

AI at the edge of regulation: Inside the EU AI Act and its impact

As AI becomes embedded in everything from wearables to autonomous vehicles, regulators are stepping in. The EU AI Act is the first major attempt to set clear, risk-based rules for responsible AI use. This article explores what the Act means, how it's shaping global policy, and what it means for edge AI companies.

Gabija Cepurnaite, Senior Consultant

June 2025

© STL Partners

Artificial intelligence is everywhere – from voice assistants and personalised shopping recommendations to life-saving medical devices. However, as AI's reach grows, so do concerns about its usage. Recent headlines have highlighted the downsides of unchecked AI, ranging from deepfake videos of politicians causing public confusion, to a glitch in an autonomous warehouse robot that raised questions about worker safety. Incidents like these serve as a reminder that while AI can unlock incredible innovation, it can also be misused or go awry with serious consequences.

Regulators have taken note. In the European Union, lawmakers have introduced the EU Artificial Intelligence Act – a landmark effort to set rules on AI's development and use.

What is the EU AI Act trying to achieve?

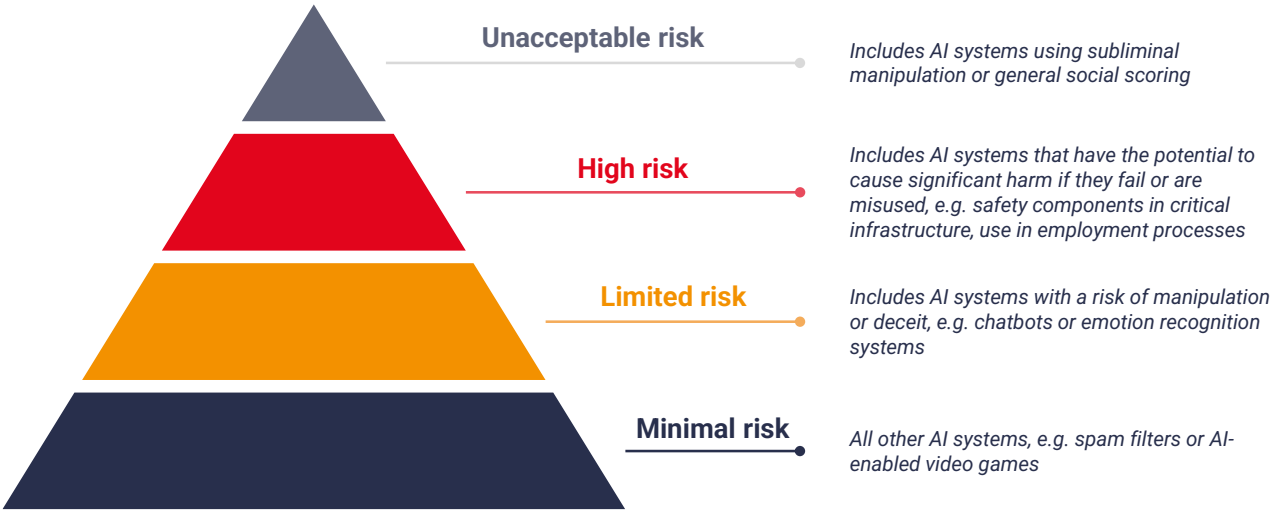
The EU AI Act is the world's first comprehensive attempt to regulate AI systems. Formally adopted in 2024, it aims to ensure AI is developed and used in a way that is safe, transparent, and respectful of fundamental rights without outright stifling innovation. In scope, it covers all types of AI systems placed on the EU market or used in the EU, whether they're made by European or overseas companies. The Act uses a risk-based approach to classify AI applications and impose rules accordingly:

- **Minimal or no risk AI:** This includes basic applications like grammar-checkers or simple chatbots. Such AI faces no special requirements under the law, but providers may voluntarily comply with codes of conduct.
- **Limited risk AI:** These systems, such as chatbots or emotion-recognition tools, require basic transparency obligations, like informing users that they are interacting with an AI system.
- **High-risk AI:** This category covers AI used in sensitive or critical areas that could significantly affect people's lives, such as:
    - Medical devices using AI
    - AI in critical infrastructure (e.g., transportation, energy)
    - Educational and vocational assessments
    - Employment-related tools like CV scanners
    - Credit scoring, insurance, and border control technologies

  Such systems are allowed, but heavily regulated. Providers must implement strict risk management, data governance, quality testing, logging, and human oversight to ensure safety and fairness. High-risk AI may also undergo audits or certification before and during deployment.
- **Unacceptable risk AI:** These AI systems are banned outright due to their potential to violate fundamental rights. They include:
    - AI that manipulates human behavior subliminally
    - Systems exploiting vulnerable groups (e.g., children or disabled individuals)
    - Real-time biometric identification in public spaces (with narrow law enforcement exceptions)
    - Social scoring systems
    - Biometric categorisation based on race, religion, political beliefs, or sexual orientation

© STL Partners

Figure 1: The four risk categories defined in the EU AI Act



Souce: STL Partners

By categorising AI in this way, the EU AI Act's objective is to focus oversight where it matters most – ensuring that AI in critical environments meets higher standards of transparency, accuracy, and human control. At the same time, the Act seeks to give developers clarity about the "rules of the road" so that beneficial AI innovation can continue responsibly. Notably, the law also introduces obligations for general-purpose AI and future technologies: for example, makers of large AI models (like generative AI systems) may be required to disclose certain information about training data or include safeguards against misuse – an attempt to future-proof the regulation as AI evolves.

Global momentum: AI regulation is going mainstream

While the EU is the first to introduce comprehensive AI legislation, many other countries are following suit. Around the world, governments are beginning to craft their own approaches to AI governance. As with GDPR, the Act's scope and ambition are expected to influence global norms, particularly for companies operating across borders, however, the efforts so far have been fragmented:

- **In the United States**, there is no overarching federal AI law, but regulation is picking up at the state level. Over 30 states passed AI-related legislation in 2024, with Colorado leading the way through its upcoming rules on high-risk AI systems. At the federal level, the focus remains on non-binding guidance. Frameworks such as NIST's AI Risk Management Framework and the White House's Blueprint for an AI Bill of Rights outline best practices but do not impose legal requirements.
- **China** has implemented top-down rules focused on controlling AI-generated content through its Interim Measures for the Management of Generative Artificial Intelligence Services, requiring all such content to be clearly labeled and traceable. These efforts are part of a broader strategy to manage information integrity and align AI development with state priorities.
- **The UK**, which initially favoured a light-touch stance, has recently shifted gears. The government announced plans in 2024 to legislate frontier AI models, signalling a move toward more formal oversight.

Taken together, these developments suggest that AI regulation is becoming a global priority, not just a European one. While approaches vary, the direction of travel is clear: governments everywhere are moving to ensure AI is developed and deployed responsibly and companies will need to adapt accordingly.

© STL Partners

What does it mean for edge AI?

Under the EU AI Act, a range of edge computing applications are likely to be classified as high-risk – not because of where they run, but because of what they do. Tasks like medical monitoring, autonomous navigation, and industrial automation carry real-world safety, health, and operational consequences. These include:

- **Autonomous vehicles**, which rely on on-board AI for split-second navigation and object detection.
- **Health wearables**, such as devices that monitor heart rate or glucose levels to support medical decision-making.
- **Industrial sensors**, which control or monitor machinery in real-time on factory floors or in energy systems.

These systems offer powerful benefits – from real-time responsiveness to enhanced user experience – but their impact on health, safety, and individual rights places them in a regulated tier. For high-risk edge AI, the implication is clear: companies will need to invest in additional testing, monitoring, documentation, and control features. Compliance will become a core part of the product lifecycle, not a post-deployment add-on.

There's also a flip side: edge computing might help with compliance in some ways. Because edge devices process data locally, they can enhance privacy by minimising what data gets sent to the cloud. This "privacy-by-design" aspect can aid compliance with data protection laws like GDPR. If done right, edge AI could reduce the risk of massive data breaches (since data isn't centralised) and make it easier to meet certain regulatory requirements around data minimisation. The EU AI Act works in tandem with privacy rules, so a well-designed edge system that keeps personal data on-site might actually tick both boxes – providing faster service and better privacy.

Conclusion

The EU AI Act represents a major step in the journey toward responsible AI – an attempt to set "rules of the road" in a fast-moving domain. Its focus on risk-based controls is poised to influence how AI is built and deployed not just in Europe, but worldwide. For edge computing, the Act is a double-edged sword: while it may raise some challenges in implementation, it also validates the importance of edge strategies (especially for privacy and real-time reliability) in a regulated future. As other countries formulate their own policies and businesses adjust, one thing is clear: the era of unregulated AI is ending. Much like financial markets, automobiles, or pharmaceuticals, AI technologies are entering an age where oversight is part of the ecosystem. The next few years will be critical as industries adapt – those that proactively embrace these rules stand to not only avoid penalties but build greater trust with users and customers.

Gabija is a Senior Consultant at STL Partners, specialising in edge anc cloud computing.

Get in touch with the author to learn more

gabija.cepurnaite@stlpartners.com

Or visit STL Partners' Edge & Cloud Hub

www.stlpartners.com/edge-computing

© STL Partners