The EU's first attempt at regulating AI, the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) (the Act) entered into force on August 1st 2024.

Transition periods for companies will vary depending on the type of AI that is being used. Employer obligations related to prohibited AI applications will take effect on February 2nd 2025, with specific obligations applying to general-purpose AI models from August 2nd 2025.

However, the majority of obligations under the Act won't go into effect until August 2nd 2026. With high-risk systems outlined in Annex I of the AI Act coming into force on August 2nd 2027.

What counts as AI under the Act?

An AI System is a machine-based system designed to operate autonomously with varying levels of sophistication and with an ability to adapt after deployment, that can infer, from inputs received, outputs such as predictions, text, recommendations or decisions, to meet certain explicit or implied objectives.

A General Purpose AI Model – an AI model capable of competently performing a wide range of tasks regardless of the way the model is placed on the market and which can be integrated into a variety of downstream systems or applications. It does not include AI models used for research, development or prototyping before being placed on the market.

A General purpose AI System is an AI System based on a General-purpose AI model which has a wide range of purposes both direct and integrated in other AI Systems.

How does the Act categorize the AI risk?

It defines 4 categories of risk to the use of AI:

- **Unacceptable risks** – these will be banned in the EU – (e.g. biometric categorisation, social scoring, untargeted facial recognition and other)

- **High risk** – significant potential risk to human health, safety, fundamental rights, environment, rule of law (e.g. utility infrastructures, law enforcement, biometric identification and others) – for these risks there will be comprehensive mandatory compliance obligations

- **Limited risk** – where lower risk is assessed (e.g. using chatbots) – lesser transparency rules will apply, such as informing users they are using AI

- **Minimal/no risk** – free use is allowed but internal codes of conduct are encouraged (e.g. AI enabled recommender systems or spam filters)

Where and to whom does the Act apply?

It applies to both 'AI developers' and 'AI users', with most employers being in the 'user' category. The Act defines and distinguishes "providers", "distributors", "importers", "deployers" and "operators". Each category has compliance obligations under the Act.

While the EU Act applies only in the EU, it will catch providers of systems that are used in the EU, wherever they are located. It will also apply to AI systems located outside the EU, if the outputs are intended for use in the EU.

What are the overarching obligations on AI Users?

- **Responsibility for Compliance**: Particularly in sectors where high-risk AI applications are used (e.g. healthcare), companies must ensure that the AI systems they use comply with the regulatory requirements outlined in the EU Act.

- **Human Oversight**: In cases of some AI systems, it will be necessary to establish mechanisms for human oversight to monitor and intervene in the functioning of the AI system.

What is the penalty?

Under the Act employers that do not comply with its provisions will face fines of up to 35 million EUR or 7% of a company's annual turnover. Smaller violations can result in fines of up to 15 million EUR or 3% of an organization's annual turnover.

What should an Employing organisation do?

How do you prepare for a workplace revolution? Are you already using AI for staff hiring, training, monitoring, remuneration, assessment, promotion welfare or security?

All these uses will need to be assessed by employers under the 4 risk categories and appropriate compliant policies prepared and implemented.

Steps to take:

- **Conduct Risk Assessment and Compliance Strategies** - to identify potential pitfalls and develop proactive strategies to ensure adherence to the EU Act.

- **Develop a due diligence process for onboarding AI power tools** - to minimise compliance risks flowing from vendor shortcomings.

- **Create Ethical AI Policies** - aligned with the EU Act by assessing AI systems for biases, ensuring transparency in decision-making processes, and implementing robust mechanisms for accountability.

- **Prepare Training and Education Initiatives** - to facilitate compliance, particularly by raising awareness about potential biases, promoting responsible data handling practices, and emphasizing the importance of transparency. By fostering a well-informed workforce, companies can proactively mitigate legal risks and position themselves as responsible AI stewards.

- **Review your incident planning and business continuity processes** - to anticipate situations where AI systems will have to be turned off to deal with an immediate or persisting risk.

This is a high level general update only. Legal advice should be obtained on specific circumstances.