

**ORGX INSIGHT INTO ACTION**

# **EU ARTIFICIAL INTELLIGENCE ACT**

*This Act ended ungoverned AI experimentation in Europe. Forcing organizations to choose whether AI becomes a regulated liability or a strategically governed advantage.*

- *Identifying which AI systems fall under regulatory scrutiny*
- *What high-risk AI governance requires in practice*
- *Preparing for transparency obligations and enforcement timelines*

LET'S TAKE A LOOK

## What is the EU AI Act?

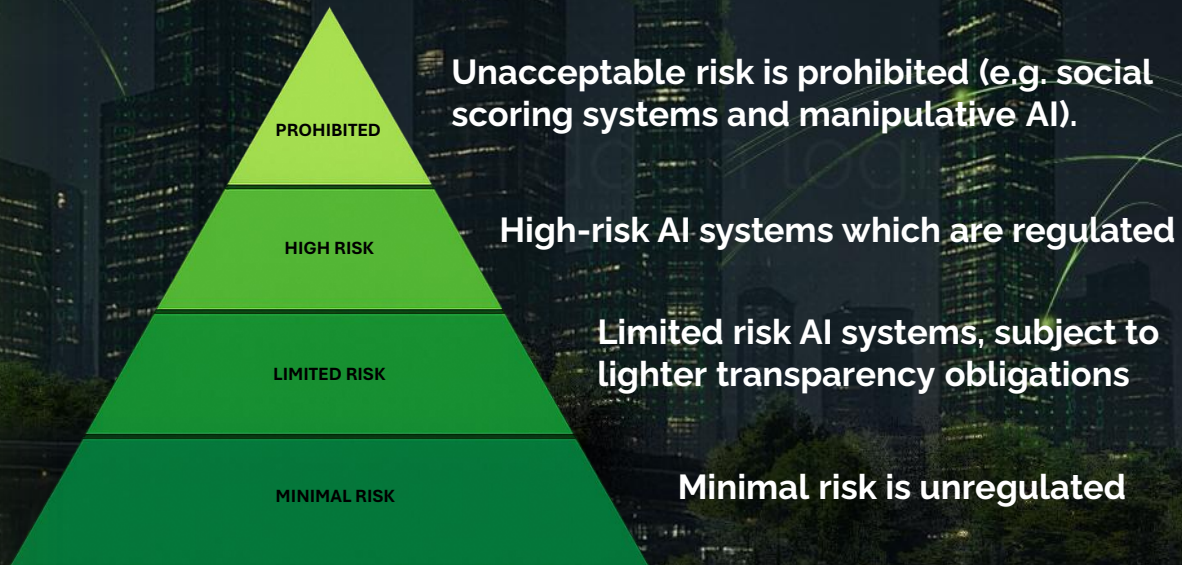
Formally adopted as Regulation (EU) 2024/1689, the AI Act sets harmonised rules for the development, placing on the market and use of AI systems in the European Union. It applies not only to EU based organisations, but also to companies outside the EU if their AI systems affect people in the EU.

The Act is horizontal and cross sector. It covers AI used in areas such as recruitment, creditworthiness, healthcare, education, law enforcement, customer interaction, and content generation.



# *The risk-based approach: Prohibited and high-risk AI*

At the core of the AI Act is a four tier risk classification:



*But two categories matter most from a compliance and governance perspective.*

## **Category #1**

### ***Prohibited AI (unacceptable risk)***

---

Certain AI practices are banned outright because they pose a clear threat to fundamental rights. These include, among others:

- AI systems that manipulate behaviour using subliminal or deceptive techniques
- AI that exploits vulnerabilities related to age, disability or socioeconomic status
- social scoring systems
- assessing the risk of an individual committing criminal offenses
- inferring emotions in workplaces or educational institutions
- certain forms of biometric surveillance and categorisation.

**These systems cannot be placed on the EU market at all.**



## **Category #2**

# **High-risk AI systems**

---

High-risk AI systems are permitted, but are highly regulated. An AI system is considered high-risk if:

- it is used as a safety component of a product that is regulated under EU legislations listed in Annex I of the Act and therefore subject to third-party conformity assessment
- it falls into one of the use cases listed in Annex III of the Act, such as AI used for employment decisions, critical infrastructure, education, biometric identification, access to essential services, law enforcement, border control, or administration of justice and democratic processes



# *What rules apply to high-risk AI systems?*

---

For high-risk AI, the Act introduces obligations that affect the entire AI lifecycle, not just deployment. Providers and deployers must ensure, among other things:

- a documented risk management system
- strong data governance to address bias and data quality
- detailed technical documentation and recordkeeping
- appropriate human oversight,
- requirements for accuracy, robustness, and cybersecurity
- a quality management system
- set of instructions for use

In practice, this turns AI compliance into an operating model and governance challenge.



## *Transparency obligations: knowing when AI is involved*

---

Beyond high-risk systems, the AI Act introduces transparency obligations for certain AI uses, set out in Article 50. These rules apply, for example, when:

- people interact directly with AI systems (such as chatbots)
- AI generates or manipulates text, images, audio or video (including deepfakes)
- emotion recognition or biometric categorisation systems are used.

In these cases, users must be clearly informed that they are interacting with AI or AI generated content. Outputs of generative AI must be detectable as AI generated, using technical measures such as labelling or machine-readable markers.

These transparency rules are designed to reduce risks of deception, manipulation and misinformation, while fostering trust in AI enabled systems.



## AI Act Timeline

The AI Act entered into force in 2024, but its obligations apply in phases. While some provisions are already relevant, major parts of the Act are set to apply on 2 August 2026 and 2 August 2027, depending on the type of AI system and the obligations involved.

For organisations using or developing AI, this means the window for “wait and see” is closing. Understanding where AI is used, what risk category applies, and how governance must change is now a strategic priority.



**WANT TO LEARN MORE?**

Let's schedule a meeting!

From Amsterdam throughout Europe  
Overschiestraat 65 • 1062 XD Amsterdam  
office@orgx.com • www.orgx.com