The EU Artificial Intelligence Act – Approval by the European Parliament

April 12, 2024 James Brown, Milad Amani

PRACTICES International, Europe, Middle East and Africa, AI and Deep Learning

The European Parliament on Wednesday 13 March 2024 approved the European Union's Artificial Act (the "**Act**"), being the world's first comprehensive piece of legislation aimed at the regulation of Artificial Intelligence ("**AI**").

Purpose

The Act's aim is to harmonise rules on AI systems in the EU by creating a common regulatory and legal framework to ensure these systems are safe, transparent and respect fundamental rights, while also establishing the EU as a hub for investment and innovation in the field of AI.

Who does it apply to?

Key to note is that the Act's reach extends well beyond parties that are located in the EU.

Title I of the Act defines various actors having association with AI applications (in a business capacity) that fall within its scope.

The definitions are broad and (though please see the Act for the precise definitions) extend to:

i. *providers* - broadly speaking those who have been primarily responsible for the development of an AI system or general-purpose AI model, and which have put it on to the market, whether they are established or located with the Union or a third country;

ii. *deployers* - broadly speaking, users of AI systems (in a professional context) having their place of establishment or who are located within the Union;

iii. provider and deployers of AI systems that have their place of establishment or who are located in a third country, where the output produced by the system is used in the Union;

iv. importers and distributors of AI systems;

v. product manufacturers who place on the market or put into service an AI system together with their product and under their own name or trademark;

vi. authorized representatives of providers, which are not established in the Union;

vii. affected persons that are located in the Union.

The above being so, it is key for commercial parties to consider now whether the Act is likely to apply to their activities.

The risk-based approach of the Act

The Act is a very substantial piece of legislation, and it is impossible within the limits of this briefing

to provide a detailed overview of its content of the obligations it imposes on parties. The intention is to provide more detailed briefings in due course.

However, at a high-level, the Act implements a risk-based approach to determining the obligations it imposes in respect of AI systems.

AI systems are classified based on the impact they may have on fundamental rights, democracy, the rule of law and environmental sustainability.

There are 4 classifications, i.e., unacceptable risk (which are prohibited), high risk, limited risk and minimal risk (which are not regulated).

The Act also provides for rules relating to general-purpose AI systems.

Prohibited applications of AI

Title II, Article 5 of the Act, lists a number of "artificial intelligence practices" which are prohibited. These include (but are not limited to):

i. systems that seek to manipulate the consciousness of persons by using subliminal techniques to persuade a person to make a decision they would not otherwise have made which causes or is likely to cause;

ii. systems that categorise people based on their biometric data to deduce certain characteristics about them or beliefs they may hold; and

iii. the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes save for in certain specified limited circumstances.

High-risk AI systems

Title III Chapter 1 of the Act provides rules for identifying when a system is a "high-risk AI system", with a substantial list provided at Annex III.

There is a "carve-out" from the classification for AI systems *"if they do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making"*.

Title III Chapter 2 of the Act provides for the *"Requirements for High-Risk systems"*. High risk AI systems must meet stringent requirements to ensure that they are trustworthy, transparent and accountable. The Act imposes obligations to conduct risk assessments and to maintain a risk management system, use high-quality data (when the system uses data for the purposes of training it), to produce technical documentation demonstrating that the system is complaint with the Act's requirements, produce and keep records of the system's performance, inform users about the nature and purpose of their systems, enable human oversight and intervention during use, and ensure accuracy and robustness.

Title III Chapter 3 of the Act is headed *"Obligations of Providers and Deployers of High-Risk AI Systems and other Parties"* and specifically provides for what providers, deployers, authorized representatives, importers and distributors must do. So, for example, Article 16 of Chapter 3 provides that providers of high-risk AI systems shall ensure that their high-risk AI systems meet the requirements of high-risk systems as set out in Chapter 2 of the Act, shall indicate their name, registered trade name or trade mark, and the address at which they can be contacted on the high-risk AI system (or if that is not possible then on its packaging or accompanying documentation) and

shall have in place a quality management system complying with Article 17 and shall keep certain documents as detailed in Article 18 (among many obligations).

Limited risk AI systems
AI systems deemed to have lower associated risk would be limited to oversight and transparency rules (i.e., informing users that they are interacting with an AI system) such as human oversight, keeping record and monitoring AI systems.

General-purpose AI systems
Title VIIIA of the Act relates to general-purpose AI models, providing for the circumstances in which such a system shall be regarded as having "systemic risk" (there being a presumption that that such a system has systemic risk when the cumulative amount of compute used for its training measured in floating point operations is greater than the measure specified in the Act at Article 51a 3), and then imposing certain obligations on providers of such systems distinguishing between those that have systemic risk and those that do not.

Fines:
The penalties for non-compliance with the Act are substantial:

- €35 million fine or, if the offender is a company, up to 7% of total worldwide annual turnover for the preceding financial year, whichever is higher, for violations of the rules on banned AI applications; and
- €15 million fine or, if the offender is a company, up to 3% of worldwide annual turnover for violations of certain of the AI Act's other key obligations; and
- €7.5 million or, if the offender is a company, up to 1% of worldwide annual turnover for the supply of incorrect, incomplete or misleading information to certain bodies specified under the Act.

By being proactive, businesses can mitigate against any potential sanctions.

Timing:
The Act is likely to come into force at around the end of May, but there will be a delay of 24 months before it becomes fully applicable save that:

i. the ban on prohibited applications will apply 6 months after the entry into force of the Act;

ii. the sections of the Act providing for penalties shall apply from 12 months following entry into force of the Regulations.

Mitigation of liability
Commercial entities should consider the extent to which they are engaged in the production, use or supply of AI models. Even if you are not currently doing so, it is likely that you soon will.

Parties should consider the development of a risk management system. A good starting point would be to work with your IT and risk department to understand your exposure to AI and to classify it according to the risk-classification system that is with the Act.

Businesses should think about putting in place appropriate contractual protections in relation to the use of AI systems (in particular appropriate warranties and indemnities to cover potential risks when procuring or providing AI systems).

The possibility of insuring against risk should also be explored.