GOODWIN

INSIGHT · FEBRUARY 14, 2024

# The EU AI Act Is (Almost) Here. What It Means for Your Business

*The EU AI regulation applies to any business that develops or deploys AI, but the greatest regulatory burdens fall on high-risk AI systems.*

BY Gretchen Scott Omer Tene Marie Fillon Thomas Dupont-Sentilles

The EU Parliament's committees for internal market and civil liberties overwhelmingly adopted the final text of the Artificial Intelligence Act (AI Act). The European Parliament will now vote on the AI Act in a formality that will see it become law in April.

The AI Act's imminent passage ushers in regulatory, governance, and ethical requirements for companies across the globe that develop, deploy, import, and distribute AI systems.

Despite its broad reach, the AI Act's practical impacts are narrower in scope, focusing on a small slice of businesses with high-risk AI systems. These companies, whose AI systems pose significant risk of harm to people's health, safety, or fundamental rights, face the bulk of regulatory requirements.

The latest draft of the AI Act sets forth a specific regulatory category covering "general-purpose AI (GPAI) models," which includes generative AI (GenAI). Providers of GPAI must comply with EU copyright law, publicly share summaries of the content used to train their models and inform downstream users about the logic underlying their decision making. More powerful GPAI models considered as posing systemic risks are subject to more stringent obligations, such as model evaluations, risk management, and incident reporting.

For most businesses, however, including providers and deployers of lower-risk AI systems, the AI Act will not portend major changes. Such companies will be subject primarily to transparency obligations, such as informing consumers that they are interacting with an AI system or flagging artificially generated content, and ensuring their personnel dealing with AI systems have sufficient AI literacy.

The AI Act also seeks to encourage compliance with ethical guidelines for trustworthy AI, environmental sustainability, and other factors to mitigate negative impacts of AI systems. Most of the rules will begin to apply two years after the AI Act enters into force, with some exceptions. For instance, rules on GenAI providers will apply just one year after the regulation enters into force; and prohibitions on unacceptable risk AI systems merely six months after the implementation date.

Companies should start determining now where their AI systems fit on the risk spectrum of regulatory requirements. Below we lay out a framework for businesses seeking to understand how the law applies to them, as well as an overview of the impacts on key stakeholders: providers of high-risk AI systems and of GPAI.

## How does the AI Act affect my business?

The following three-step framework can help companies begin to determine how the AI Act will affect them.

*Step 1: Determine your role in the AI value chain.* Different players occupy different roles in the AI value chain. The AI Act regulates several key roles, including providers, deployers, distributors, manufacturers, and importers of AI systems.

*Step 2: Determine the risk level of your AI system.* The AI Act categorizes AI systems based on the level of risk they pose, establishing four main risk categories.

- **Unacceptable risk.** The AI Act bans these particularly high-risk AI systems outright. Examples include technologies that manipulate cognitive behavior, systems that exploit vulnerable groups or individuals, social-scoring systems, and biometric-categorization systems.
- **High risk.** These systems are subject to extensive regulatory obligations. They include systems related to education, employment, biometrics, immigration, and law enforcement.
- **GPAI.** The regulation treats GPAI as its own risk category. These systems, which include large scale GenAI models, must implement AI governance and transparency requirements, including providing downstream users with information to help them comply with their legal obligations.
- **Other.** All other AI systems, like AI-powered chatbots, face limited regulatory requirements.

*Step 3: Determine your regulatory obligations.* To determine the scope of regulatory obligations that apply to your business, overlay your role in the AI value chain with your category of risk. The intersection of these two categories will determine your regulatory obligations. For instance, if you are a *provider* (role) of a *high-risk AI system* (risk level), you will have a certain list of legal obligations under the AI Act, which is different from those that apply to *deployers* of high-risk AI or to providers of *unacceptable risk* systems.

More complicated situations can arise. A single company might play multiple roles or provide or deploy several AI systems that pose varying types of risk, thus becoming subject to multiple different sets of legal requirements. For example, a tech company that creates and sells a machine-learning tool for data analysis would be a provider, but at the same time it could apply such tools in-house as a deployer and modify the deployed tools to help sift through recruitment applications (a high-risk use case). The tech company would need to ensure compliance with legal obligations applicable to both roles and to different risk levels.

Finally, a company that did not originally develop an AI system could be considered a high-risk provider in certain circumstances, for example, if it makes certain modifications to, or places its name or trademark on, an existing high-risk AI system.

## How does the AI Act classify AI systems as high risk?

An AI system will be considered high risk in two situations: first, if the AI system is a product covered by certain EU harmonization legislation or is a safety component of such covered product (for example, toys, medical devices, or machinery) that mandates a third-party conformity assessment.

Second, if the intended use case for the AI system falls within a list of presumed high risk uses. Of these, we anticipate a concentration of high-risk use cases relating to biometrics, safety components for critical infrastructure, and education or employment-related systems. Those in the financial services sector should note that credit scoring and risk assessments and pricing for life or health insurance are classified as high risk.

In this second category, it is possible to rebut the presumption of high risk if the AI system does not pose a significant risk of harm to people's health, safety, or fundamental rights. But this self-assessment will be subject to scrutiny by the regulatory authorities.

## What are the main obligations relating to high-risk AI systems?

The AI Act imposes the strictest regulatory requirements on businesses that develop or deploy high-risk AI systems.

Providers of high-risk systems must comply with an extensive list of obligations before, during, and after launching their AI. These requirements are designed to encourage safe and trustworthy AI. They include maintaining comprehensive technical documentation and risk and quality management systems throughout the AI system's lifecycle, using quality datasets, facilitating transparency, and ensuring systems allow for automatic event recording for traceability and monitoring.

High-risk AI systems must pass a conformity assessment before being placed on the EU market, as evidenced by the CE mark, which represents compliance with EU legal standards.

Deployers of high-risk AI systems are subject to obligations that recognize the risks arising from their use of such AI systems and the need to monitor performance as they operate in a live environment. Deployers' obligations include complying with providers' instructions for use and ensuring the input data are transparent and suitable for the AI system's intended purpose.

All participants in the AI deployment chain are subject to monitoring and reporting obligations with respect to risks presented by high-risk AI systems.

## What are the main obligations on GPAI model providers?

GPAI model providers — including GenAI providers — must maintain detailed technical documentation of the model and share certain information with providers of AI systems who intend to integrate the GPAI model into their AI system. They also need to develop policies and disclose information on content used to train models, requirements that are intended to bolster protection for copyright holders. Free open source GPAI models (that do not have systemic risks) are exempted from most of these obligations.

The AI Act requires high-powered GPAI models that pose systemic risks to fulfill the obligations applicable to all GPAI model providers, as well as additional obligations, such as model evaluations, mitigation of systemic risks, and cybersecurity protection. They also must report serious incidents to the AI Office, a new regulatory agency that the AI Act sets up at the EU level.



## CONTACTS

### Gretchen Scott
Partner

gscott@goodwinlaw.com
London | +44 (0)20 7447 4292

### Omer Tene
Partner

otene@goodwinlaw.com
Boston | +1 617 570 1094

Marie Fillon
Partner

mfillon@goodwinlaw.com
Paris | +33 (0)1 85 65 72 30

Thomas Dupont-Sentilles
Partner

tdupontsentilles@goodwinlaw.com
Paris | +33 (0)1 85 65 71 40