Can We Rule the Machines? A deep dive into the EU AI Act

EU AI Act: A Milestone in Artificial Intelligence Regulation

On August 1, 2024, **the European Union's Artificial Intelligence Act (EU AI Act)** officially came into force, signalling the arrival of **the world's first comprehensive AI regulation**. While most of its provisions will become mandatory only in August 2026, **certain rules - particularly those banning prohibited AI practices - take effect in February 2025**. This makes now the perfect time to examine the purpose and key elements of the AI Act, plus what it means for the financial sector and technology providers offering AI-powered business solutions.

Due to the breadth and complexity of the EU AI Act, **we've split this topic into two parts**. **In this first article, we'll explore the Act's core objectives, its territorial scope,** and its implementation **timeline**, together with key milestones. We'll also examine **the broader regulatory landscape**, comparing the EU's approach to AI governance with those of other major economies. **In our next blogpost**, we'll dive into **the key elements** of the AI Act and outline **the most critical requirements for banks, financial service providers, and their suppliers**, as well as **the essential steps they need to take to ensure compliance**.

The Core Objectives of the AI Act

At its heart, **the AI Act aims to create a harmonised legal framework across the EU that both nurtures innovation and safeguards our fundamental values**. In an era where rapid AI development presents unprecedented challenges - not only for sectors like finance but for all industries - **the regulation provides clear, risk-based criteria to address concerns** such as algorithmic bias, opacity, and data misuse. As the first law of its kind, it sets a global benchmark by balancing stringent protections for health, safety, and individual rights with measures designed to stimulate technological progress and economic growth. Its horizontal approach ensures that these **rules apply uniformly across all sectors and Member States**, offering legal certainty and **paving the way for a trusted, human-centric AI ecosystem** that underpins a competitive, integrated internal market.

International AI Regulatory Landscape

The EU AI Act is the most comprehensive legal framework for artificial intelligence to date, but it is not the only regulatory effort worldwide. Other major economies have also recognised the need for AI governance, though their approaches vary significantly.

In the United States, there is currently no overarching federal AI regulation, however agencies such as the Federal Trade Commission (FTC) have issued guidelines on ethical AI use. Donald Trump's return to office marked significant changes in U.S. artificial intelligence (AI) regulation. After taking office, **President Trump revoked the executive order signed by Joe Biden in 2023, which aimed to ensure the safe and ethical governance of AI development. In his new executive order, Trump emphasised promoting innovation and strengthening U.S. technological leadership in the AI field**. As part of this approach, he announced the "Stargate" infrastructure project, a $500 billion initiative designed to enhance the country's AI infrastructure and solidify its leadership in the global tech race.

China, in contrast, has implemented a state-controlled regulatory framework, embedding AI governance into broader national strategies like the **New Generation Artificial Intelligence Development Plan.** The goal of this plan is for China to take a leading role in the development and application of artificial intelligence by 2030. The country **focuses on balancing rapid AI development with strict government oversight**.

Meanwhile, **Japan has adopted an ethics-based approach** under its Society 5.0 initiative, **promoting AI to enhance human-centric innovation** while aligning with global best practices. Japan is currently working on comprehensive AI legislation, which is expected to come into effect in 2025.

In 2022, **Canada introduced the Artificial Intelligence and Data Act (AIDA), aiming to ensure the safe and responsible use of AI systems**. The AIDA focuses on regulating high-risk AI systems, minimising individual and collective harms, and enhancing transparency and accountability. **Canada, one of the early adopters of AI regulation, continues to refine its Pan-Canadian AI Strategy with a focus on responsible AI governance and international harmonization.**

Despite the variety of national strategies, **international coordination on AI regulation remains a significant challenge. However, global organisations are working to create alignment.** The OECD's AI Principles and UNESCO's AI Ethics recommendations are being adopted by various countries to establish common ground. Additionally, the G7 nations are actively engaged in discussions to develop shared regulatory approaches, while UNESCO, ISO, and other international bodies continue to work on building comprehensive AI regulatory frameworks.
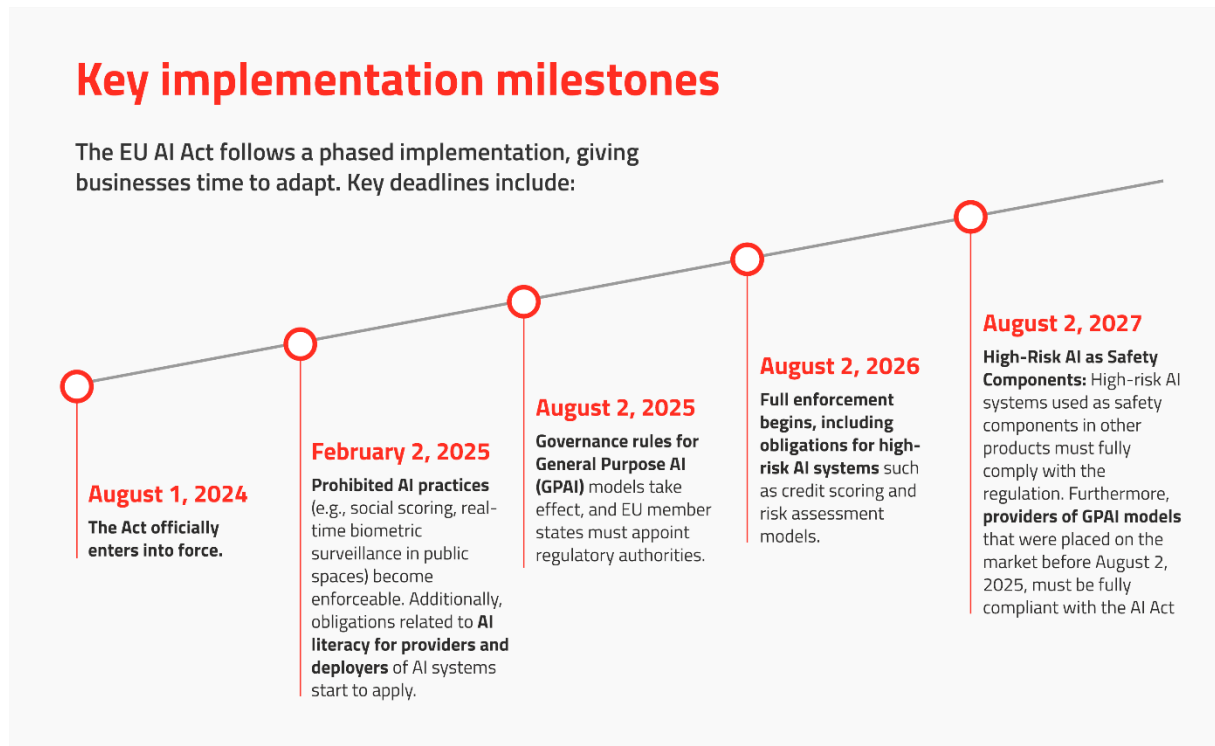
These efforts highlight the **increasing recognition of the need for global collaboration in AI governance. Common principles such as transparency, accountability, and the mitigation of bias** are emerging as universal priorities. However, significant political and economic differences continue to impede the development of a unified global regulatory framework. **For financial institutions and technology providers operating across multiple markets, this fragmented landscape creates a complex web of compliance requirements, forcing them to stay vigilant as global standards evolve.**

To achieve synergy in AI regulation, it is essential to harmonise key areas such as data privacy, algorithmic transparency, and ethical AI use. **Establishing international standards** for AI safety, fairness, and accountability can help **mitigate risks and ensure that AI technologies benefit society as a whole. Enhanced cooperation** between countries and international bodies **is crucial to address these challenges and create a cohesive global regulatory environment.**

Territorial Scope of the AI Act

The EU AI Act has a broad territorial scope, like the GDPR. It applies not only to companies operating within the EU but also to those outside the EU if they offer AI systems to EU users or if their AI-generated outputs are used within the EU. This extraterritorial reach means **that businesses worldwide must ensure compliance if they develop, market or deploy AI solutions in the EU, reinforcing the Act's role in shaping global AI governance.**

Key Implementation Milestones

Key implementation milestones

The EU AI Act follows a phased implementation, giving businesses time to adapt. Key deadlines include:

August 1, 2024
The Act officially enters into force.

February 2, 2025
Prohibited AI practices (e.g., social scoring, real-time biometric surveillance in public spaces) become enforceable. Additionally, obligations related to **AI literacy for providers and deployers** of AI systems start to apply.

August 2, 2025
Governance rules for **General Purpose AI (GPAI)** models take effect, and EU member states must appoint regulatory authorities.

August 2, 2026
Full enforcement begins, including obligations for high-risk AI systems such as credit scoring and risk assessment models.

August 2, 2027
High-Risk AI as Safety Components: High-risk AI systems used as safety components in other products must fully comply with the regulation. Furthermore, **providers of GPAI models** that were placed on the market before August 2, 2025, must be fully compliant with the AI Act

With these deadlines approaching, banks and other financial institutions should start preparing now to ensure compliance and maintain a competitive edge in the evolving AI landscape. You can find here the detailed timeline.

Conclusion

AI regulation continues to evolve, not only to keep up with rapid technological advancements but also to refine key details and ensure practical implementation. For the banking sector, these regulatory changes bring both challenges and opportunities. **Compliance is not just a legal requirement - it enhances trust, strengthens market position, and ensures responsible AI adoption**.

Stay with us as **we continue to analyse the EU AI Act**! In our next post, we'll dive into its key components and what they mean for banks, financial service providers, and their partners - along with the vital steps they must take to stay compliant. **Don't miss it!**

And feel free to [book an appointment with our expert](book) any time.

Can We Rule the Machines? A deep dive into the EU AI Act – Part 2

After exploring the main goals of the EU AI Act, the region it applies to, the rollout schedule, and how other leading economies regulate AI in the first part of this series, **we now arrive at the heart of the matter**. In this second blogpost, we take a closer look at the **key elements of the AI Act and what they mean in practice**. We'll break down the most critical duties for banks, financial service providers, and their suppliers, and outline the vital steps they must take to ensure compliance. Let's dive in!

Key Elements of AI Act and Implications for Banks

With a strong focus on risk management, transparency, and accountability, the **AI Act introduces a risk-based approach to AI governance**. For banks and financial institutions, compliance with this regulation will be critical as AI-powered solutions, such as credit scoring and fraud detection, fall under its scope. This section provides an overview of the AI Act's core elements, with particular emphasis on aspects relevant to the banking industry.

A Risk-Based Approach to AI Regulation

The AI Act categorises AI systems into four risk levels, each with corresponding regulatory obligations. **This tiered approach ensures that higher-risk AI applications face stricter requirements** while allowing minimal oversight for low-risk systems.

Unacceptable Risk - Prohibited AI Practices

AI systems deemed to pose an unacceptable risk are banned outright under the AI Act. These include **social scoring systems** that evaluate individuals based on behaviour or socioeconomic status, like China's social credit system, **real-time biometric identification in public spaces** (e.g., facial recognition for mass surveillance), with just a few exceptions for law enforcement purposes or **manipulative or exploitative AI** that can harm vulnerable groups, such as children or individuals with disabilities.

For banks, this means they cannot deploy AI systems that rank customers based on arbitrary behavioural data for service eligibility or impose discriminatory lending practices based on opaque profiling.

High Risk - Strict Compliance Requirements

AI applications classified as high risk require rigorous compliance measures, as they significantly impact people's rights and financial stability. This category includes **credit scoring and risk assessment systems**, which influence loan approvals and terms or **automated insurance claims processing**, where AI determines claim validity and payouts.

Banks using high-risk AI systems must:

- Undergo a **conformity assessment** before deploying such AI models.

- **Register the AI system in an EU-wide database** for transparency.

- Maintain comprehensive **data logging and documentation** for auditing purposes.

- Implement **human oversight mechanisms** to ensure AI-driven decisions can be reviewed and overridden if necessary.

These requirements will likely increase compliance costs for financial institutions but will also enhance the reliability and fairness of AI-based banking operations.

Limited Risk - Transparency Obligations

AI systems that fall under the limited-risk category require clear disclosure and user awareness. An example: **chatbots and virtual assistants** used in customer service interactions.

For these systems, banks must inform customers that they are interacting with an AI system and clarify the type of data being processed. While these transparency obligations are relatively light, non-compliance could erode customer trust and invite regulatory scrutiny.

Minimal Risk - Voluntary Guidelines

AI applications classified as **minimal risk are subject to no mandatory requirements, but organisations are encouraged to adhere to ethical AI principles**. An example: **basic automation tools** that enhance operational efficiency without making impactful decisions.

Banks leveraging minimal-risk AI tools should follow industry best practices, such as implementing internal ethical guidelines and maintaining a commitment to fairness and transparency.

Regulating General-Purpose AI Models

Recognising the rapid advancement of AI technologies, the **AI Act dedicates a separate section to general-purpose AI models**, such as **large language models (LLMs)** that power AI-driven customer support and document processing or **image and video generation tools**, which could be misused for fraudulent purposes.

While banks may not directly develop these models, their integration into financial services (e.g., AI-assisted loan documentation or automated investment strategies) necessitates due diligence and compliance with emerging standards.

The purpose of the regulation is to ensure that the developers and providers of such models possess comprehensive knowledge of their models throughout the entire AI value chain, thereby enabling their integration into downstream AI systems and fulfilling the obligations prescribed by the law.

Sanctions and Enforcement

The EU AI Act establishes a system of **penalties designed to be effective, proportionate, and dissuasive**. High-risk breaches may incur fines of up to 35 million EUR or 7% of annual turnover, while other violations can result in fines of up to 15 million EUR or 3% of turnover, whichever is higher. Emphasising transparency, accountability, and fundamental rights, the **Act aims to balance rigorous oversight with the need for innovation**. Importantly, the penalty framework also considers the challenges faced by SMEs and start-ups, **ensuring that while violations are punished, smaller organisations are not overly burdened.**

Getting Ready: Key Steps for Banks to Comply with the EU AI Act

To ensure compliance with the EU AI Act, banks must take several proactive steps. First, they need to **assess their existing AI systems and categorise them according to risk levels**, identifying high-risk areas like e.g. credit scoring. **A comprehensive risk management framework must** then **be developed**, ensuring that robust measures are in place for these high-risk systems. **Collaboration with AI providers** is crucial to ensure alignment with regulatory standards and maintain compliance. Furthermore, banks should **prioritise AI literacy and continuously train staff** on the evolving legal landscape and its practical applications. A solid governance framework should be implemented, starting with securing **leadership support and assembling a diverse, skilled team** across legal, compliance, data science, and cybersecurity domains. **Setting clear priorities and gradually implementing AI governance initiatives** will be key. **Staying engaged with industry developments and contributing to AI governance discussions** will also help build a well-informed, collaborative environment that keeps the bank ahead of regulatory changes.

How AI System Providers Can Meet the EU AI Act?

AI system providers play a pivotal role in helping organisations comply with the EU AI Act. They are responsible for ensuring that their AI solutions meet the necessary regulatory requirements, especially for high-risk applications. This involves **providing clear documentation** on the system's design, functionality, **and risk assessment**, as well as **ensuring that the AI systems are transparent, explainable, and free from bias**. Providers must also **implement strong data protection measures** and ensure that their **AI models are continuously monitored for compliance throughout their lifecycle**. Additionally, they need to **assist their clients** in integrating compliance into their workflows, offering support for audits, **updating systems** to meet evolving regulatory standards, and **providing guidance** to educate them **on AI-related compliance requirements**. **Effective collaboration with users and maintaining an open dialogue with regulatory authorities** are essential for AI providers to navigate the complex compliance landscape.

Conclusion

In conclusion, successfully navigating the EU AI Act and its complex requirements demands a proactive and adaptable approach. For financial institutions, this means not just complying with regulations but **embracing AI with a forward-thinking mindset**. By carefully preparing, collaborating with the right partners, and staying engaged with ongoing regulatory changes, they can turn AI's challenges into opportunities. The **journey doesn't end here; continuous learning, adjustment, and a commitment to responsible AI will be key** as the landscape evolves. Stay tuned for more insights as we continue to explore this ever-changing field.

And feel free to [book an appointment with our expert](#) anytime.