GT GreenbergTraurig

Alert | Innovation & Artificial Intelligence

November 2024

EU Artificial Intelligence Act – Business Implications and Compliance Strategies

On Aug. 1, 2024, the EU Artificial Intelligence Act (AI Act) entered into force and will gradually take effect over the next 36 months. This marks not only the end of yet another legislative saga within the European Union but also the beginning of a new era in AI regulation. The AI Act creates an extensive regulatory framework which will affect businesses worldwide and across virtually every sector. Given that parts of the AI Act will apply starting Feb. 2, 2025, companies should consider developing and implementing compliance strategies now.

The AI Act aims to promote human-centric and trustworthy AI while ensuring a high level of safety, fundamental rights, and environmental protection. At the same time, legislators hope to boost innovation and employment and to make the European Union a leader in the development of secure and ethical AI. Whether the AI Act will be able to fulfil these objectives remains to be seen, but the AI Act introduces an unprecedented regulatory framework which will be relevant across multiple business sectors and could serve as a blueprint for regulations in other jurisdictions.

The AI Act follows a risk-based approach and relies on "self-assessment" of AI systems by their manufacturers, providers, deployers, etc. in accordance with certain risk categories. Based on the category, certain measures need to be taken (and in some cases, the particular AI system may not be operated at all). "Self-assessment" means that the responsible person must proactively assess the risk category in accordance with the criteria specified in the AI Act and apply the required measures for the

relevant risk category. Violations of the AI Act will result in fines imposed by competent authorities, but can also trigger other obligations, including the withdrawal of the AI system from the market. Except for limited situations, the AI Act does not deal with privacy and the processing of personal data through AI, nor with copyright issues or liability for the outcome produced by AI.

Broad Scope of Application

The AI Act applies not just to providers, importers, distributors, and manufacturers of AI systems but also to deployers of AI systems, i.e., a person or entity who uses or integrates an AI system (except for personal, non-professional use).

Additionally, the AI Act has a broad (extra-)territorial scope. Similar to other EU regulations in the digital context, the AI Act covers companies or individuals based in the European Union or who offer services on the EU market. But the AI Act goes one step further: It covers third-country providers and deployers of AI systems, even if only the output produced is used in the European Union. How this far-reaching regime will be enforced remains to be seen.

Prohibited AI Practices

The AI Act prohibits certain AI practices outright, reflecting use cases that are particularly related to fundamental rights, such as

- systems for the evaluation/classification of persons based on their social behaviour or personality characteristics ("social scoring");
- systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; and
- biometric categorisation systems and real-time biometric identification systems in publicly accessible spaces for the purpose of law enforcement (except for certain enumerated purposes such as the search for specific victims of abduction).

These practices will be prohibited as of Feb. 2, 2025.

High-Risk AI Systems

The AI Act also sets out a framework for so-called high-risk systems, which include safety-critical systems that are either embedded in certain product categories (as set out in Annex I of the AI Act) or stand-alone systems intended to be used in critical infrastructures, employment, law enforcement, or judicial and democratic processes (as set out in Annex III). The classification of high-risk systems follows a complex framework and may be ambiguous.

All AI applications classified as high-risk systems must be registered in a database maintained by the EU Commission before being made available. Moreover, they are subject to an extensive compliance mechanism that establishes legal requirements with regard to

- risk management;
- data and data governance;
- technical documentation;

- record keeping;
- transparency;
- human oversight; and
- accuracy, robustness, and cybersecurity.

The obligations regarding high-risk AI systems will apply from Aug. 2, 2026.

General Purpose AI Models

The AI Act introduces separate requirements for general purpose AI (GPAI) models, defined as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

In this context, it is important to note that the GPAI-related obligations only apply to providers of GPAI models (e.g., a large language model) and not to providers or deployers of "downstream systems" that implement such model (e.g., a chatbot).

GPAI model providers must keep technical documentation up to date and make it available to competent authorities on request (including training and testing procedures and the results of their evaluation). They will also be required to make publicly available a detailed summary of the content used for training the GPAI model and to implement a policy to comply with EU copyright laws.

If GPAI models develop systemic risks (which is presumed when the cumulative amount of computation used for the training measured in floating point operations (FLOPs) is greater than 10^25), the provider must notify the EU Commission within two weeks and must comply with further obligations such as performing model evaluations, making risk assessments, taking risk mitigation measures, and ensuring an adequate level of cybersecurity protection.

The GPAI regulatory framework will apply from Aug. 2, 2025.

Transparency Obligations

If AI systems are intended to interact with human beings, and unless this is "obvious from the circumstances and the context of use," their provider must inform these users that they are interacting with an AI system. Similarly, deployers of emotion recognition systems, biometric categorisation systems, and systems that generate "deep fakes" must inform the people exposed thereto of this interaction.

The transparency obligations will apply from Aug. 2, 2026.

AI Literacy

The AI Act provides that both providers and deployers of AI systems must take measures to ensure a sufficient level of AI literacy of their staff and other persons involved in operating AI systems on their behalf. The measures depend on various criteria, such as the technical knowledge, experience, education, and training of the individuals involved, as well as the context in which the AI systems will be used.

The AI literacy requirement will apply from Feb. 2, 2025.

Sanctions

The AI Act provides for noncompliance penalties designed to be "effective, proportionate, and dissuasive." If a party engages in a prohibited AI practice, a fine of up to EUR 35 million or 7% of worldwide annual turnover (whichever is higher) may be imposed. Failure to comply with other AI Act obligations can lead to fines of up to EUR 15 million or 3% of annual turnover.

Moreover, the EU Market Surveillance Regulation (EU 2019/1020) is incorporated into the AI Act's sanction mechanism, which may result in a number of actions in the event of noncompliance, including an enforceable obligation to withdraw AI systems from the market.

Regulatory Enforcement

To ensure consistent implementation and enforcement of the AI Act across the European Union, several authorities and bodies at both the EU and national levels are being set up. A key player at the EU level is the AI Office, established in January 2024. The AI Office is central to the AI Act's enforcement, particularly in overseeing GPAI models. It is empowered to evaluate GPAI models, request data from providers, and enforce corrective measures. Further, the EU Commission and the AI Office will play an integral role in drawing up codes of practice, guidelines, and implementing acts essential for the AI Act's practical application.

At the national level, the AI Act requires each EU member state to designate at least one notifying authority and one market surveillance authority to ensure compliance with the AI Act. Some member states have already shared their (initial) plans: In Germany, the Federal Network Agency (Bundesnetzagentur) will take a leading role in market surveillance. Spain established the Spanish Agency for Monitoring Artificial Intelligence (AESIA) in anticipation of the AI Act, and Denmark designated the Danish Agency for Digitisation as the national supervisory authority within the AI Act framework.

Compliance Strategies and Next Steps

As the AI Act sets out a complex and far-reaching regulatory framework, businesses across virtually all sectors should consider taking proactive measures to assess their AI practices and enhance compliance. Investments in AI governance may help enable organizations to navigate the fast-evolving regulatory landscape and establish a competitive advantage. Companies may consider taking the following next steps:

Impact assessment: Companies should understand what specific regulatory impact the AI Act will have on their business. Essential questions to address at this stage include:

- AI inventory and applicability of the AI Act: Which AI driven systems are (or will be) used, developed, or placed on the market? Does the system in question qualify as an AI system within the scope of the AI Act?
- What is the organization's regulatory role? Is it acting as provider, deployer, importer, distributor, or product manufacturer of AI systems?
- Which risk category applies (prohibited AI practice; high-risk system; transparency risk)?

Implement compliance mechanisms: Organizations should consider designing, implementing, and maintaining tailored compliance mechanisms based on the organization's role and the applicable risk category. A pragmatic compliance strategy should consider not only the specific regulatory impact but also the organization's size, culture, and overall approach to managing compliance risks.

Monitor regulatory landscape: The AI Act's regulatory framework will be further defined by guidelines, codes of conduct, and implementing acts. These documents are important for understanding the AI Act's detailed requirements and enhancing compliance (e.g., for GPAI models, a finalized code of practice is expected by April 2025).

Policy engagement and dialogue with regulators: Businesses, particularly those dealing with high-risk systems and GPAI models, should consider engaging in the European Commission's ongoing consultations. Early involvement may offer insights into future regulatory developments and shape the creation of guidelines. Engaging in dialogue with regulators and market surveillance authorities can also help companies understand enforcement strategies and design a pragmatic compliance approach.

Outlook

In this transformative era of AI regulation, the EU AI Act represents both a challenge and an opportunity for businesses to redefine their AI strategies. Embracing a pragmatic regulatory approach may help to foster innovation while minimizing compliance risks.

Authors

This GT Alert was prepared by:

- Dr. Viola Bensinger | +49 30.700.171.150 | Viola.Bensinger@gtlaw.com
- Dr. Paul Dürr | +49 30.700.171.151 | Paul.Duerr@gtlaw.com

not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2024 Greenberg Traurig, LLP. All rights reserved.