GT GreenbergTraurig

Alert | Innovation & Artificial Intelligence

March 2024

EU Artificial Intelligence Act – EU Parliament Adopts Groundbreaking Regulatory Framework

The European Parliament has adopted the Artificial Intelligence Act (AI Act). While the AI Act still requires adoption by the EU Council before taking effect, this is considered a formality given the lengthy trilogue negotiations that resulted in the current version. The AI Act creates a comprehensive legal framework for AI systems. It follows a risk-based approach, prohibiting some types of AI use cases outright and establishing a complex compliance mechanism for high-risk systems. It also introduces specific provisions for general purpose AI models. The AI Act has a broad scope and may affect businesses worldwide and across virtually every sector.

On 13 March 2024, the European Parliament adopted the AI Act. Since the EU Commission presented its first draft almost three years ago, the use of AI and general purpose AI models has increased significantly. Hence, the regulatory proposal was (and still is) the subject of hefty debate.

The AI Act relies on self-certification of AI systems by their manufacturers, providers, deployers, etc. into certain risk categories. Based on the category, certain measures need to be taken (and in some cases, AI systems may not be operated at all). "Self-certification" means the responsible person assesses the risk category in accordance with the criteria provided by the AI Act and applies the required measures for the relevant risk category. The AI Act also includes certain conformity assessment procedures that integrate the existing EU conformity assessments. Violations of the AI Act will result in fines by competent national authorities, but can also trigger obligations to withdraw AI from the market. Other than may be expected,

the AI Act does not (except for limited situations) deal with privacy and the processing of personal data through AI, nor with copyright issues or liability for the outcome produced by AI.

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. It is not yet clear whether the AI Act will be able to fulfil these goals. What is certain, however, is that the Act sets an extensive regulatory framework which will be relevant across multiple business sectors.

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 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 whose services are offered 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. It remains to be seen how this broad-reaching regime will be enforced.

Prohibited Artificial Intelligence Practices

The AI Act follows a risk-based approach. Certain AI practices are outright prohibited, 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).

High-Risk AI Systems

The AI Act also sets out a comprehensive framework for so-called high-risk systems. These include safety-critical systems or systems intended to be used in critical infrastructures, employment, law enforcement, or judicial and democratic processes. However, the classification of high-risk systems follows a complex framework and may be ambiguous.

All AI applications classified as high-risk systems need to be registered, before being made available, in a database kept by the EU Commission, and 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.

General Purpose AI Models

Separate requirements have been introduced for general purpose AI (GPAI) models. A GPAI model is defined as "an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform 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."

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 adhering to EU copyright law.

If GPAI models develop systemic risks (which is presumed when the cumulative amount of compute used for the training measured in floating point operations (FLOPs) is greater than 10^25), the provider is required to 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.

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, manufacturer, deployer, etc. must inform these users that they are interacting with an AI system. Similarly, users of emotion recognition systems or biometric categorisation systems must inform the people exposed thereto of this interaction.

Sanctions

The AI Act provides for significant noncompliance penalties, which are designed to be effective, proportionate, and dissuasive. If the prohibition of AI practices is disregarded, a fine of up to €35 million or 7% of worldwide annual turnover (whichever is higher) may be imposed. Noncompliance with several other AI Act obligations will be subject to fines of up to €15 million or 3% of worldwide 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 non-compliant AI systems from the market.

At the same time, EU member states are obliged to establish regulatory sandboxes to promote the development of AI in the European Union.

Next Steps

The AI Act awaits formal endorsement by the EU Council. If approved, it will enter into force 20 days after its publication in the official Journal and be fully applicable 36 months thereafter. However, certain provisions will apply earlier (e.g., bans on prohibited practices will take effect six months after entry into force, and GPAI rules will take effect 12 months after entry into force).

Authors

This GT Alert was prepared by:

- Dr. Viola Bensinger | +49 30.700.171.150 | viola.bensinger@gtlaw.com
- Carsten Kociok | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- Paul Dürr | +49 (0) 30.700.171.151 | paul.duerr@gtlaw.com