



POLICY BRIEF

15 05 2024

11

THE AI ACT:

THE FIRST WORLD-WIDE AI REGULATION

IRINA CARNAT & ARIANNA ROSSI



The AI Act: the first world-wide AI regulation	
BACKGROUND AND FIELD OF APPLICATION	<p>The EU's AI Act is the world's first comprehensive AI law that establishes harmonized rules for the development and use of AI systems. It derives from the need of creating and using human-centric and trustworthy AI systems that protect the health, safety and fundamental rights.</p> <p>The AI Act is integral part of the EU Digital Strategy that intends to promote innovation and competitiveness at the international level, while establishing safeguards against the risks and possible harms generated by AI.</p>
HIGHLIGHTS	<p>The key elements of the AI Act can be summarized as follows:</p> <ul style="list-style-type: none"> • The AI Act is a risk-based regulation: it establishes obligations for developers (or providers) and users (or deployers) of AI systems used in the EU (even when they are not based in the EU) depending on the level of risk that their systems pose. The higher the risks, the stricter the compliance requirements for product safety. • Certain AI systems are prohibited because they pose an unacceptable risk, such as those that perform social scoring, compile facial recognition databases from scraping activities, exploit vulnerabilities or use manipulative techniques to cause harm. • AI systems that significantly affect health, safety (such as medical devices) or fundamental rights, they are considered as high-risk. They have many requirements concerning risk management, data governance, transparency, documentation, human oversight, among others. They will need to be assessed before being placed on the market and throughout their lifecycle. • There are specific obligations for general-purpose AI models (GPAI), distinguishing between those with system risks and those that do not pose systemic risks. The difference is based essentially on the model's size determined by its computing power (and amount of data used for training). All GPAIs require the provision of the relevant technical documentation and information for downstream developers, but those with systemic risks have additional obligations, such as performing model evaluations, report serious accidents, and adopt cybersecurity measures. • Finally, there are transparency requirements for certain AI systems, mainly those intended to interact with people, and more broadly generative AI. Providers of such AI systems have to



	<p>disclose that the content was generated by AI, design the model to prevent it from generating illegal content, and also to publish summaries of copyrighted data used for training.</p> <ul style="list-style-type: none"> • Timeline: The regulation fully enters into force 2 year after being published in the Official Journal. However, the ban of AI systems posing unacceptable risks will apply 6 months after the entry into force; provisions concerning codes of practice will apply 9 months after entry into force; rules on general-purpose AI systems that need to comply with transparency requirements will apply 12 months after the entry into force; and finally obligation concerning high-risk systems on the other hand will have more time to comply with the requirements as they will become applicable 36 months after the entry into force.
RELATED POLICY BRIEFS	<ul style="list-style-type: none"> - No. 12: Transparency in the AI Act - No. 13: Classification of AI systems as high-risk and relevant obligations under the AI Act - No. 14: Data governance in the AI Act - No. 15: AI literacy in the AI Act