

Market Intelligence Briefing

July 2025

AI Act

**Regulation from
the EU Commission**

August 2024

EU Policy Watch

AI Act

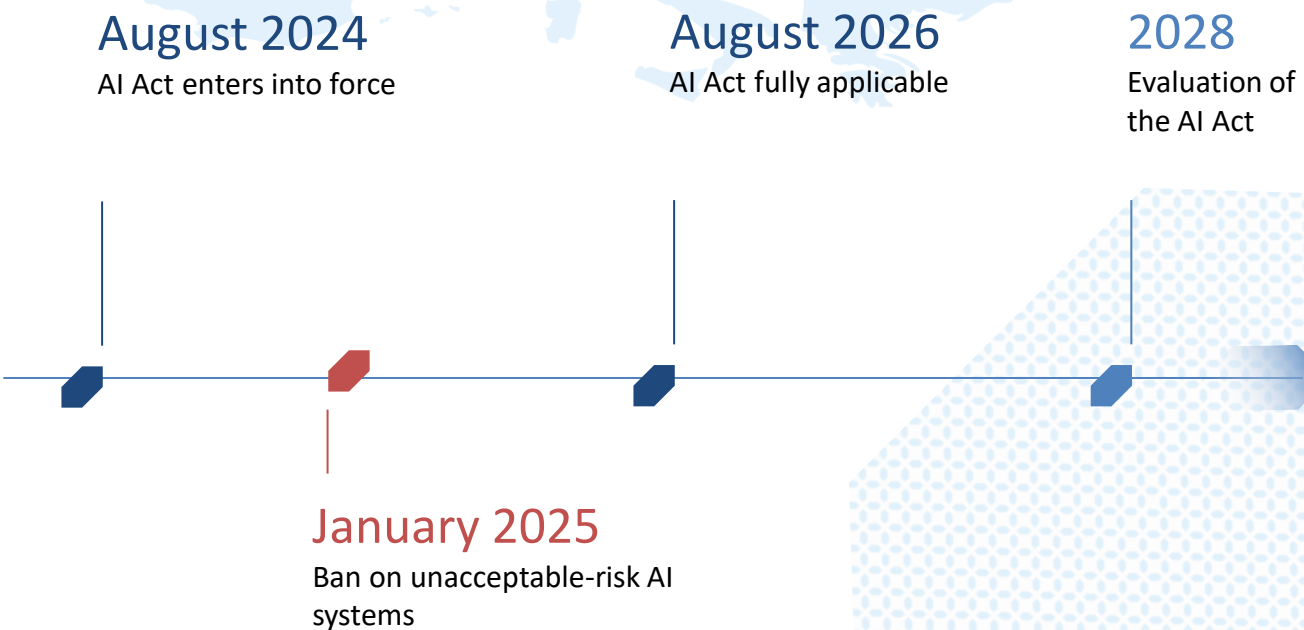
Context

The [Artificial Intelligence Act \(AI Act\)](#) is the European Union's landmark legal framework for regulating artificial intelligence. Proposed by the European Commission in April 2021 and formally adopted in 2024, the regulation entered into force on **1 August 2024 and will be fully applicable from August 2026**.

It follows the [EU's broader digital strategy](#) to position Europe as a global leader in trustworthy, human-centric AI. The AI Act is grounded in a **risk-based regulatory model** and builds upon the principles established by the [General Data Protection Regulation](#) (GDPR), aiming to safeguard fundamental rights, promote innovation, and ensure safety and transparency in AI deployment.

The Act applies to both public and private actors, including companies located outside the EU whose AI systems are used within the EU single market. It excludes AI systems developed exclusively for military or national security purposes, as well as those used solely for non-professional research or private use.

Timeline for implementation



Core structure and risk-based approach

At the heart of the AI Act is a **tiered regulatory framework** that classifies AI systems into four categories of risk: unacceptable, high, limited, and minimal. The level of regulatory obligation increases with the potential impact of the AI system on users' rights and safety.

Unacceptable risk AI includes systems that pose a clear threat to fundamental rights and are thus banned entirely. This includes applications like cognitive behavioural manipulation of individuals, real-time biometric identification in public spaces (with narrow exceptions for law enforcement), emotion recognition in schools or workplaces, and AI systems used for social scoring by public authorities.

High-risk AI covers systems that are likely to significantly affect individuals' lives, particularly in regulated domains such as education, employment, law enforcement, migration, critical infrastructure, and health. Providers of high-risk AI must comply with extensive requirements such as conformity assessments, quality and risk management systems, technical documentation, human oversight measures, data governance protocols, and cybersecurity safeguards. Deployers of high-risk systems must ensure they use systems appropriately and conduct fundamental rights impact assessments where applicable.



Risk classification of the AI Act by [trail](#)

Core structure and risk-based approach

Limited-risk AI includes systems like chatbots, AI-generated image or video content, and other tools where the main concern is ensuring transparency. In these cases, users must be clearly informed when they are interacting with AI or viewing content generated by AI. This supports informed consent and accountability in human-AI interaction.

Minimal-risk AI systems, such as spam filters and product recommendation engines, do not face specific legal obligations but are encouraged to follow voluntary codes of conduct. The Act ensures that such applications can continue to operate freely while encouraging best practices in their design and use.

General-Purpose AI and foundation models

A key innovation in the AI Act is the introduction of a regulatory framework for [General-Purpose AI \(GPAI\)](#), which includes **foundation models**—large-scale AI systems trained on broad data corpora and adaptable to a wide range of downstream tasks. This includes models such as GPT-4, LLaMA, and other foundational language and vision models.

Providers of general-purpose AI must meet baseline transparency obligations. These include maintaining up-to-date technical documentation, publishing summaries of training data (while respecting trade secrets and copyright), and ensuring lawful use of copyrighted material. Additional requirements apply to models posing **systemic risk**, such as those with high computational power, large-scale deployment, or the ability to generalize across tasks in ways that could affect public safety or democratic institutions.

For systemic-risk GPAI models, providers must conduct and document adversarial testing, assess potential societal impacts, implement robust safeguards (including watermarking and synthetic content labelling), and report serious incidents to the newly established [AI Office](#). These models are also subject to cybersecurity requirements and must disclose compute energy usage and environmental impact. The Act thus aims to ensure that high-impact foundation models are deployed responsibly, with appropriate oversight and safeguards to prevent misuse or harm.

Governance and enforcement

The enforcement of the AI Act will be coordinated at both the EU and national levels. The European Commission has established an [AI Office](#) to oversee implementation, particularly concerning general-purpose AI and cross-border cases. Each Member State is required to designate one or more **national competent authorities** responsible for supervision, enforcement, and market surveillance. These bodies will operate in coordination through the [European AI Board](#), which provides strategic guidance, ensures consistency in application, and supports information sharing among Member States.

The governance framework also includes a **scientific panel of independent experts** and a **multi-stakeholder advisory forum**, which offer technical advice and ensure that the regulatory process remains adaptive to technological change. The Act supports innovation through **regulatory sandboxes**, which allow developers to test high-risk AI systems in controlled environments and provides support measures for SMEs and start-ups to ease the compliance burden.

Penalties for non-compliance are significant. Providers that place prohibited AI systems on the market may be fined up to **€35 million or 7% of global annual turnover**. Breaches of high-risk or GPAI obligations can result in fines of up to **€15 million or 3% of turnover**, while misleading or inaccurate documentation may lead to fines of up to **€7.5 million or 1.5%**. The severity of fines scales with the size of the provider, ensuring proportional enforcement.

Conclusion

The AI Act marks a pivotal moment in the global governance of artificial intelligence. It is the first comprehensive regulatory framework to address the full lifecycle of AI systems, balancing innovation with legal certainty, ethical safeguards, and risk mitigation. Its risk-based structure allows for differentiated obligations depending on the potential harm AI systems can cause, while its targeted provisions on foundation models reflect the evolving role of general-purpose AI in society and the economy.

The Act also reinforces the EU's role as a global standard-setter, encouraging international actors to align with its principles in order to maintain access to the EU market. Its impact will shape the behaviour of AI developers and deployers worldwide, particularly those working on large-scale, general-purpose systems.

LUXINNOVATION MARKET INTELLIGENCE BRIEFING

Discover more insightful content at www.luxinnovation.lu/knowledge-hub

Luxinnovation Contributors

Research & Writing: Tiffany Devresse – Market Intelligence Analyst

Editing & Review: Sara Bouchon – Director Market Intelligence



LUXINNOVATION
#MakingInnovationHappen