# A Deep Dive into the EU AI Act

On 13 March 2024, the European Parliament held a landmark poll in which members voted convincingly to endorse the EU Artificial Intelligence Act (the "**Act**").

The Act is one of the first comprehensive legislative frameworks in the world to directly govern and regulate the use of artificial intelligence ("**AI**"). It goes further than the assortment of laws introduced by China in 2022-2023 and the executive order of President Biden in the US in October 2023. In the UK, although the government published the AI Regulation White Paper in March 2023 (see here) which set out its proposed AI regulatory framework, there is yet to be anything made statutory. Expectations, therefore, are that the rest of the world will follow in the EU Parliament's footsteps.

Significantly, the Act has extraterritorial ramifications and will affect providers beyond EU borders. AI systems that are being supplied, or used to generate an output that will be used, within the EU internal market will fall inside the scope of the provisions, even where that supplier or user of the AI system is located outside the EU.

Although there are still two years until the Act takes full effect (as certain parts of it will be implemented in phases such as the general purpose AI rules which will come into effect 12 months after entry into force), we recommend staying alert to the legislation to be prepared in case it affects your business.

## Purpose of the Act

The Act aims to make the EU a haven for users and developers of AI. By introducing comprehensive transparency requirements and obligations, users can be more certain that the AI they use is safe and will not exploit their fundamental rights and values. The Act seeks to balance innovation with protecting fundamental rights and safety, outlining rules for high-risk AI systems while fostering trust and accountability in AI development and deployment. In turn, it is hoped that this will create the optimal environment for innovation and, subsequently, attract investment.

## How Does the Act Define AI?

The Act's definition of an "AI System" is rather broad, but in essence an "AI System" is:

1. one that is 'machine-based' and 'designed to operate with varying levels of autonomy' (*Article 3(1)*); *and*

2. has a 'capability to infer' information 'from inputs or data' (*Article 12*).

## To Whom Does it Apply?

The Act applies to:

- providers and deployers of AI systems, even where their place of establishment is outside the EU, where the output produced by the system is used in the EU (*Article 6(1)(a) – (b)*);

- importers and distributors of AI Systems (*Article 6(1)(d)*); and

- product manufacturers who sell a product on the market, which uses an AI system, under their own name or trademark (*Article 6(1)(e)*).

'Providers' are those who develop AI systems and place this on the EU internal market (*Article 3(3)*) and 'deployers' are those persons who use an AI system (*Article 3(3)*).

The Act expressly provides that it does not apply to, amongst others, AI systems used for national security (*Article 2(3)*), scientific research (*Article 2(6)*), personal non-professional activity (*Article 2(10)*) or AI systems released under free and open-source licenses (*Article 2(12)*).

**The Regulatory Framework**

The Act aims to categorise AI based on its risk to cause harm. The obligations imposed vary depending on this categorisation. The categorisations are as follows:

1. **Prohibited AI Practices (*Article 5*)**

AI practices which fall within this category are considered to impose an unacceptable level of risk. This includes AI that, for example:

- uses purposefully manipulative or deceptive techniques with the objective or effect of distorting the ability of a person(s) to make informed decisions (*Article 5(1)(a)*);

- conducts a risk assessment on a person to assess their likelihood of committing a criminal offence and bases that assessment solely on the profiling of that person or their personality traits and characteristics (*Article 5(1)(d)*); or

- creates or expands facial recognition databases by using data of facial images which were randomly scraped from the internet or CCTV (*Article 5(1)(e)*).

2. **High-Risk AI Systems (*Articles 6-49*)**

AI systems will be considered 'high risk' if they are (a) intended to be used as a safety component of a product, or where the AI system itself is the product, and (b) that product is required to undergo a third-party conformity assessment (pursuant to union harmonisation legislation) before it can be placed on the EU internal market or put it into service (*Article 6(1)*). Furthermore, systems will also be considered high risk where they are intended to be used in critical infrastructures (such as energy or transport), to govern the success of applications to educational institutions or jobs, to be used in healthcare devices, or to be used in law enforcement or judicial proceedings (*Article 6(2) and Annex III*).

Before the AI system can be placed on the market or put into service, the provider will be required to register themselves and their system on an EU database, though this is yet to be set up by the European Commission (*Article 49 and 71*).

High risk AI applications are then subject to a raft of extensive operational requirements. Such requirements include the need to: establish a risk management system in relation to the AI system (*Article 9*); use high quality data sets to train the AI (*Article 10*); log the activities of the AI system (*Article 12*); provide clear instructions to users of the AI (*Article 13*); ensure that humans

oversee the AI (*Article 14*); and be designed in such a way that they are sufficiently accurate, robust and have effective cybersecurity (*Article 15*).

Where the AI system demonstrates compliance with harmonised standards as mentioned in Article 40, the provider will need to undergo an internal conformity assessment or a conformity assessment with the involvement of a notified third-party (*Article 43*). Where the provider has not applied these standards, the standards do not exist, or one of the common specifications in Article 41 are unavailable, they will need to undergo a third-party conformity assessment as detailed under Annex VII (*Article 43*).

### 3. Limited Risk AI Systems (*Article 50*)

Providers of AI systems intended to interact directly with natural persons must design them in such a way that a natural person is informed that they are interacting with an AI system (*Article 50(1)*).

For example, providers of AI that generate synthetic audio, images, video or text content must ensure that the outputs of the AI system are marked as artificially generated (*Article 50(2)*). Equally, deployers of AI systems that generate media constituting deep fakes must disclose that the content has been artificially generated (*Article 50(3)*).

The mark or disclosure, as referred to above, must be clear and distinguishable and must be provided to the natural person at the first stage of interaction with the AI or its output (*Article 50(5)*).

### 4. Minimal Risk AI Systems

AI systems which are considered 'minimal risk' (such as spam filters) are not subject to any form of restrictions or regulations under the Act. However, all operators of AI systems are encouraged to implement a Code of Conduct supporting ethical AI (*Article 95*).

### 5. General Purpose AI Models (*Articles 51-56*)

The Act differentiates between 'general purpose AI models' and 'general purpose AI models with systemic risk'. The obligations differ depending upon the categorisation.

#### a. General Purpose AI (*Article 53*)

A general-purpose AI model is an AI model that displays significant generality, is capable of competently performing a wide range of distinct tasks and which can be integrated into a variety of downstream systems or applications (*Article 3(63)*).

All providers of general-purpose AI models must comply with a set of obligations, which includes drafting and keeping technical documentation about the model, as well as making information available to downstream providers of AI systems who intend to integrate the general-purpose AI model into their AI systems (*Article 53(1)(a) and (b)*). Providers will also need to put in place a policy to comply with EU copyright law which respects holders of copyright who do not wish for their personal data to be used by general purpose AI models (*Article 53(1)(c)*). Finally, general purpose AI model providers must publish a summary about the content used in the training of the general purpose AI model using a template produced by the AI Office (*Article 53(1)(d)*).

### b. General Purpose AI Models with Systemic Risk

A general purpose AI model shall be classified as one with systemic risk if either: (a) it has high impact capabilities (determined using indicators and benchmarks); or (b) it is deemed, based on a decision of the EU Commission, to have high impact capabilities (*Article 51*). Where a general purpose AI model meets these requirements, the provider must notify the EU Commission within two weeks of the requirement being met or when it becomes known to have been met (*Article 52*).

In addition to the obligations in Article 53, providers of general purpose AI models with systemic risk must perform model evaluation in accordance with standardised protocols to identify and mitigate systemic risk as well as assess and mitigate possible systemic risks at EU level that may stem from development or use of these models (*Article 55(1)(a) and (b)*). Providers must also make available, to the AI Office and national competent authorities, information about serious incidents and measures that may be implemented to address them (*Article 55(1)(c)*). Finally, such providers must ensure that the general purpose AI model has adequate cybersecurity and physical infrastructure (*Article 55(1)(d)*).

**Enforcement**

Enforcement of the Act takes place at both a Union and member state level.

Each member state is required to select a market surveillance authority and a notifying authority as national competent authorities who must enforce the Act (save for in relation to GPAI with systemic risk) (*Article 70*).

GPAI with systemic risk will be supervised by the European Artificial Intelligence Office ('**AI Office**') which will sit within the EU Commission (*Article 53*). The AI Office must develop codes of practice to ensure the Act is properly implemented by providers of GPAI with systemic risk (*Article 56*).

Lastly the Act provides that an Artificial Intelligence Board shall be formed, made up of one representative from each member state (*Article 65*). The board is tasked with providing non-binding advice and sharing technical expertise to ensure the effective application of the Act throughout the EU (*Article 66*).

**Penalties**

If a person engages with any practice that falls within Article 5 (Prohibited AI Practices) they will be subject to a fine of up to €35,000,000 or, where the offender is a corporate entity, up to 7% of its worldwide annual turnover (whichever is higher) (*Article 99(3)*).

Non-compliance with other obligations under the Act, other than those set out in Article 5, will be subject to administrative fines of up to €15,000,000 or, where the offender is a corporate entity, up to 3% of its total worldwide annual turnover (whichever is higher) (*Article 99(4)*).

**Comment**

The Act is the first comprehensive regulation on AI by a major regulator anywhere. AI applications influence what information we see online by predicting what content is engaging to a consumer, capture and analyse data from faces to enforce laws or personalise advertisements, and are used to diagnose and treat cancer. In the long term, AI will affect many

parts of our lives and so SMEs and startups will need to stay abreast of their legal obligations under the Act (or use the Act as a benchmark standard until similar local laws are implemented) to illustrate trustworthiness and build consumer confidence.

**Roger Blears and George Jones**
**4 June 2024**