LEGAL ALERT

# The EU Artificial Intelligence Act

ČECHOVÁ & PARTNERS
advokáti attorneys

The Artificial Intelligence Act (the "**AI Act**") as a legal framework regulating the using artificial intelligence in the European Union, aims to enhance the internal market's functionality and boost the adoption of AI technologies that are both human-centric and trustworthy.

# I. INTRODUCTION

The scope of the AI Act includes creating a uniform legal framework for the development, deployment, and use of artificial intelligence systems within the European Union. It aims to promote the uptake of AI that is both human-centric and trustworthy, while also ensuring a high level of protection for health, safety, and fundamental rights, including democracy, the rule of law, and environmental protection through a clearly defined risk-based approach. This novel regulation is designed to support innovation and prevent fragmentation in the internal market of the European Union by standardising requirements and setting proportionate obligations on all value chain participants.

The AI Act neither covers areas beyond the jurisdiction of EU law nor it impacts the authority of Member States regarding national security. Additionally, it does not interfere with how Member States delegate responsibilities related to national security, regardless of the entity involved.

Non-compliance with the AI Act's requirements may lead to administrative penalties as high as EUR 15 million or 3% of a company's total worldwide annual turnover. For violations involving prohibited AI systems, fines can reach up to EUR 35 million or 7% of the company's total worldwide annual turnover for the previous financial year, depending on which amount is greater.

### Time is ticking

The AI Act will enter into force 20 days after its official publication in the Official Journal of the European Union and will take effect gradually.

Provisions related to prohibited AI systems shall apply from 6 months after the AI Act enters into force. Other key provisions on GPAI models, governance, confidentiality, reporting to authorities, as well as penalties, shall apply within 12 months. The remaining part of the AI Act will take effect either 24 months from the date of entry into force or 36 months for certain provisions related to high-risk AI systems under EU product safety regulation. The AI Act is expected to be published in the Official Journal of the EU before the end of Q2 2024.

* * *

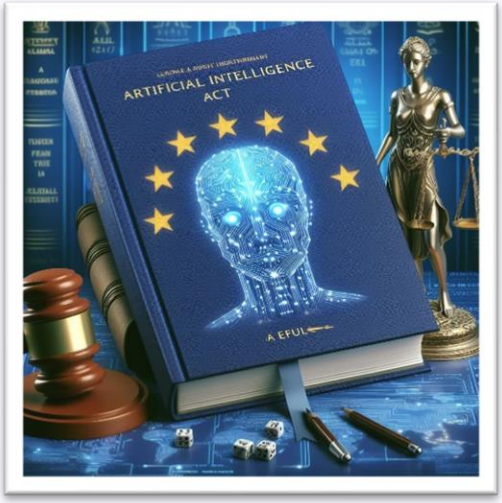
Therefore, a primary objective of this Legal Alert is to help understand some key features of the AI Act regulation to enable businesses to prepare early and efficiently for the practical implementation of the AI Act.

## II. SCOPE OF APPLICATION

The AI Act applies to:

- ✓ Providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the EU (whether located in the EU or not);
- ✓ Deployers of AI systems established or located in the EU;
- ✓ Providers and deployers outside the EU, where the output of the AI system is used in the EU;
- ✓ Importers and distributors of AI systems;
- ✓ Product manufacturers placing on the market or putting into service an AI system along with their product;
- ✓ Authorised representatives of providers established outside the EU;
- ✓ Affected persons located in the EU.

## III. KEY DEFINITIONS




The basis of the AI Act is the definition of an artificial intelligence system.

**Artificial intelligence system** ("**AI system**") is a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

**General-purpose AI model** ("**GPAI model**") is 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, except for AI models that are used for research, development or prototyping activities before they are released on the market.

**General-purpose AI system** ("**GPAI system**") means an AI system which is based on a general-purpose AI model, that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

**Risk** means the combination of the probability of an occurrence of harm and the severity of that harm.

## IV. SUPPLY CHAIN

**PROVIDER**
a natural or legal person, public authority, agency or other body that develops an AI system or a GPAI model or that has an AI system or a GPAI model developed and places it on the market or puts the AI system into service under its own name or trademark;

**DEPLOYER**
a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;

**IMPORTER**
a natural or legal person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country;

**DISTRIBUTOR**
a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market;

**AUTHORISED REPRESENTATIVE**
natural or legal person located or established in the EU who has received and accepted a written mandate from a provider of an AI system or a GPAI to, respectively, perform and carry out on its behalf the obligations and procedures established by AI Act.

## V. CRITERIA

The AI Act adopts a risk-based approach to the regulation of AI systems.

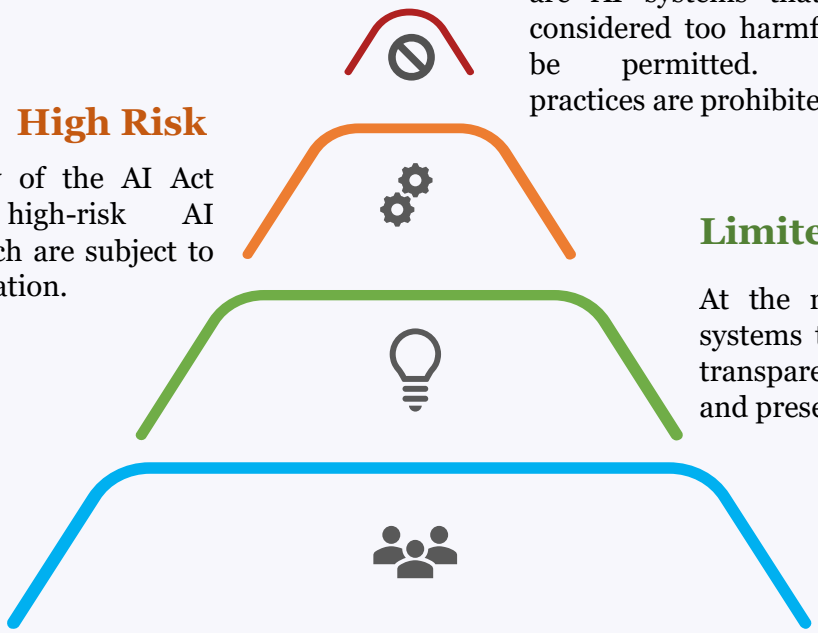
This approach imposes regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety. For other non-high-risk AI systems, only very limited transparency obligations are imposed.

### Unacceptable Risk

At the top of the pyramid are AI systems that are considered too harmful to be permitted. Such practices are prohibited.

### High Risk

The majority of the AI Act addresses high-risk AI systems, which are subject to strict examination.



### Limited Risk

At the next level, are AI systems that are subject to transparency obligations and present a limited risk.

### Minimal Risk

The broad base of the pyramid represents minimal risk AI systems. This category includes the majority of AI systems currently available in the EU single market. Minimal risk AI systems are unregulated.

## VI. PROHIBITED AI PRACTICES

The AI Act establishes a list of AI systems that are prohibited due to their unacceptable risk levels, encompassing those that clearly threaten security, employment, and fundamental rights, or otherwise contravene EU values by undermining the foundational principles upheld by the EU.

For example, prohibited AI practices include:

1) AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

2) AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

3) AI system for making risk assessments of natural persons in order to assess or predict the likelihood of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics;

4) AI system that creates or expands facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

5) AI system to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

6) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the objectives specified in the AI Act (e.g., targeted search for specific victims of abduction or missing persons, prevention of foreseeable threat of a terrorist attack, localisation or identification of a person suspected of having committed a criminal offence).

## VII. HIGH-RISK AI SYSTEMS

AI systems that negatively affect safety or fundamental rights are considered high-risk AI systems and are divided into two categories:

1) AI systems used in products covered by the EU's product safety legislation, as detailed in Annex 1 of the AI Act. This category includes, among other things, toys, aviation, cars, medical devices, and lifts.

2) AI systems falling into specific areas that must be registered in an EU database:

- Biometrics, in so far as their use is permitted under relevant EU or national law;
- Management and operation of critical infrastructure;
- Education and vocational training;
- Employment, worker management, and access to self-employment;
- Access to and enjoyment of essential private services and essential public services and benefits;
- Law enforcement;
- Migration, asylum, and border control management;
- Administration of justice and democratic processes.

### COMPLIANCE STANDARDS

These AI systems must comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before being placed on the EU market. Predictable, proportionate, and clear obligations are also placed on providers and users of these systems to ensure safety and respect for existing legislation protecting fundamental rights throughout the entire lifecycle of the AI systems. Requirements should apply to high-risk AI systems concerning the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy, and cybersecurity.

Providers of high-risk AI systems are mainly required to ensure compliance with specific regulations, maintain a quality management system, document technical details, manage system logs, conduct conformity assessments, register their systems, take corrective actions for non-compliance, inform relevant authorities, affix the CE marking, and demonstrate conformity to national competent authorities upon request.

# VIII. TRANSPARENCY OBLIGATIONS FOR LIMITED-RISK AND MINIMAL RISK AI SYSTEMS

## LIMITED-RISK AI SYSTEMS

For other, non-high-risk, AI systems, only very limited transparency obligations are imposed by the AI Act. This mainly concerns generative AI systems such as ChatGPT, Gemini, DALL-E, etc.

However, transparency obligations will apply for AI systems that:

- interact with humans,
- are used to detect emotions or determine association with (social) categories based on biometric data, or
- generate or manipulate content ("deep fakes").

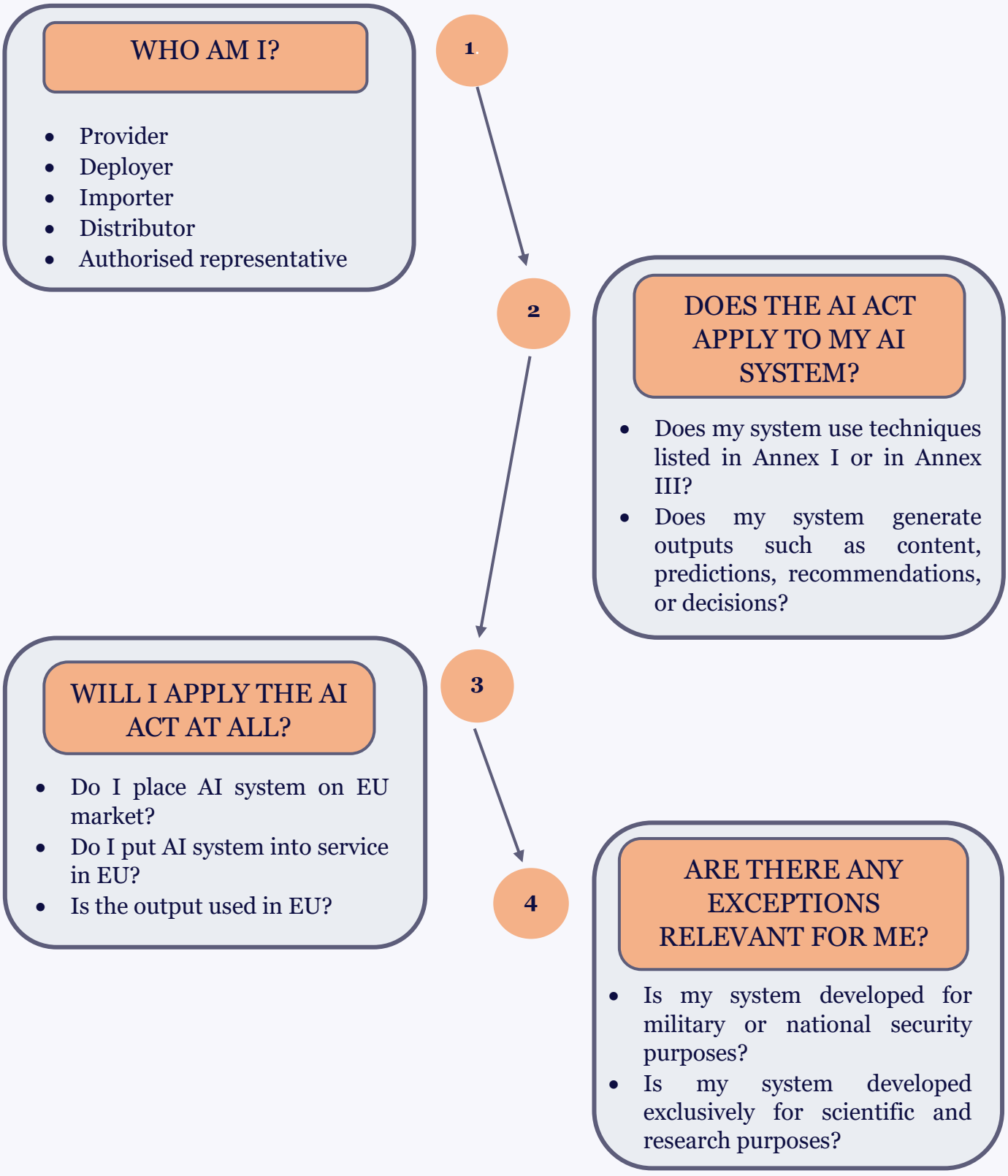
When persons interact with an AI system or their emotions or characteristics are recognised through automated means, people must be informed of that circumstance, i.e., an individual interacting with e.g., a chatbot must be informed that they are engaging with a machine so that they can make an informed decision on whether to proceed. If an AI system is used to generate or manipulate image, audio or video content that appreciably resembles authentic content, providers are obliged to clearly disclose that the content is generated through automated means, subject to exceptions for legitimate purposes (law enforcement, freedom of expression, etc.).

## MINIMAL-RISK AI SYSTEMS

The lowest level of risk described by the AI Act is a minimal risk, which is unregulated. This category includes all AI systems that do not fall under the previously mentioned categories, such as spam filters and AI-enabled video games.

The key aspect of this classification is that it seeks to minimize regulatory burdens on such low-risk systems, thereby promoting innovation and development in those areas where the risks associated with the use of AI are deemed negligible or even non-existent.

## X. NAVIGATING MAP
## or
## HOW SHOULD YOU PROCEED
## & WHAT ARE THE MAIN INITIAL CONSIDERATIONS?



* * *

This legal alert was prepared in May 2024 for general information purposes only and does not constitute a legal advice. The alert is not a comprehensive or exhaustive summary and provides only a brief and indicative summary of the material legislative rules.

All of the images above were created by a generative AI system.

For further information, specific assessment or legal advice on the AI Act, please do not hesitate to contact our specialised AI team colleagues Kristína Maschkanová, attorney (kristina.maschkanova@cechova.sk) and Simona Haláková, partner (simona.halakova@cechova.sk).