# The EU AI Act

Decoding what we know so far, and actions business should take now.

**KPMG Ireland**
**kpmg.ie**

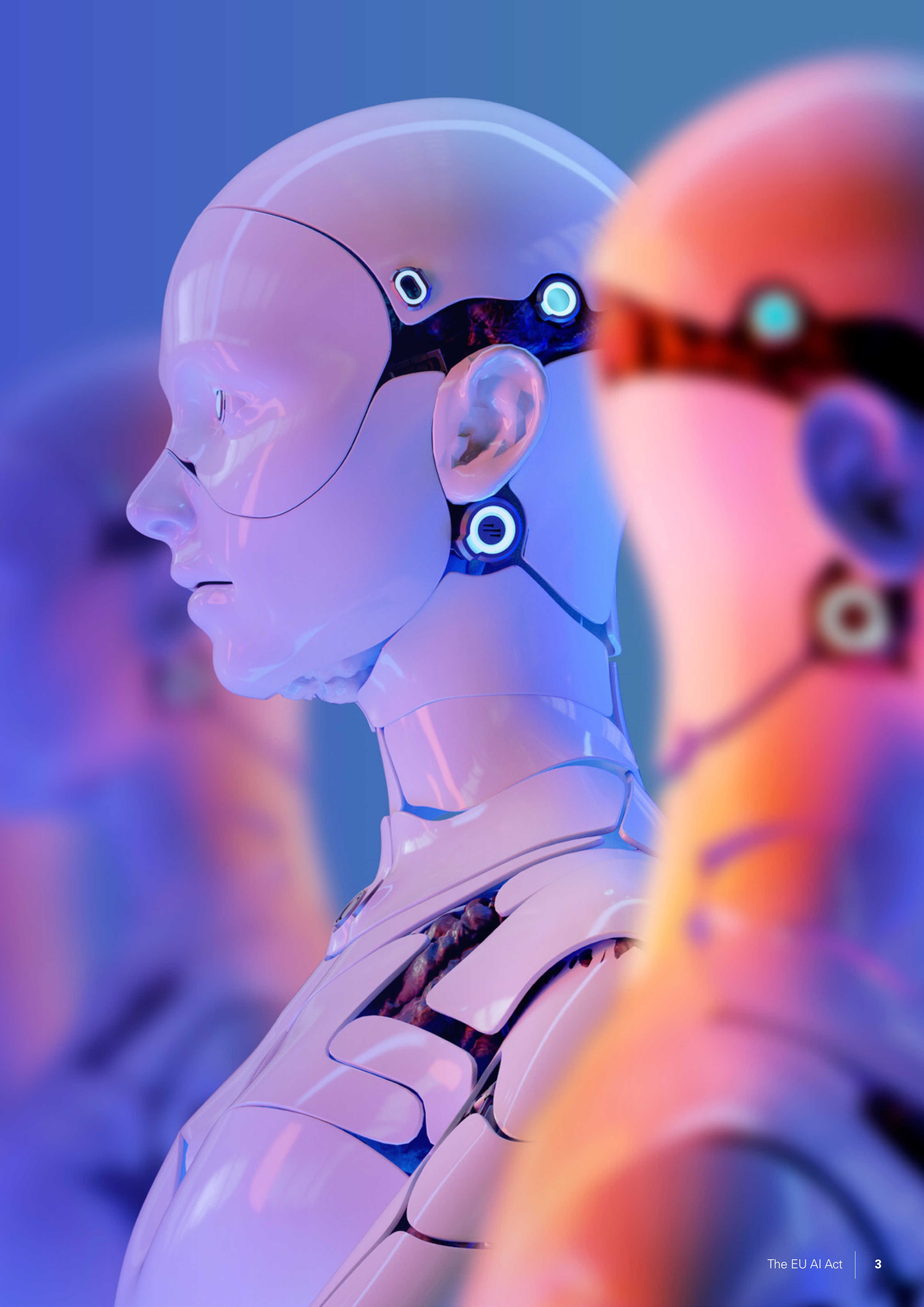
# Introduction

In December of 2023, European lawmakers announced a provisional agreement on the final text of a new AI Act. Subsequently, an unofficial text apparently representing the provisional agreement was leaked online, giving developers and users of AI systems the first chance to consider in detail what the proposed new framework could mean for them. Businesses are now in a position to consider the role AI systems plays in their organisation and how to mitigate potential risks that may arise as a result of this new legislative advancement.

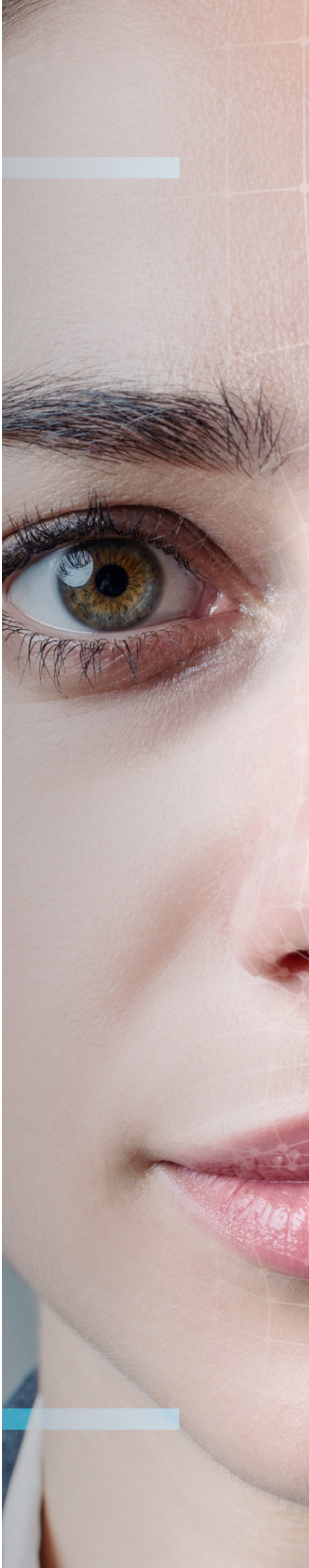
The Act represents a major overhaul for businesses that develop or deploy AI systems. This paper sets out the key developments of the AI Act and how it applies to business that either develop or deploy AI systems. A synopsis of these developments is detailed on pages 4-6, with additional detail included on page 7 onwards.

## The Definition of AI

An **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 content, predictions, recommendations, or decisions that can influence physical or virtual environments."



# The Act differentiates between three types of AI systems:



**Unacceptable risk AI systems,** these are systems considered to pose an unacceptable risk and are prohibited by the Act. These practices include systems that target vulnerable people or groups of persons, systems that materially distort a person's behaviour, the use of biometric categorisation and identification systems, and systems that classify natural persons that lead to unjustifiable detrimental treatment.

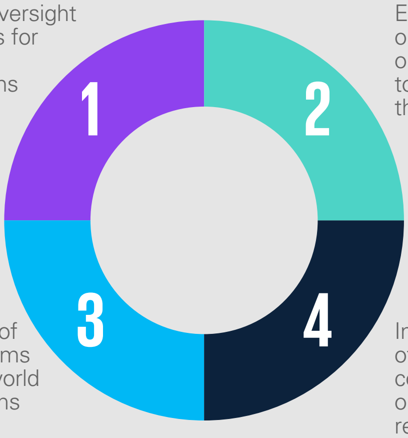
**High-Risk AI systems** are those where if based on their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence.

**A General Purpose AI System** is an AI model that displays significant generality and is capable to competently perform 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.

# How will the Act impact your business?

The Act will impact both developers and deployers of AI systems and will legislate the following:

## Key Figures



Human oversight measures for high-risk AI systems

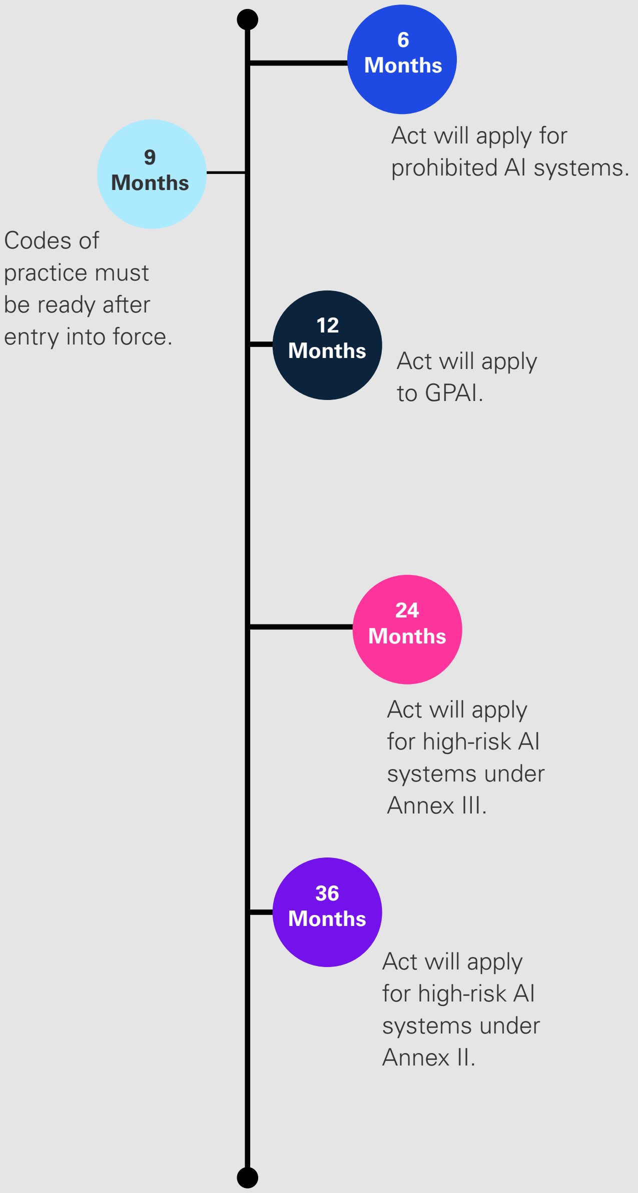
Effective employer obligations for organisations planning to deploy AI at the workplace

Testing of AI systems in real world conditions

Implementation of codes of practice for the proper compliance with the obligations of the regulation for providers of General-Purpose AI systems.

# What are the timelines?

It is expected that the EU AI Act will be subject to further negotiations at an EU level, but will be formally passed in law in early 2024.



6 Months

Act will apply for prohibited AI systems.

9 Months

Codes of practice must be ready after entry into force.

12 Months

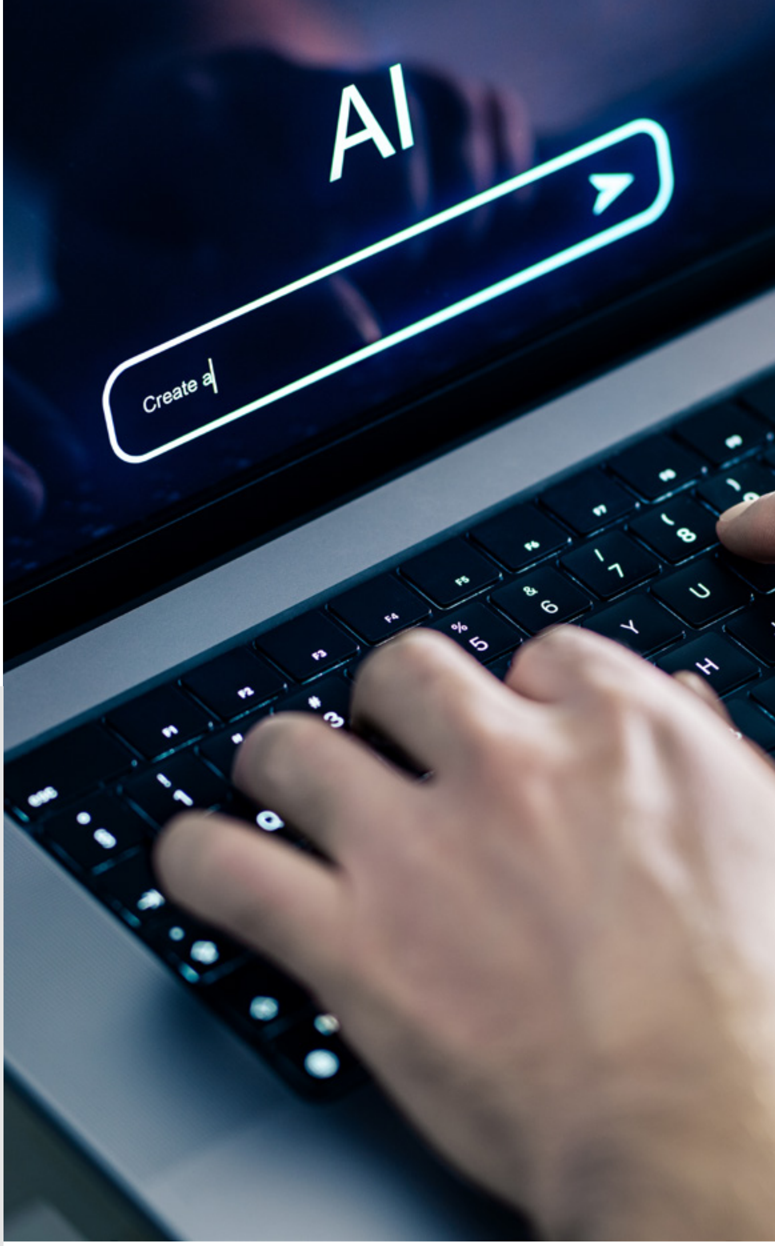
Act will apply to GPAI.

24 Months

Act will apply for high-risk AI systems under Annex III.

36 Months

Act will apply for high-risk AI systems under Annex II.



# How can KPMG help?

Businesses that produce or deploy AI systems in the course of their work should consider how AI can be made compliant with the EU AI Act (and what impact that may have on the business and its operational performance). KPMG offer a multi-disciplinary professional service that enables us to support clients across a wide range of activities. Our experienced teams ranging from regulatory to data privacy and cyber security can ensure that your business is best positioned to adapt to the changing landscape of the AI market.

If you have any questions regarding the impact the Act will have upon your business, please contact Sean Redmond.

# Why do we need the Act?

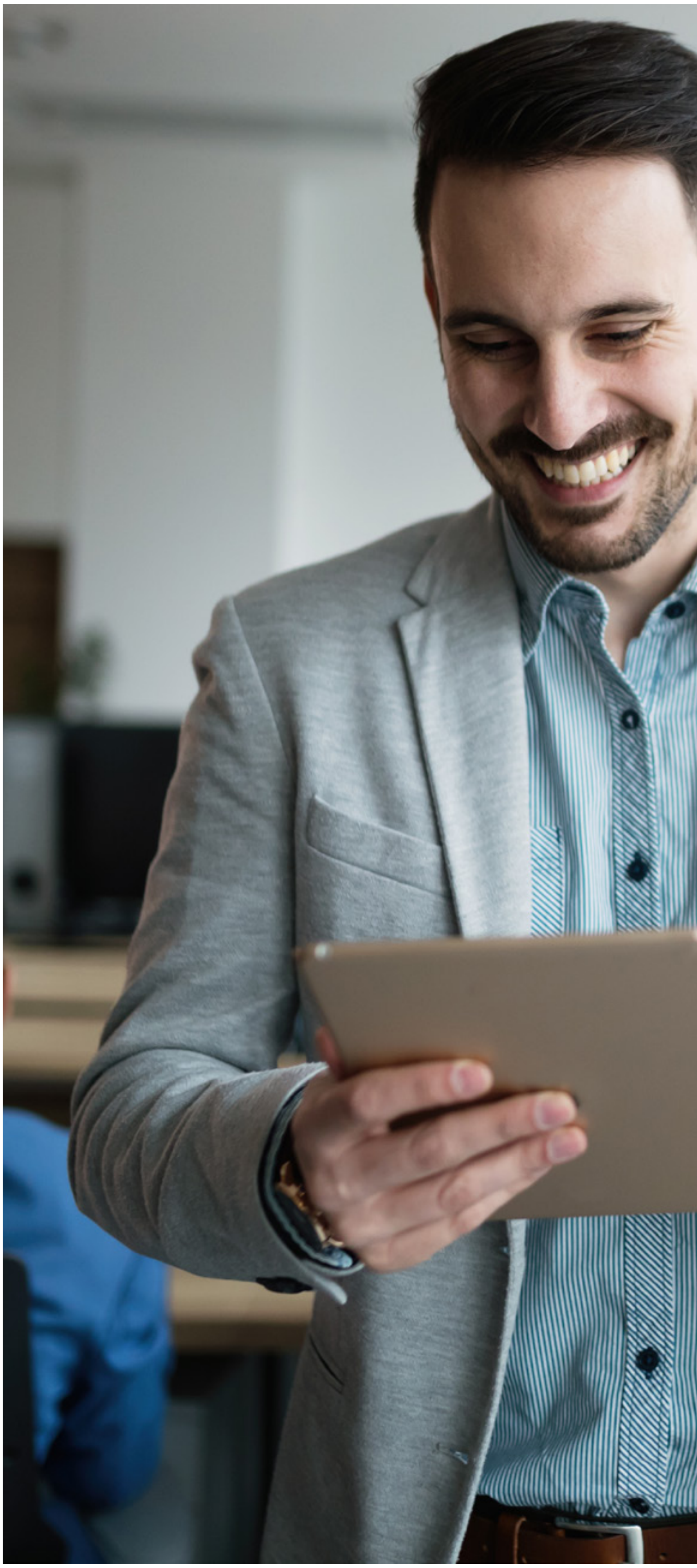
The EU AI act provides a much-needed definition of an AI system,

> “which 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 content, predictions, recommendations, or decisions that can influence physical or virtual environments.”

The Act is intended to ensure better conditions for the development and use of AI and is a pillar of the EU’s digital strategy. Furthermore, the Act takes aim at the emerging issue of Deep Fake technology.

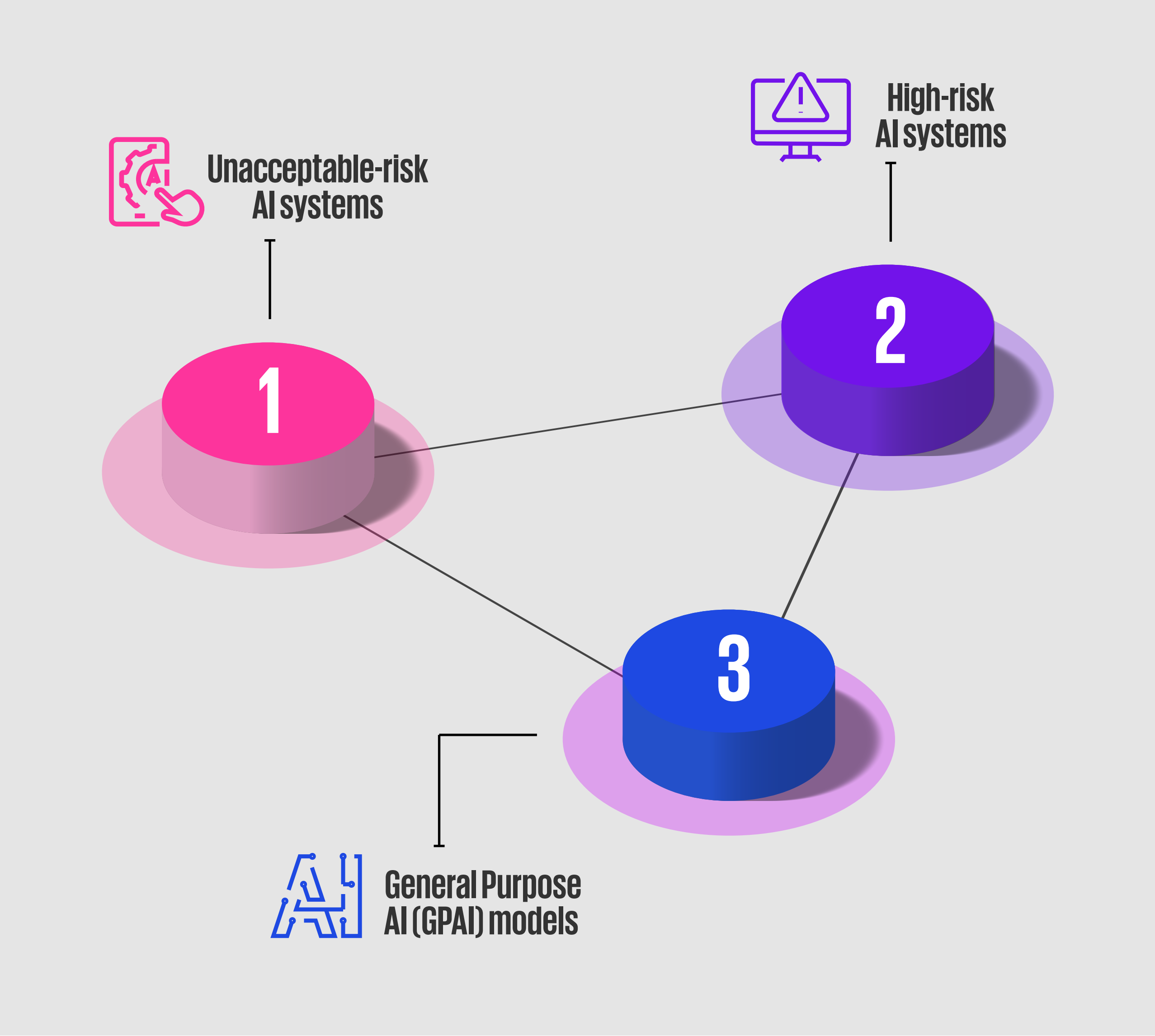
> “Deep Fakes” are defined as “AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful.”

The act places a requirement on deployers of this technology to disclose that the content has been artificially generated —or manipulated.



# What are the key details of the Act?

The AI Act classifies AI systems into three risk categories: unacceptable-risk AI systems, high-risk AI systems and General Purpose AI (GPAI) models.


Unacceptable-risk AI systems
1
High-risk AI systems
2
3
General Purpose AI (GPAI) models

# Unacceptable Risk:

AI practices that are considered to pose an unacceptable risk are prohibited by the Act.

These include:

- AI systems that deploy subliminal techniques or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person’s behaviour by appreciably impairing the person’s ability to make an informed decision.
- AI systems that exploit any of the vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation.
- The use of biometric categorisation systems that categorise individually natural persons based on their biometric data.
- AI systems for the evaluation or classification of natural persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, which leads to detrimental or unfavourable treatment that is unjustified or disproportionate.
- Real-time’ remote biometric identification in public spaces for law enforcement, except for specific necessary objectives like searching for victims or missing persons, preventing threats to safety, or identifying suspects in serious crimes.
- AI systems creating facial recognition databases through untargeted scraping from the internet or CCTV footage.
- AI systems inferring emotions in workplaces or educational institutions, except for medical or safety reasons.

# High Risk

High-risk AI systems are those that are safety components of products, or which are themselves products (as set out in a specified list of EU regulations), and those where if based on their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas which are:

1 Private companies should treat ESG 1.
Certain Biometric AI systems

2 Critical infrastructure including management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity.

3 Education and vocational training including systems that determine access or evaluating learning outcomes

4 Employment, workers management and access to self-employment including recruitment, promotions and termination, assessment of performance and allocation of tasks

5 Access to and enjoyment of essential private services and essential public services and benefits including AI systems intended to evaluate eligibility for access to essential public assistance benefits and services, to evaluate the creditworthiness of natural persons or establish their credit score, access to emergency services, risk assessment and pricing in relation to life and health insurance.

6 Law enforcement - systems intended to be used by or on behalf of law enforcement authorities for certain purposes.

7 Migration, asylum and border control management; and

8 Administration of justice and democratic processes

Even when included in one of the above categories, AI systems shall not be considered as high risk 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. This shall be the case if one or more of the following criteria are fulfilled:

- the AI system is intended to perform a narrow procedural task;
- the AI system is intended to improve the result of a previously completed human activity;
- the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
- the AI system is intended to perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

# General Purpose AI Systems ("GPAI")

One of the new additions to the Act is the regulation of GPAI models. Defined as an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform 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. General purpose AI systems may be used as high-risk AI systems by themselves or be components of other high risk AI systems. The Act establishes that all providers of GPAI models must:

- Draw up technical documentation, including training and testing process and evaluation results.
- Draw up information and documentation to supply to downstream providers that intend to integrate the GPAI model into their own AI system in order that the latter understands capabilities and limitations and is enabled to comply.
- Establish a policy to respect the Copyright Directive.

Publish a sufficiently detailed summary about the content used for training the GPAI model.

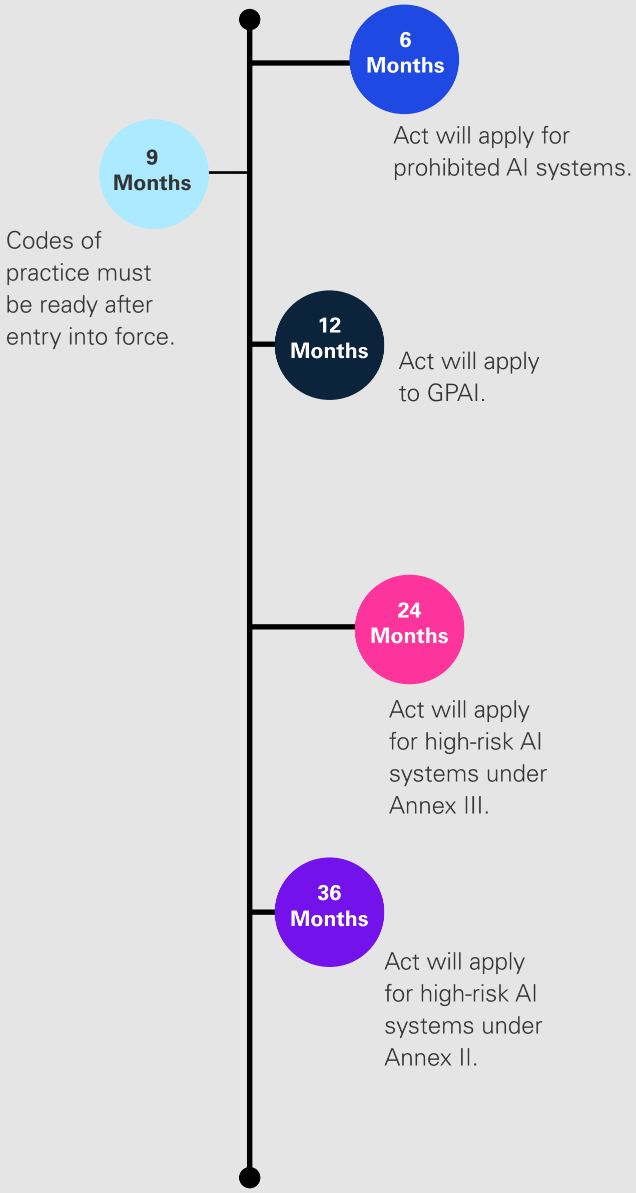
# How will this impact your business going forward?

| | | |
|---|---|---|
| **Human Oversight** | For Providers of AI Systems | The Act legislates for oversight obligations on those building and selling high-risk systems in the marketplace or using them.  Appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. High Risk AI providers must design their AI systems to implement human oversight. Oversight measures should be proportionate to the risks, level of autonomy and context of use of the AI system. These measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator. |
| | For Users of AI Systems | Deployers of high-risk AI systems must take appropriate technical and organisational measures to ensure they use the systems in accordance with the instructions and they must assign human oversight to individuals who have the necessary competence, training and authority, as well as the necessary support to so. |
| **Employer Obligations** | For Providers of AI Systems | Not applicable. |
| | For Users of AI Systems | Importantly for organisations planning to deploy AI at the workplace, before putting into service or use a high-risk AI system, deployers who are employers shall inform workers representatives and the affected workers that they will be subject to the system. |
| **Testing of AI Systems** | For Providers of AI Systems | The Act requires that High-Risk AI systems be tested in real world conditions. The system for the design, development and testing of AI systems shall be approved by the relevant market surveillance authority, and in accordance with certain criteria, including registration in the EU database, establishment of the provider in the Union or appointment of a legal representative within the Union, adherence to data transfer safeguards, and ensuring the reversibility of the AI system's outcomes.<br>Providers have an obligation to inform and instruct the users of their systems about this testing. Providers are required to obtain informed consent of users to participate in testing in real world. The decisions of the AI system must be effectively reversed and disregarded, and that personal data is protected and deleted upon the withdrawal of consent of the participant.<br>Providers have a responsibility to report any serious incident identified in the course of the testing to the relevant market surveillance. |
| | For Users of AI Systems | Deployers of AI must monitor the operation of the high-risk AI system on the basis of the instructions of use provided and when relevant, inform providers of any challenges or issues experienced. |

| | | |
|---|---|---|
| **Codes of Practice and Compliance** | For Providers of AI Systems | The Codes of Practice represent a central tool for the proper compliance with the obligations of the regulation for providers of GPAI. The EU's AI Office and AI Board shall ensure that the codes of practice cover:<br>The relevant information to include in technical documentation for authorities and downstream providers.<br>Identification of the type and nature of systemic risks and their sources.<br>The modalities of risk management accounting for specific challenges in addressing risks due to the way they may emerge and materialise throughout the value chain.<br>All GPAI model providers may demonstrate compliance with their obligations if they voluntarily adhere to a code of practice until European harmonised standards are published, compliance with which will lead to a presumption of conformity. Providers that don't adhere to codes of practice must demonstrate alternative adequate means of compliance for Commission approval.<br>An AI Office will be established, sitting within the Commission, to monitor the effective implementation and compliance of GPAI model providers. The AI Office may conduct evaluations of the GPAI model to assess compliance where the information gathered under its powers to request information is insufficient, and investigate systemic risks, particularly following a qualified report from the scientific panel of independent experts. |
| | For Users of AI Systems | Not Applicable. |

# What's Next Timelines for implementation

The EU AI Act will likely be passed into law early in 2024, however businesses will have some time to prepare before it begins to apply. After the act enters into force the AI Act will apply in accordance with the following timeline.



**6 Months**

Act will apply for prohibited AI systems.

**9 Months**

Codes of practice must be ready after entry into force.

**12 Months**

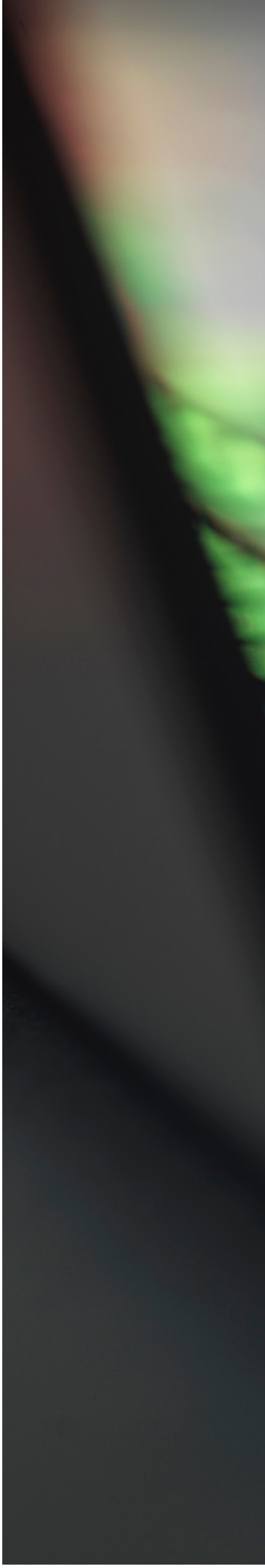
Act will apply to GPAI.

**24 Months**

Act will apply for high-risk AI systems under Annex III.

**36 Months**

Act will apply for high-risk AI systems under Annex II.



# How we can help?

Businesses that produce or deploy AI systems in the course of their work should consider how AI can be made compliant with the EU AI Act (and what impact that may have on the business and its operational performance). KPMG offer a multi-disciplinary professional service that enables us to support clients across a wide range of activities. Our experienced teams ranging from regulatory to data privacy and cyber security can ensure that your business is best positioned to adapt to the changing landscape of the AI market.

If you've any questions please contact Sean Redmond.

## Contact us

**Sean Redmond**
Data Advisory and
AI Risk & Regulation
**T:** +353 87 050 4838
**E:** sean.redmond@kpmg.ie

**Emma Coogan**
AI Risk & Regulation
**T:**+353 87 216 1626
**E:** emma.coogan@kpmg.ie

**Dani Michaux**
Cyber Security
**T:** +353 87 050 4769
**E:** dani.michaux@kpmg.ie

**Jackie Hennessey**
Technology Risk
**T:** +353 87 050 4171
**E:** jackie.hennessy@kpmg.ie

**Greg Wiseman**
Data Advisory and Modelling
**T:** +353 87 050 4408
**E:** greg.wiseman@kpmg.ie

**Emma Ritchie**
KPMG Law
**T:** +353 87 050 4628
**E:** emma.ritchie@kpmglaw.ie

kpmg.ie

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Produced by: KPMG's Creative Services. Publication Date: Febuary 2024 (10085)