DAVIS GILBERT

Privacy, Technology + Data Security

The EU Artificial Intelligence Act: Key Takeaways and Analysis

The Bottom Line

- The EU AI Act will soon begin to restrict, regulate or prohibit AI-related activity that impacts the EU market.
- Both AI providers and deployers will have to follow stringent rules that ensure the technology is used transparently, safely and ethically.
- Companies that operate or conduct business in the EU should conduct an assessment of their AI systems to determine where their activities may fall under the AI Act's risk categories and adopt applicable compliance measures.

Jurisdictions worldwide, including several U.S. states, are starting to set new legal and regulatory guidelines for the use and development of artificial intelligence (AI) systems. However, the European Union is taking the lead with the EU Artificial Intelligence Act, considered to be the world's first comprehensive legal framework for AI. Formally adopted by the European Parliament on March 13, 2024, and approved by the EU Council on May 21, 2024, the AI Act's final text is expected to be officially published in the coming weeks.

While the AI Act will take effect in a tiered approach over the next couple of years, here is what businesses need to know now.

Applicability and Scope

The AI Act regulates "AI systems," defined as machine-based systems that operate autonomously, adapt over time and generate outputs like predictions or decisions that can influence physical or virtual environments. Its regulations also encompass "general-purpose AI models" (GPAI models), which are versatile algorithms trained with large data sets that comprise larger AI systems and allow them to perform a wide range of distinct tasks.

The AI Act applies broadly, covering two main categories of businesses:

- "providers" – entities that offer or market AI systems or GPAI models in the EU market
- "deployers" – those who use an AI system in the EU

Importantly, providers or deployers outside of the EU are also subject to the AI Act if the output of their AI systems are used within the EU, making the law's reach truly global.

Risk Thresholds

A key feature of the AI Act is its risk-based categorization, which can apply individually or in combination with each other.

AI systems categorized as posing an **unacceptable risk** are prohibited outright. The law's list of prohibited activities includes using AI systems or AI models for:

- social scoring
- purposely manipulative or deceptive techniques
- exploitation of vulnerable populations
- creation of facial recognition databases through scraped internet or closed-caption television (CCTV) data
- predictive policing
- most emotion recognition systems in workplace or educational settings
- certain biometric categorization and identification activities

High-risk AI systems are permissible, subject to additional compliance obligations under the law. Some examples of high-risk categories are expressly listed in the AI Act, including AI systems used as a safety component of products such as machinery, toys, medical devices and cars; and AI systems used in sensitive industry sectors, such as biometrics, critical infrastructure, education and employment.

Providers and deployers of high-risk AI systems may, depending on the circumstances, be subject to a litany of requirements, which could include:

- completing fundamental rights impact assessments
- registration in a public EU database
- implementing risk and quality management systems
- using high-quality data to reduce bias
- ensuring transparency
- logging automated activities

- reporting incidents
- maintaining human oversight
- appointing an EU representative
- guaranteeing the system's accuracy, robustness and security

AI systems that do not rise to the level of an unacceptable risk or a high risk may be considered **limited risk** or **minimal risk**, and will be subject to fewer regulatory requirements. However, the risk level of such systems may vary depending on the application for which they are used.

As it relates to GPAI models, the AI Act differentiates between those with and without "systemic risk," which is deemed present in models with high-computing power capabilities. All providers of GPAI models must appoint an EU representative and maintain detailed technical documentation and other information about the model, and must comply with EU copyright laws. Those with systemic risk must also conduct advanced evaluations, manage risks, report incidents and ensure robust cybersecurity. These measures aim to ensure the safe and responsible deployment of powerful AI systems.

Disclosure Obligations

The AI Act also sets forth transparency and disclosure obligations for AI systems that interact with humans or generate content. It requires that such AI systems clearly inform users they are dealing with a machine unless it is obvious from the context. For AI-generated content, such as synthetic audio, images, videos or text, providers must mark these outputs to indicate they are artificially generated or manipulated. Deployers of deep fake content must also disclose its artificial nature, ensuring transparency and trust in digital content.

Additionally, any AI-generated or manipulated text intended for public information must be identified as such unless it has undergone human review. AI systems used for emotion recognition or biometric categorization must inform individuals about their use and operation, ensuring that people are aware of how their personal data is being processed.

Enforcement and Penalties

Enforcement will be managed by the EU and its individual member states, supported by an EU AI Office and national authorities. While the AI Act does not expressly provide a private right of action, proposed directives may create an avenue for civil enforcement in EU courts in the near future. The AI Act provides a range of fines and penalties for different violations, from €7.5 million or 1% of total worldwide annual turnover (whichever is higher) for providing incorrect, incomplete or misleading information to regulatory authorities, to €35 million or 7% of global annual turnover

(whichever is higher) for violations involving prohibited AI systems. Given the potential for significant liability under the law, organizations have a strong financial incentive to comply with the AI Act's requirements.

Impact on Businesses

The EU AI Act will significantly impact ordinary companies and businesses that develop or use AI systems. Providers of AI technologies will need to comply with these stringent regulations, ensuring their systems are transparent, safe and ethically sound. This includes conducting thorough risk assessments and implementing robust data management practices to prevent bias and discrimination. Deployers of AI will also need to disclose when they use AI to interact with customers, label AI-generated content and ensure any deep fakes are clearly identified as having been created with AI.

The key for businesses navigating these new regulations is proactive compliance. Companies should start by conducting an internal audit of the AI systems they use to understand where they may fall in the AI Act's risk categories. Develop a clear plan to meet transparency requirements, such as informing users about AI interactions and labeling AI-generated content. For any company that would be considered a high-risk AI provider, it's also crucial to appoint an EU representative and maintain up-to-date technical documentation. Businesses should also implement robust cybersecurity measures to protect their AI systems and be prepared to report incidents promptly. By taking these steps, companies can not only avoid penalties but also build trust with their customers and stakeholders, positioning themselves as responsible and ethical players in the AI landscape.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Paavana Kumar
Partner
212 468 4988
pkumar@dglaw.com

Samantha Rothaus
Partner
212 468 4868
srothaus@dglaw.com

Zachary Klein
Associate
212 237 1495
zklein@dglaw.com

Andrew Richman
Associate
212 468 4804
ajrichman@dglaw.com