EU AI Act

Digital & Data Legal
March 2025

pwc

PwC Digital & Data Team

Our role

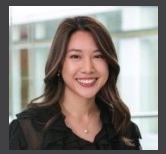
Our team advises clients on digital laws and regulations, including those in relation to personal data. We are **thought leaders** with a strong track record of working with governments, regulators and businesses to accelerate thinking around the responsible use of data and technology.

We provide support to on a broad range of matters, which is reflective of our **diverse client base** (many of whom operate in multiple jurisdictions worldwide).

Our team of lawyers include SMEs across numerous fields and sectors including **UK & EU GDPR**, **direct and digital marketing**, **commercial contracts**, **data subject rights handling,** and **artificial intelligence.**

Chris Cartmell
Head of Digital & Data Solicitor
M: +44 7483 353965
E: chris.cartmell@pwc.com

Stephanie Baker
Senior Associate, Solicitor
(Qualified in Australia)
M: +44 7483 349262
E: stephanie.m.baker@pwc.com



Michelle Lee
Senior Associate, Solicitor
M: +44 7483 929870
E: michelle.yee.loo.lee@pwc.com

Agenda

1. Introduction to the EU AI Act
2. Key concepts
3. Prohibited AI
4. AI Literacy
5. Impact on organisations - scenario
6. Key takeaways

pwc

Legal Academy

1

Introduction to the EU AI Act

The EU AI Act is a horizontal regulation, applicable to all industry sectors

Purpose and goals

- Ensure AI systems placed on the EU market are **safe** and **respect fundamental rights**
- Ensure **legal certainty** to facilitate investment and innovation in AI
- Facilitate the development of **a single market for lawful, safe and trustworthy AI systems**
- A **risk-based approach** that does not hinder innovation unnecessarily

Governance and enforcement

European AI Office

Independent panel of scientific experts for general purpose AI

European level

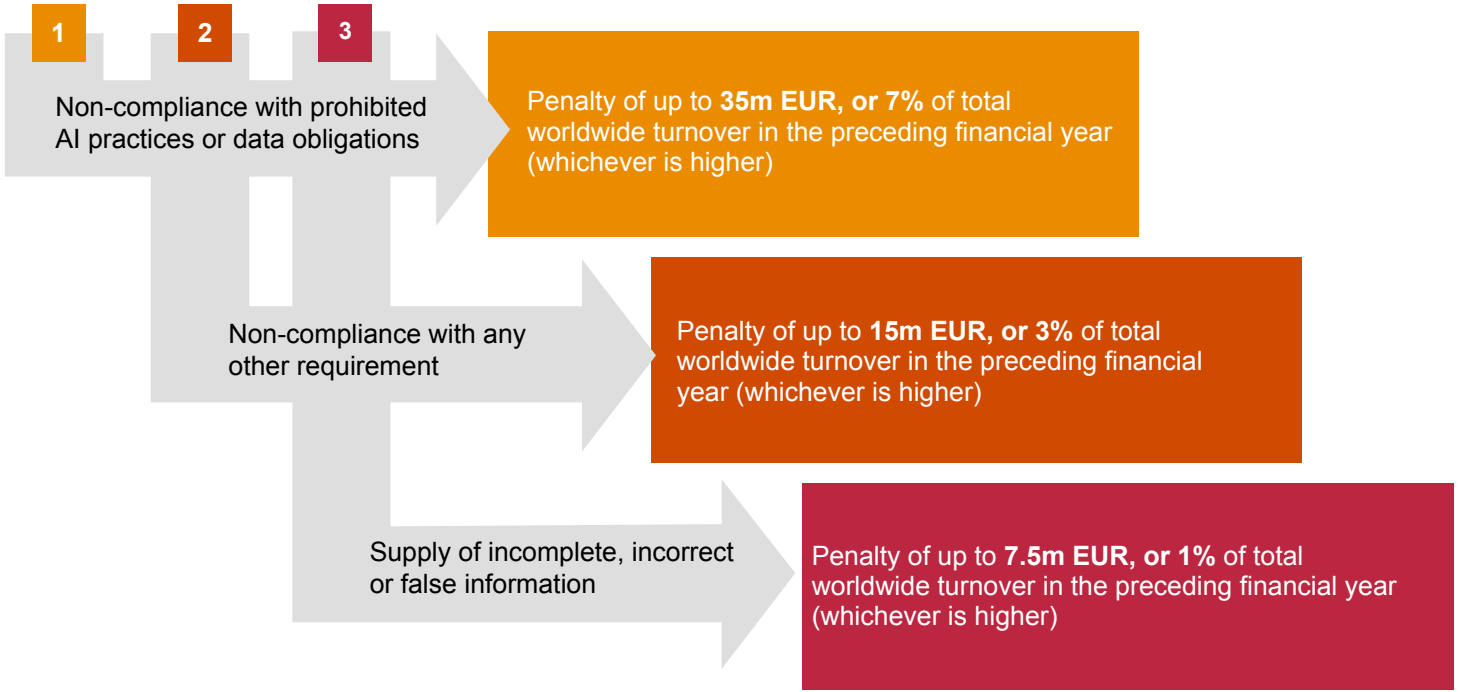
National market surveillance authorities

National level

Who and what is affected?

- **AI systems and AI models –** Machine-based solutions that operate with some autonomy and infer how to achieve objectives and influence the world without being explicitly programmed
- **In all sectors –** The AI Act is a horizontal regulation which applies to all AI systems, across all sectors
- **In and outside the EU –** Applies to all AI systems operating on the EU market or with **an impact in the EU**, even if the system is based abroad
- **Across the AI value chain –** Obligations apply predominantly to providers (creators) of AI systems and deployers (users) of AI systems

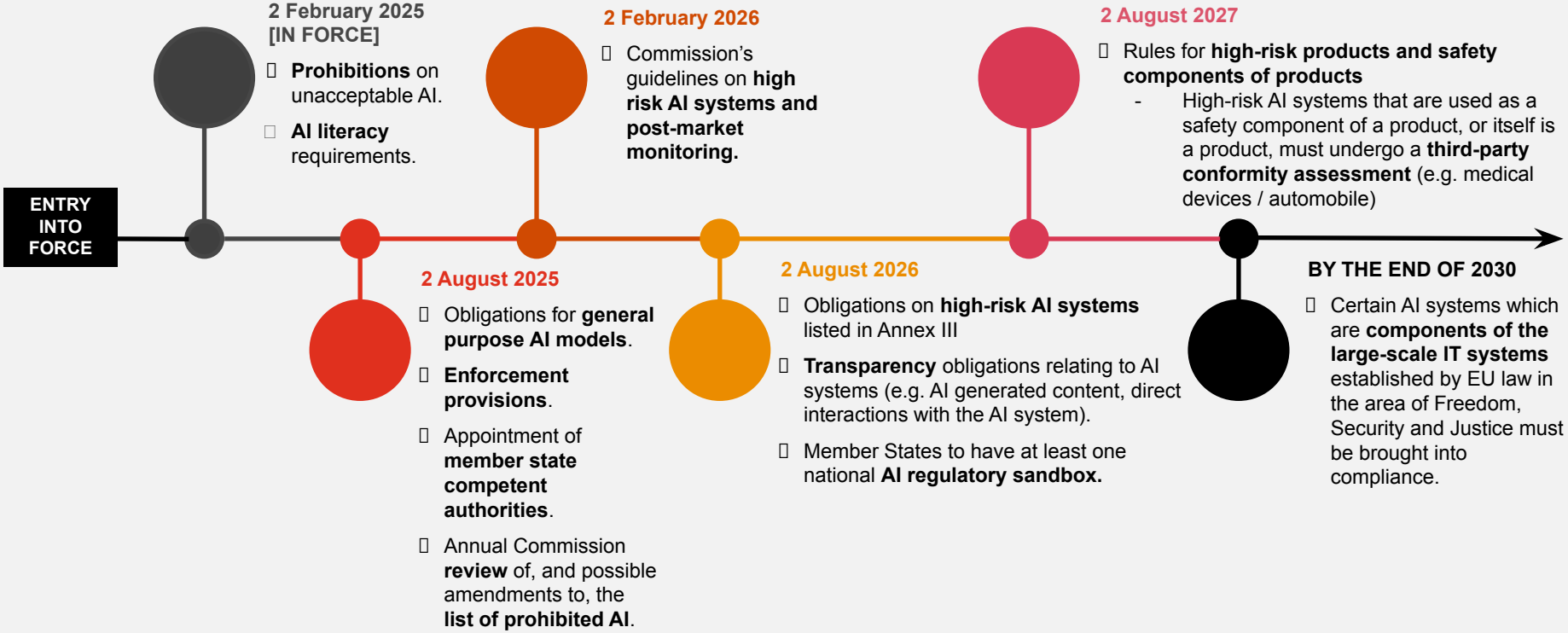
Violations could result in fines



Timeline

Entry into force: 1 Aug. 2024 20 days after publication in the Official Journal of the EU.

Entry into application: 2 Aug. 2026 (Exceptions exist for specific provisions)



Time for a question

True or false?

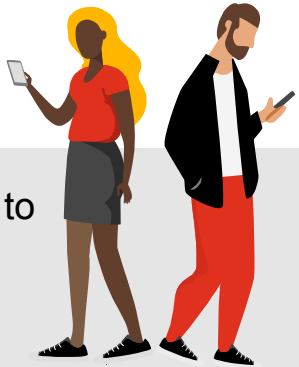
The AI Act will apply to a US-based company offering AI systems to EU customers.

Time for a question

TRUE

True or false?

The Act is market-based legislation and will apply to any company that offers AI systems to customers based in the EU.



2

Key Concepts

What different roles can an organisation play?

- The legal framework will apply to both **public and private** actors **inside** and **outside** the EU as long as the AI system is placed on the EU market or the output is used in the EU.
- It can concern both providers and deployers of AI systems. It does not apply to private, non-professional uses. In general, the Act distinguishes between the following roles:

Providers

Any person, public authority, agency or other body that **develops** an AI system or that has an AI system developed with a view to **placing it on the market** or **putting it into service** under its own name or trademark.

Deployers

Any 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.

Importers

Any person established in the EU that **places on the market** or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the EU.

Distributors

Any person in the supply chain, other than the provider or the importer, that **makes an AI system available** on the EU market without affecting its properties.

What do we mean by “AI system”?

The definition: ‘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**.

		Example of a spam filter
Varying levels of autonomy, may exhibit adaptiveness	• **Some degree of independence of actions from human involvement** and of capabilities to operate without human intervention • AI **could have self-learning capabilities**, to change while in use.	Operates without human involvement and refines through feedback
Explicit or implicit objectives	• Objectives are **explicitly stated by humans or implicit in the tasks and data** • Objectives **may be different from the intended purpose**	Objective is to identify spam email and other similar messages
Infers how to generate outputs	• AI systems can **create outputs and derive models and / or algorithms from inputs / data** through techniques like machine learning or logic- and knowledge-based approaches • Inference goes beyond basic data processing, to **enable learning, reasoning or modelling**	It is "taught" to do so through many examples of spam emails, "learning" patterns how to distinguish them
Influence physical or virtual environments	• The **contexts** in which the AI systems operate	It changes the contents of your inbox and your spam folder

What do we mean by “general-purpose AI model”?

The definition: ‘General-purpose AI model is an AI model, including where such an AI model is **trained with a large amount of data** using self-supervision at scale, that displays **significant generality** and is capable of competently performing 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**.’

		Example of GPT-4
Trained with a large amount of data	• Vast dataset from **various sources** that includes a **diverse array** of information. • Helps the AI learn **patterns, relationships, and knowledge** that can be applied to different situations.	Trained on diverse and extensive dataset, including books, websites, and other written materials.
Significant generality	• AI can perform well across a **broad range of tasks and domains.** • Ability to **adapt to different contexts** and provide useful outputs in various scenarios.	Answers questions, writes essays, generates creative content, and translates languages.
Integrated into a variety of downstream systems	• Can be **embedded** into different software / applications to enhance functionality • Used as a **component** in various products / services	Used in many applications including chatbots, virtual assistance, content creation tools and educational platforms.

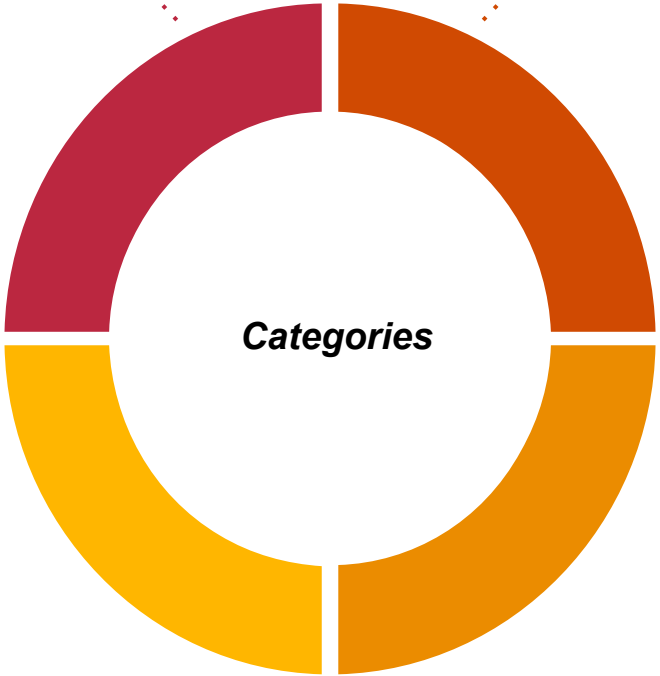
3

Prohibited AI

Risk assessment

Prohibited AI systems

There are **prohibited AI practices**, which are banned outright. This includes a very limited set of particularly harmful uses of AI that contravene EU values because they violate fundamental rights.



High-risk AI systems

High-risk AI systems are permitted on the EU market and subject to **compliance with certain mandatory requirements** and an **conformity assessment**. The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation.

Low-risk AI systems

Low-risk AI systems are low risk because they **neither use personal data nor make any predictions** that influence human beings. According to the EU Commission, **most AI systems will fall into this category**. A typical example is industrial applications in process control or predictive maintenance.

Limited-risk AI systems

AI systems under this category are **subject to transparency obligations** to allow individuals interacting with the system to make informed decisions. This is the case for a chatbot, where transparency means letting the user know they're speaking to an AI-empowered machine. Providers need to ensure that natural persons are informed that they're interacting with an AI system.

Examples of prohibited AI Systems

AI practices that pose unacceptable risks to fundamental rights and EU values are prohibited:

Manipulative, or deceptive techniques to distort behaviour and impair informed decision-making	• An AI chatbot that impersonates a friend or relative with a synthetic voice to deceive individuals into making harmful decisions.
Social scoring	• Tax authorities using an AI predictive tool on taxpayers' social habits or internet connections to single out individuals for inspections.
Biometric categorisation inferring sensitive attributes	• To deduce an individual's race from their voice or religious orientation from their tattoos or facial features.
Real-time biometric identification	• To identify protestors in public spaces for minor offences
Risk of committing criminal offences	• Reviewing taxpayers' returns to predict potential criminal tax offences on basis of profile built by AI system that uses variables like place of birth and number of children.
Emotion recognition in workplaces and educational institutions	• Using webcams and voice recognition systems to track employees' emotions, such as anger.
Untargeted scraping of facial images from the internet/CCTV	• AI systems that create or expand facial recognition databases through untargeted scraping of facial images from CCTV footage.

[1] Provided examples of areas and AI systems classified as 'prohibited' are not exhaustive.

Which of the below would be a prohibited AI system?

Which of the below would be a prohibited AI system?

Examples of high-risk AI Systems

The classification as ‘high risk’ depends not only on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used:

Non-banned biometrics	• Remote biometric identification systems.
Critical infrastructure	• Safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity.
Education and vocational training	• Assessing the appropriate level of education for an individual.
Employment, workers management and access to self-employment	• Promotion and termination of contracts, allocating tasks based on personality traits or characteristics and behavior, and monitoring and evaluating performance.
Access to and enjoyment of essential public and private services	• Evaluating creditworthiness to assess whether to provide loans.
Law enforcement	• Evaluating evidence reliability during criminal investigations or prosecutions.
Migration, asylum and border control management	• Examination of application for asylum, visa and residence permits, and associated complaints related to eligibility.
Administration of justice and democratic processes	• Influencing elections and referenda outcomes or voting behavior, excluding outputs that do not directly interact with people, like tools used to organise, optimise and structure political campaigns.

[1] Provided examples of areas and AI systems classified as ‘high risk’ are not exhaustive.

4

AI Literacy

What is AI Literacy?

The definition: ‘AI literacy’ means **skills, knowledge and understanding** that allow **providers, deployers and affected persons**, taking into account their respective rights and obligations in the context of this Regulation, to make an **informed deployment** of AI systems, as well as to **gain awareness about the opportunities and risks** of AI and possible harm it can cause.

Article 4: Providers and deployers of AI systems shall take measures to ensure, to their best extent, a **sufficient level** of AI literacy of their staff and **other persons** dealing with the operation and use of AI systems on their behalf, taking into account their **technical knowledge, experience, education and training** and **the context** the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Enforcement	In force, but unlikely to be enforced until national market surveillance authorities are designated in August 2025.
AI Pact	Supports and encourages organisations to collaborate and share their experience and knowledge.

Practical application

Ensure general understanding of AI

Consider role of AI within organisation.

Document the AI systems used and the people involved in operations and use.

Consider risks that AI systems pose

Consider what employees need to know and be aware of.

Set AI literacy goals and priorities based on relevant risk levels.

No one size fit all approach

Will be context-dependent, taking into account factors such as size and financial resources of organisation and persons involved.

Set appropriate strategies and actions

Can include e-learning modules, internal webinars and conducting regular surveys amongst employees to evaluate effectiveness of measures.

Other resources

EU AI Office has published ‘living repository’ of practices implemented by organisations to ensure AI literacy as indicative examples.

5

Impact On Organisations

Scenario

GlobalTech, a multinational technology company **headquartered in Germany**, is planning to create an **AI system to evaluate employee performance**. The AI system is designed to analyse various data points, including keystrokes, mouse movements and email communications to assess productivity. Using this information, the AI system will then provide recommendations for promotions, terminations, and other HR decisions.

During the trial run, five employees will be operating the AI system. This includes a contractor who is an AI specialist and has been brought in for this purpose. The other four persons work in the IT department and have **some general knowledge** of AI systems. GlobalTech is planning to test the AI system on a **small sample of 20 employees in its headquarter in Germany.**

If the trial of the AI system works well, GlobalTech plans to expand its use to other offices across Europe, Middle East and Asia. GlobalTech also has plans to **license** the AI system out to other companies.

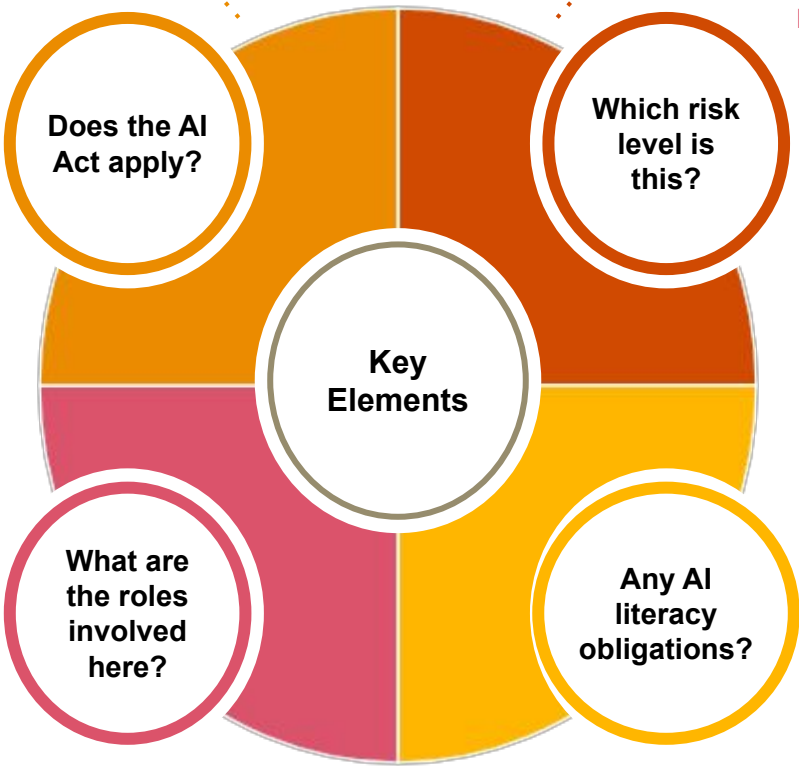
Scenario

Yes, the AI Act applies

- As GlobalTech is developing this AI system in Germany (i.e. within the EU), it will be in scope of the Regulations.

Provider and Deployer

- **Provider:** GlobalTech is developing this AI system and placing this system into service.
- **Deployer:** GlobalTech as they are using AI system. Other companies that are granted the licence to use the AI system will likely be considered deployers.



High risk

- The AI system could be high-risk as it will be used for the purposes of **employment management** (e.g. promotion and termination of contracts).
- Assess presence of significant risk to harm the employees' health, safety, or fundamental rights (e.g. risk to privacy).
- GlobalTech should starting preparing for the new obligations that are coming into force soon.

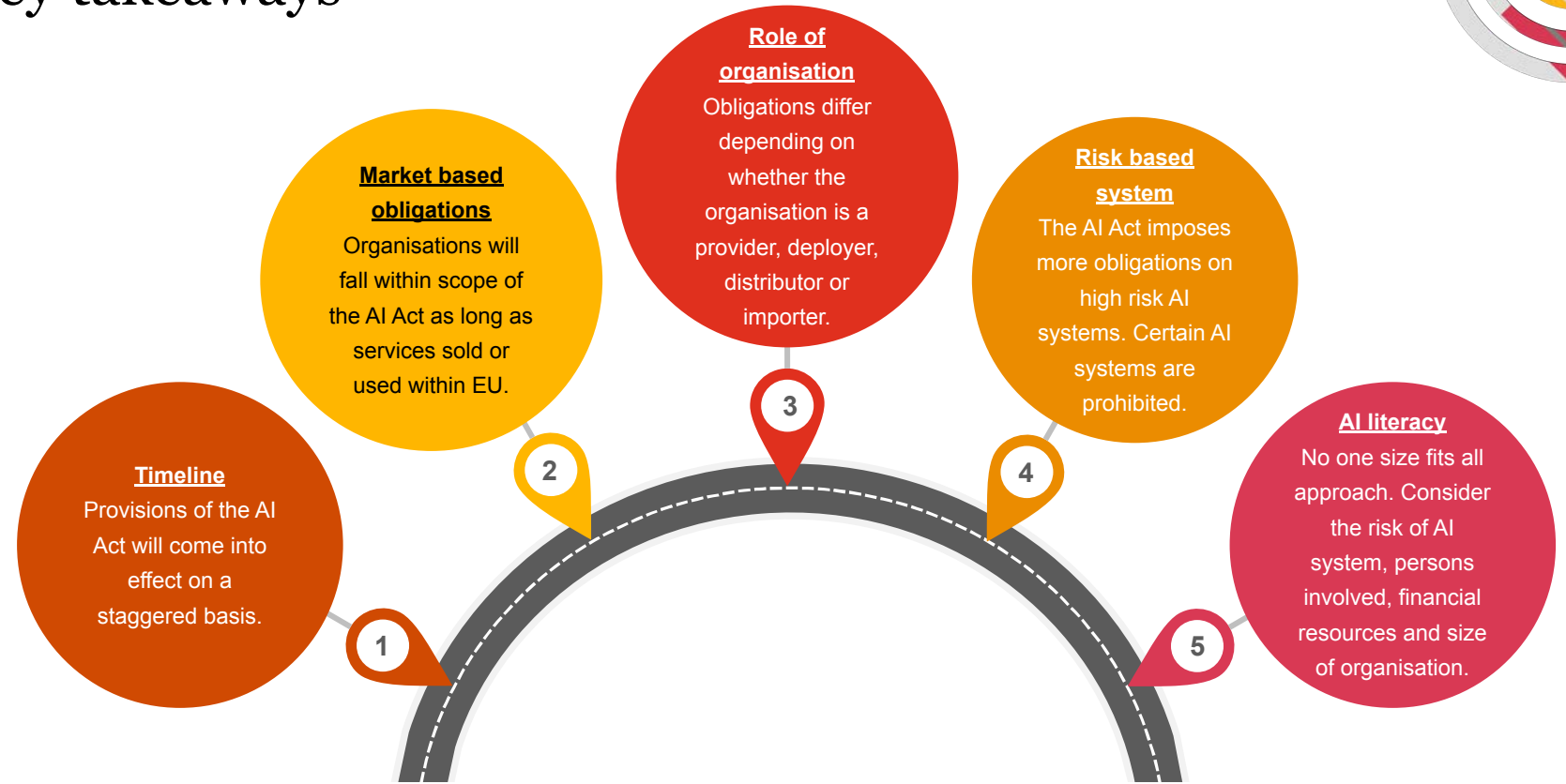
Yes, there will be

- No one size fits all approach - GlobalTech likely need to provide different levels of training (e.g specialist vs non-specialist content).
- This can be in the form of e-learning modules or video webinars.
- Licensing: Provide manuals to help its client operate the AI system and understand risks involved.

6

Key takeaways

Key takeaways



Thank you

Stephanie Baker
Senior Associate, Solicitor
(Qualified in Australia)
M: +44 7483 349262
E: stephanie.m.baker@pwc.com
in/stephanie-baker-209471131

Michelle Lee
Senior Associate, Solicitor
M: +44 7483 929870
E: michelle.yee.loo.lee@pwc.com
linkedin.com/in/michelle-yee-loo-lee

Chris Cartmell
Head of Digital & Data Solicitor
M: +44 7483 353965
E: chris.cartmell@pwc.com
in/chris-cartmell-828632b

pwc