WRITTEN BY

OLIVER GÖNDÖR
Associate
CMS Slovakia

NAVIGATING THE AI ACT

Artificial Intelligence (AI) is revolutionizing industries and companies, offering unprecedented opportunities for innovation and growth. However, as AI technologies advance rapidly, concerns about their legal and ethical impact and risks have become increasingly prominent.

In response to these challenges, EU has embarked on an attempt to establish a comprehensive regulatory framework for AI, as we articulated in our Digital Regulation Hub. The CMS Digital Regulation Hub is home to the Digital Regulation Tracker Tool, which provides an overview of the key regulatory instruments in the legal and industry sectors which are critical to decision-makers.

On 13 March 2024, the European Parliament approved the Artificial Intelligence Act. The Council is anticipated to officially approve the conclusive version of the AI Act in April 2024. The regulation will apply directly in member states without the need for them to implement it into their national legislation.

WHAT IS THE SCOPE OF APPLICATION?

The regulation should affect member states' competences in national security and areas beyond EU law. Military and defense systems are excluded, as are AI systems used solely for research, innovation, or non-professional purposes.

WHAT IS THE GENERAL PRINCIPLE OF THE NEW REGULATION?

The regulation adopts a risk-based approach, imposing stricter rules on AI systems with higher risks to rights and freedoms. It categorizes AI into high and limited risk categories.

High-risk AI, posing significant threats to fundamental rights, is prohibited, with some exemptions for law enforcement. Such high-risk AI systems include social scoring based on personal behavior and characteristics, those enabling biometric identification and categorization of people in real time, and remote biometric identification systems such as facial recognition.

Stringent obligations are imposed on AI systems such as recruitment and HR tools, and medical and health monitoring devices, which are classified as high risk due to the risk of significant harm to fundamental rights, rule of law, health, or the environment. These obligations include mandatory impact assessments on fundamental rights, conformity assessments, data governance, risk, cybersecurity and quality management, human oversight, transparency and accuracy, and registration in an EU database.

AI systems with limited risk must meet transparency requirements to ensure that users are informed when interacting with them.

WHAT ABOUT THE FOUNDATION MODELS AND GENERAL-PURPOSE AI SYSTEMS?

A general-purpose AI (GPAI) is an AI model that includes extensive training with large datasets. These models are competent for performing tasks such as writing a poem, a recipe, or sharing a transfer deed. In addition, these models can be integrated into various apps or systems. This definition excludes AI models utilized solely for research, development, and developing prototypes before market release.

GPAI model providers should start to prepare for the new regulation by compiling technical documentation on training and testing processes, summaries of the training data used, implementing a policy to adhere to the Copyright Directive, and preparing documentation for downstream providers intending to integrate a GPAI model.

In addition, more obligations should apply to GPAI models that pose a systemic risk, e.g. conducting evaluations of models as well as evaluating and mitigating potential systemic risks, including identifying their origins, and monitoring, documenting and reporting significant incidents and potential corrective actions to the competent authorities.

WHO WILL BEAR THE OBLIGATIONS?

The primary responsibility for meeting the obligations rests with the providers, or developers, of high-risk AI systems irrespective of whether they operate in the EU or in a third country. Entities that intend to introduce high-risk AI systems to the market or deploy them for use in the EU must comply with the AI Act, irrespective of whether they operate within the EU or in a third country. Additionally, providers from third countries are included in the scope of regulation if their high-risk AI systems' output is utilized in the EU.

ARE THERE ANY SANCTIONS FOR NON-COMPLIANCE WITH THE RULES?

Based on the provisional agreement, a failure to comply with the regulations will result in fines ranging from EUR 7.5 million or 1.5% of global turnover, to EUR 35 million or 7% of global turnover, depending on the violation and the company's size. Civil claims arising from non-compliance that cause harm to individuals are not sanctions by nature, but settling such claims might be expensive.

WHEN WILL THE AI ACT COME INTO FORCE?

The final text of the AI Act is expected to be published in the Official Journal of the European Union in Q2 2024 after final formal approval by the Council and the completion of legal-linguistic revisions on the AI Act. Then the legislation will be published in the Official Journal of the EU and enter into force 20 days after publication. The AI Act will become effective two years after its entry into force. Certain provisions (prohibited AI systems) will take effect within six months, with regulations concerning GPAIs coming into force within 12 months.

HOW SHOULD I PREPARE FOR IT?

It is worth training your staff on the proper use of freely accessible AI tools and adopting a code of conduct for using AI tools in your organization. These two straightforward solutions can protect your organization from unexpected questions from customers regarding employees' tasks performed by AI or even copyright infringement disputes. In addition, your employees could perform certain work via freely accessible generative AI models.

SUMMARY OF THE PRACTICAL STEPS TO TAKE BEFORE THE AI ACT COMES INTO FORCE:

- Mapping where AI is or could be used in your organization.
- Assessing gaps between current policies and new requirements, and analyzing dataset biases, data governance plans, and transparency requirements.
- Establishing a comprehensive AI governance framework, including cyber security officers, data protection officers, and internal risk managers.
- Concluding bulletproof contracts to safeguard against suppliers' misuse of AI systems.

CMS Digital Regulation Tracker Tool provides an overview of the key regulatory instruments in the legal and industry sectors:

https://cms.law/en/svk/publication/digihub