WT Client Alert

AI Act – new rules for tech companies

The adoption of the Artificial Intelligence Act means a wide range of responsibilities for tech businesses in the European Union. This article guides through the new regulatory framework and its practical implications.

21 March 2024

On 13 March 2024, the European Parliament adopted the AI Act – **landmark EU legislation comprehensively addressing all issues connected with the regulatory framework of artificial intelligence**.

The AI Act is poised to take full effect within 24 months of its publication, presumably in late 2026. However, the ban on AI systems posing an unacceptable risk will be enforced within 6 months – potentially **during 2024**! Additionally, the rules regarding general purpose AI systems will become applicable within 12 months, likely in mid-2025.

What is the AI system?

The AI Act will apply to **AI systems**, which are defined as ***machine-based*** *systems designed to operate with varying levels of* ***autonomy****. These systems may exhibit* ***adaptiveness*** *after deployment and for explicit or implicit objectives, infer, from the input they receive, how to* ***generate outputs*** *such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*.

> The broad definition of AI systems makes the **scope of application of the AI Act very flexible**, covering not only software products, but also all other tools, hardware or solutions that could be qualified as autonomous systems that can learn and make conclusions regarding new situations based on the input data previously delivered to them. Additionally, this broad definition makes the AI Act applicable not only to AI products as such, but also to any other products or solutions that use AI components.

Who is subject to it?

The AI Act applies to entities dealing with AI systems, above all :

- **providers** – entities developing AI systems and placing them on the market or putting them into service under their own brand;
- **deployers** – entities using AI systems under their own authority.

However, the AI Act also applies to further types of entities such as **importers, distributors and authorised representatives**.

Prohibited AI systems

The AI Act presents a risk-based approach and applies different requirements to different categories of AI systems depending on how they impact individuals (natural persons affected by the given AI system).

The first category refers to **prohibited AI systems** that pose an unacceptable risk. Prohibited AI systems include, with some exceptions, for example:

- systems deploying **subliminal, manipulative or deceptive techniques** affecting individuals making informed decisions;
- **social scoring** systems leading to detrimental or unfavourable treatment;
- **facial recognition** systems using untargeted scraping of facial images from the internet or CCTV footage;
- **emotion recognition** systems in the areas of workplace and education institutions;
- certain **biometric categorisation** systems;
- certain **real-time remote biometric identification** systems.

High-risk AI systems

The core category of the AI Act is that of **high-risk AI systems**, i.e., systems that may pose a significant risk of harm to the health, safety or fundamental rights of natural persons.

According to the AI Act, high-risk AI systems are **those covered by the EU product safety legislation**, as well as systems categorised, but not limited to, as follows:

- AI systems used in **critical infrastructure**;
- AI systems intended for **education and vocational training**;
- AI systems for **employment**, workers management and access to self-employment;
- **law enforcement** AI systems;
- **migration, asylum and border control** management systems.

The list of high-risk AI systems is not exhaustive, meaning that sample categories of high-risk AI systems may be supplemented in the future and aligned with technology trends.

Apart from high-risk AI systems, the AI Act also refers to other medium- or low-risk AI systems.

Obligations for high-risk AI systems

Providers and/or deployers of high-risk AI systems will face a chain of obligations, such as:

- implementation of **risk management systems** throughout the entire lifecycle of the high-risk AI system; this comprises among other things the identification and analysis of the known and reasonably foreseeable risks, as well as the adoption of targeted risk management measures;
- implementation of adequate **data governance mechanisms** – to ensure that the data used for training, validating and testing AI models is suitable for the intended purpose and of appropriate quality;

- drawing up and maintaining detailed **technical documentation** of the AI system;
- equipping the systems with **record-keeping functionalities** for the automatic logging of events during the operation of the AI system;
- maintenance of **human oversight** over the AI system;
- maintenance of an appropriate level of **accuracy, robustness and cybersecurity** of the AI system;
- implementation of **quality management systems**;
- performing **impact assessments** or **conformity assessments** for certain categories of AI systems;
- implementation of **post-market monitoring** – for the purpose of collecting and analysing AI system data;
- **registration** obligations in EU database;
- **information/transparency obligations** towards individuals affected by the AI system.

General purpose AI

Apart from the standard AI systems, the AI Act also defines a separate category: **General-purpose AI system (GPAI)**. This is a system of a general nature that can be used in a wide range of downstream systems or applications.

> GPAI includes AI models that can perform a variety of tasks, are general-purpose and usually learn autonomously from large amounts of data and may be used in a wide range of applications.

Under the AI Act, GPAI faces a separate set of requirements, particularly relating to:

- implementation of detailed **technical documentation** of the model;
- implementation of specific **policies to respect copyright laws**;
- making available “sufficiently detailed” **summaries of the content of training datasets**;
- **labelling obligations** towards AI-generated or manipulated content.

Sanctions for non-compliance

Depending on the type of violation and the size of the company, the AI Act brings severe sanctions for non-compliance. Breach of the AI Act prohibitions may result in fines of up to **EUR 35 million** or **7% of total worldwide annual turnover**, while t**he** failure to meet the obligations set out for high-risk AI systems may incur penalties of up to **EUR 15 million** or **3% of total worldwide annual turnover**.

Broader legal framework

Although the AI Act primarily targets high-risk applications and GPAI, it is important not to overlook the broader spectrum of AI implementations. Businesses should thoroughly assess the deployment of all AI technologies within their operations, as well as review those already functioning prior to the adoption of the AI Act, ensuring compliance not only with the AI Act, but also with existing legal frameworks. This includes privacy and data protection issues governed under the GDPR, as well as adherence to intellectual property, consumer protection and anti-discrimination laws, which apply to a wide array of AI systems.

What we can do for you

At Wolf Theiss we have more than 40 experts dealing with AI in 13 jurisdictions across the entire CEE/SEE region. We can advise you on all legal aspects relating to your AI-based or AI-driven product or solution. We are particularly well placed to:

- assist you in defining the scope of application of the AI Act to your organisation and your products;
- advise you on the preparation of your organisation for the regulatory requirements of the AI Act on the internal and external level;
- provide you with the full documentation required under the AI Act and other relevant legislation;
- represent you in all formal proceedings stemming from the AI Act;
- assist you in reaching full legal compliance with the regulatory requirements of the AI Act.

For more information, please contact:

Jakub Pietrasik
Counsel
Leading IP/TMT Warsaw

E jakub.pietrasik@wolftheiss.com
T +48 22 378 8969

Zuzanna Nowak-Wróbel
Associate

E zuzanna.nowak-wrobel@wolftheiss.com
T +48 22 378 8968

Julia Zuzanna Biedrzycka
Associate

E julia.biedrzycka@wolftheiss.com
T +48 22 378 8985