Act marks a major advancement in the regulation of AI across the EU, carrying considerable consequences for financial services organisations – particularly Fintechs – and for service providers operating without regulation. The AI Act, while imposing strict requirements, also provides opportunities to establish trust, safeguard consumers and promote innovation in financial services. Although it is probable that financial services organisations will have to allocate resources to meet the requirements of the AI Act, those that manage to do so can benefit from a competitive advantage and enhanced access to the EU market.

Contact

Dr. Andreas Fillmann
Partner, Frankfurt
T +49 69 17392 423
E andreas.fillmann@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

squirepattonboggs.com

© Squire Patton Boggs. All Rights Reserved 2025

67896/03/25