

Publication

08/02/2024

EU Sets Key Artificial Intelligence Regulation Dates

On August 1, 2024, the regulation of artificial intelligence (AI) took a major leap forward as the EU AI Act officially entered into force. While the Act is enforced within the EU, its extraterritorial scope has important implications for U.S. companies—any company placing AI models in the EU market, including where output of an AI system is used in the EU, may be subject to the Act's requirements. With the August 1, 2024 effective date, companies that provide or deploy AI should evaluate whether and how the EU AI Act impacts them and begin establishing internal policies and procedures for compliance.

The EU AI Act takes a risk-based approach to AI regulation, dividing AI systems into four risk categories: unacceptable, high, limited, and minimal. AI systems with unacceptable risk are prohibited. High-risk AI systems face the most significant regulation. Limited risk systems have some regulation, while minimal risk AI systems are unregulated.

Prohibited AI, except for a limited set of exceptions, includes systems that: use subliminal, manipulative or deceptive techniques to distort behavior or impair the ability to make informed decisions; exploit vulnerabilities due to age, disability, or social or economic situation; or use facial recognition databases, infer emotions, or categorize individuals based on biometrics to infer certain characteristics. High-risk AI generally refers to systems that have an impact on health, safety or

CLIENT SERVICES

Intellectual Property

Cybersecurity & Data Privacy

Cybersecurity & Data Privacy

RELATED PEOPLE

Alfred C. Tam

David A. Wheeler

Josh Hanson

Kate H. Campbell

fundamental rights, including AI systems that: function as safety components in critical infrastructure; make decisions about access to education and vocation training; evaluate job applications or promotion decisions; or determine access to essential private and public services. Limited risk AI includes systems with the risk of impersonation, manipulation or deception such as chatbots, deep-fakes or AI generated content. Minimal risk AI includes common AI systems used in inventory management systems, spam filters, or AI-enabled video games.

In addition to regulations for AI systems, the EU AI Act contains regulations for AI models. Under the Act, deployers of general purpose AI (GPAI) models face significant obligations related to record keeping, documentation, cybersecurity, model evaluation, risk assessment, and incident reporting. GPAI models are defined within the Act as AI models with the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems. Under the Act, GPAI models with “high-impact capabilities” could pose a systemic risk and have a significant impact on the EU market, due to their reach and their actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole. GPAI providers will be required to notify the European Commission if the total number of computations used to train their model exceeds 10^{25} floating-point operations (FLOPs), approximately equivalent to GPT-4. When this threshold is met, the presumption will be that the model is a GPAI model posing systemic risks, and providers of systemic-risk GPAI models are required to continuously assess and mitigate the risks they pose and to ensure cybersecurity protection. Note, however, that this is only an initial threshold, and the Act calls for adjustment over time to account for technological developments.

With the August 1, 2024 effective date, the following key deadlines are now in place:

- February 2, 2025: Prohibitions on unacceptable risk AI enter into force. Prohibited AI systems must be withdrawn from the market.
- August 2, 2025: Obligations for providers of general purpose AI models enter into force.
- February 2, 2026: Requirements for post-market monitoring of AI systems enter into force (through the adoption of the Implementing Act).
- August 2, 2026: Obligations for the majority of high-risk AI systems enter into force.

With the near-full enforcement a year away, companies should determine what risk category prospective AI systems fall into so that they can understand and prepare for compliance with the associated requirements. Indeed, penalties for non-compliance with the EU AI Act are more aggressive than penalties under the EU's General Data Protection Regulation (GDPR). Penalties under the EU AI Act range from the greater of €35 million or 7% of global revenue for violations related to prohibited AI to the greater of €15 million or up to 3% of global revenue for violations of other obligations of providers or deployers of AI.

It is important to note that the EU AI Act is not the only set of AI regulations currently affecting U.S. companies. Laws in Utah and Colorado directly impact the use and development of AI models within the U.S. as well—with more state, and possibly federal, laws to follow. Utah's Artificial Intelligence Policy Act and Colorado's AI Act contain disclosure requirements, while Colorado's law also mandates significant risk-related assessments and documentation.

As the era of AI continues to boom, companies must stay on top of the growing number of regulations and will be



best positioned to do so by establishing internal AI-governance programs. If you are looking for guidance related to AI classification, governance or compliance, NGE has attorneys with significant background in AI that are also certified AI Governance Professionals by the International Association of Privacy Professionals. If you need assistance with the use or development of AI, please contact your Neal, Gerber & Eisenberg attorney, or a member of our Cybersecurity & Data Privacy team—Kate Campbell, Alfred Tam, and David Wheeler.

The content above is based on information current at the time of its publication and may not reflect the most recent developments or guidance. Neal Gerber Eisenberg LLP provides this content for general informational purposes only. It does not constitute legal advice, and does not create an attorney-client relationship. You should seek advice from professional advisers with respect to your particular circumstances.