McCann FitzGerald

TRAINING & DEVELOPMENT PROGRAMME

Knowledge Network

AI Series

Decoding the AI Act
Navigating the Legal Landscape

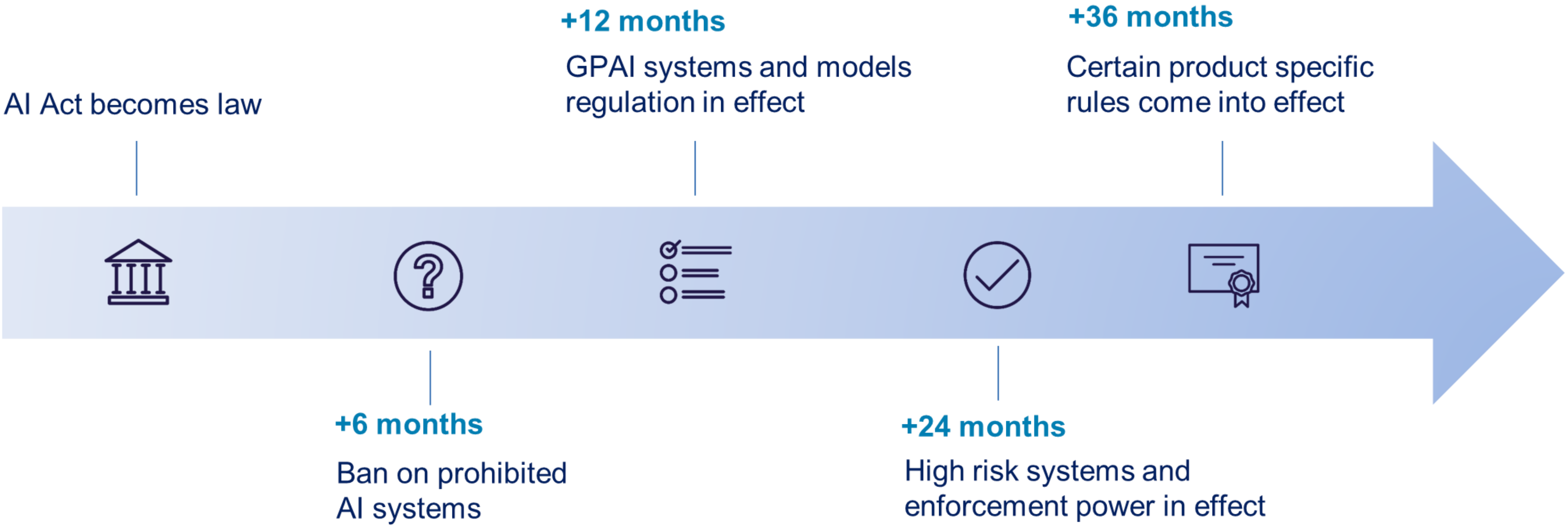
Wednesday, 1 May 2024 | 8.30 am to 9.30 am

Doug McMahon
Partner
+353 1 607 1459
Doug.McMahon@mccannfitzgerald.com

The AI Act – A Brief and potted history

- 1 October 2020 – The EU Council discusses AI and invites the EU Commission to draft regulations
- 21 April 2021 – The EU Commission proposes the AI Act
- 6 December 2022 – The EU Council agrees its position on the AI Act
- 9 December 2023 – The EU Council and European Parliament reach provisional agreement
- 13 March 2024 – The EU Parliament passes the AI Act

Timeline for Implementation



AI Act becomes law

+6 months

Ban on prohibited AI systems

+12 months

GPAI systems and models regulation in effect

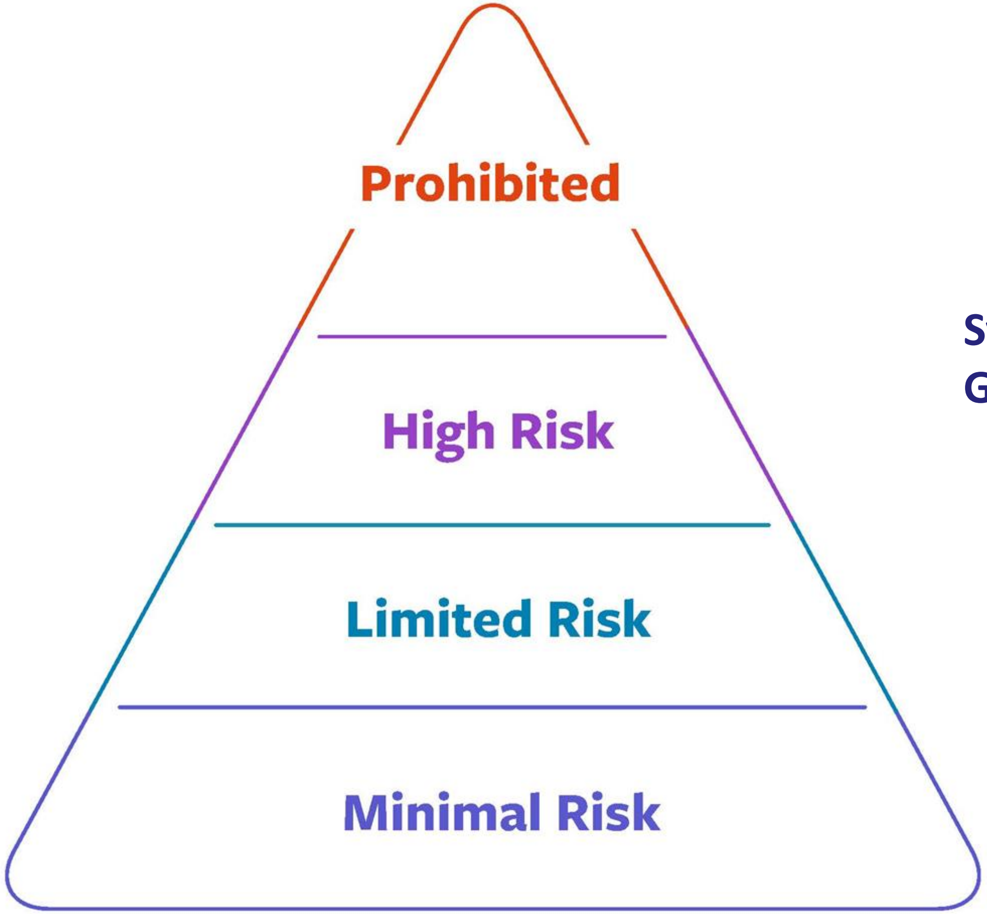
+24 months

High risk systems and enforcement power in effect

+36 months

Certain product specific rules come into effect

A Risk Based Approach



Systemic Risk –
GPAI Models

Some Terminology

AI system is “a machine-based system designed to operate with varying levels of autonomy and 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.”

Some Terminology

Provider “means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.”

Some Terminology

Deployer “means 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.”

Extra Territorial Effect

- The AI Act applies to:
  - Providers who place on the market or who put into effect AI systems or GPAI Models within the EU, regardless of whether they are established in the EU
  - Deployers of AI systems that have their place of establishment or are located in the EU
  - Providers and Deployers of AI systems that are established in a third country, but where output is used in the EU

Prohibited Practices

- Subliminal techniques, or purposefully manipulative or deceptive techniques, with the objective or the effect of:
  - materially distorting behaviour by appreciably impairing the ability to make an informed decision,
  - causing a person to take a decision that they would not otherwise have taken,
  - in a manner that causes or is reasonably likely to cause that person, another person, or group of persons, significant harm.
- Exploits vulnerabilities due to age, disability or specific social or economic situation, with the objective or effect of materially distorting the behaviour of that person in a manner that causes or is reasonably likely to cause that person, another person or a group of persons significant harm

Prohibited Practices

- The use of social scores that leads to either:
  - detrimental or unfavourable treatment of persons or groups in social contexts that are unrelated to the contexts in which the data was originally generated or collected
  - detrimental or unfavourable treatment of persons or groups that is unjustified or disproportionate to their social behaviour or its gravity
- Assessing or predicting the risk of a person committing a criminal offence, based solely on profiling or on assessing personality traits and characteristics

Prohibited Practices

- Inferring emotions of a natural person in the areas of the workplace or education institutions, except for medical or safety reasons

High Risk AI Systems

- The AI Act classifies some use of AI as "High Risk" e.g.
  - When used as a safety component of a product, or the AI system is itself a regulated product, and it is required to undergo third party conformity assessment
  - Certain uses of biometric systems
  - Use as safety components in the management and operation of critical infrastructure, including digital infrastructure
  - Certain uses for education and vocational training
  - Law enforcement, migration, asylum and border control management
  - Administration of justice

High Risk AI Systems - Employment

- AI systems intended to be used for the recruitment or selection of persons, including to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates
- AI systems intended to be used to make decisions affecting work-related relationships, promotions, allocation of tasks, and monitor and evaluate performance

McCann FitzGerald

High Risk AI Systems – Access to Services

- Use of AI systems by public authorities to evaluate the eligibility for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke or reclaim such benefits and services
- Use of AI systems to evaluate creditworthiness or establish a credit score, with the exception of fraud prevention
- Use of AI systems for risk assessment and pricing in relation to natural persons in the case of life or health insurance

Avoiding High Risk Categorisation

- An AI system is not considered high risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of a natural person, including by not materially influencing the outcome of decision making. In particular, an AI system will not be high risk where it:
  - Is intended to perform only a narrow procedural task;
  - Improves on an activity previously completed by a human;
  - Is intended to detect decision-making patterns but does not influence or replace decisions made by humans; and/or
  - Performs a preparatory task to an assessment relevant for the purposes of the non-product related uses cases for high risk AI systems.

High Risk AI Systems

- Obligations on providers of high-risk systems include:
  - Implement a risk management system
  - Data governance for training models
  - Technical documentation
  - Record keeping
  - Transparency
  - Human oversight
  - Accuracy, robustness and cybersecurity
  - Quality management systems
  - Conformity assessment

High Risk AI Systems

- Obligations on deployers of high-risk systems include:
  - Technical and organisational measures to ensure the use of such systems in accordance with the instructions for their use
  - Implement human oversight
  - Control input data and ensure relevant
  - Report issues/incidents to providers and relevant regulatory authority
  - Logs
  - DPIAs
  - Transparency
  - Fundamental Rights Impact Assessment

Limited Risk Systems

- Transparency obligations where the AI system interacts directly with natural persons
- Watermarking of AI produced synthetic audio, image, video or text content
- Disclosure of "deep fakes" and where AI generated or manipulated text is published for the purpose of informing the public on matters of public interest

General Purpose AI Models and Systems

- All GPAI models and systems must:
  - Draw up technical documentation for downstream providers
  - Comply with EU copyright law and disseminate detailed summaries about content used in training
  - Provide for watermarking AI generated or manipulated content
- GPAI models presenting systemic risk must:
  - Conduct model evaluations
  - Assess and mitigate systemic risks
  - Conduct adversarial testing
  - Report serious incidents
  - Ensure sufficient cybersecurity protection

Enforcement

- Enforcement will be complex, with a layered governance structure involving notifying and notified bodies, conformity assessment bodies, an AI Board, an AI Office, national competent authorities, and market surveillance authorities
- European Artificial Intelligence Office will be tasked with coordinating enforcement efforts, and certain tasks in relation to AI systems based on GPAI models
- No one stop shop mechanism
- Fines of up to 7% of annual worldwide turnover, but 3% and 1% are the maximum for most breaches

What should I do today?

- Audit current use of AI systems
- Identify the road map for use of AI systems in the organisation
- Make plans to cease using any AI systems that will be prohibited
- Identify responsibilities within the organisation for AI Act compliance
- Consider the compliance burden as part of budgetary planning activities

Questions?