EU AI ACT: OVERVIEW AND FAQS

JUNE 2024

Weil

FAQs

Click on the questions below to go straight to that section

The EU Artificial Intelligence Act (the "**Act**") enters into force 20 days after publication in the EU's Official Journal, with most obligations to take effect within 24 months. The below provides an overview of the key elements of the Act alongside frequently asked questions as to what it might mean for organisations in practice.

THE WHAT

1. **What is an AI system?** What does the Act regulate? It regulates AI systems. The first question to ask is what is an AI system? The definition in the Act 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*". Breaking this down and picking out the key characteristics, an AI system needs to:

   (a) be a machine-based system, i.e. run off machines;

   (b) operate with "varying levels of" autonomy, i.e. have the ability to operate with some degree of independence from humans and without human intervention (however it remains unclear where the threshold lies here, how much autonomy?);

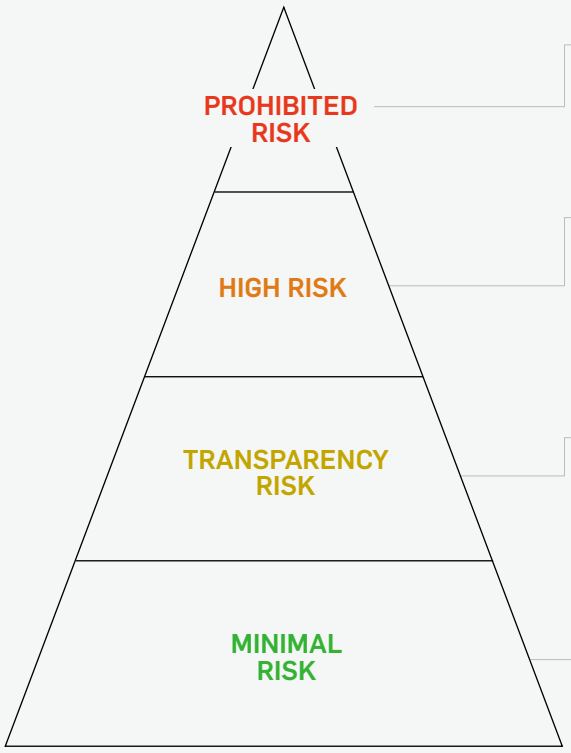
   (c) exhibit adaptiveness; essentially self-learning capabilities, which allow the system to change while in use (although arguably this is an optional feature as the Act states it "*may*" or "*could*" exhibit this); and

   (d) most importantly, have the ability to infer. This means the capability to derive information from input data to then use that and any any prompts/ parameters to generate output. The recitals helpfully confirm that the definition is not intended to cover more traditional AI systems, which automatically execute operations based on rules set by humans.

   There are also some exceptions, for example, the Act does not apply to AI systems where the sole purpose is scientific research and development or to open source AI systems (see Question 4 below).

   Still not clear? We expect the definition of AI systems and how this is applied in practice to crystallise through Commission delegated act and guidelines.

2. **How does the Act regulate AI systems?** The Act categorises AI systems into different risk levels, with the obligations commensurate to the risk level.



Prohibited risk AI systems are banned entirely. The kind of AI systems that fall into this category include the likes of social scoring systems or emotion recognition systems in the workplace.

High risk AI systems are where the majority of the compliance obligations lie, for both providers and deployers. The Act provides a high-level list of high-risk systems at Annex III, which includes AI used for remote biometric identification, critical infrastructure, and access to education and employment. It also includes AI systems used as safety components in certain products (listed in Annex II).

AI systems that present specific transparency risks, which includes AI systems that directly interact with individuals or which generate or manipulate text, video, audio and/or images. For example, chatbots, virtual assistants, and AI systems generating deep fakes. The Act places obligations on providers and, in certain circumstances, deployers with respect to transparency.

Lastly, **minimal risk AI systems**, which are all other AI systems which do not fall into the above categories, such as spam filters and recommender systems. The Act does not place any specific obligations on these systems beyond AI literacy requirements. It is expected that the vast majority of AI systems are likely to fall into the minimal risk category.

However, determining with certainty where any AI system lies is important, as the cost of compliance for high-risk systems, and any fines for non-compliance, are significant.

See the Annex for further information on compliance obligations associated with these systems.

3. **What about GPAI models?** The Act also regulates general-purpose AI (GPAI) models.

   These are essentially very powerful models, the key criteria being that they can perform a wide range of distinct tasks, which are typically trained on large amounts of data.

   It takes a two tiered approach; "normal" GPAI models, and GPAI models with systemic risk, the latter having stricter compliance obligations. A GPAI model falls in the systemic risk category if it has high impact capabilities evaluated on benchmarks (when the cumulative amount of compute used for its training exceeds 10^25 floating point operations) or per decision by the AI Office.

   Compliance obligations include maintaining technical documentation (including on the training and testing process), documents for providers to help them understand the model, a policy on how EU copyright laws will be observed, and making public a summary about content used to train the model (based on template to be published by the AI Office).

4. **What about open source GPAI models and AI systems?** The Act does not apply to open source AI systems released under free and open source licences, unless they are prohibited AI systems, high risk AI systems or AI systems that present a specific transparency risk. However, this exception is not available if the AI system has been monetized in any way. This will include, for example, if the AI system itself is free, but support services are commercialised.

   An exception also exists for GPAI models released under free and open source licences (unless it also presents systemic risk), although limited obligations still apply (namely the requirement to put in place a copyright policy and publish a summary of the training data).

THE WHO

5. **Who does the Act apply to?** The Act applies to providers, importers, distributors, product manufacturers, authorised representatives and deployers (i.e. the users of systems, but not necessarily the end-users).

Each of these roles comes with a different set of compliance obligations. The majority of obligations fall on providers, and then deployers.

PROVIDER

- Person that develops an AI system or GPAI model or has it developed
- Places them on the market or puts them into service in the EU under its own name or trade mark
- Whether for payment or free of charge

IMPORTER

- Person established in the EU
- Places on EU market an AI system that bears the name or trade mark of a non-EU person

DISTRIBUTOR

- Person other than the provider or importer
- Makes AI system available on the EU market

DEPLOYER

- Person using an AI system
- Under its authority
- Except where the AI system is used in the course of a personal, non-professional activity

AUTHORISED REPRESENTATIVE

- Person established in the EU
- Written mandate in place with provider of an AI system or GPAI model to perform and carry out that provider's obligations under the Act

PRODUCT MANUFACTURER

- Places on the market or puts into service in an AI system
- Together with their product
- Under own name or trade mark

GLOSSARY

Placing on the market: *first making available of an AI system or a GPAI model on the EU market*

Putting into service: *supply of an AI system for first use directly to the deployer or for own use in the EU*

Making available on the market: *supply of an AI system or GPAI model for distribution or use on the EU market in the course of commercial activity*

6. **My organisation does not develop AI systems, but just uses them. Does that mean we could only ever be a deployer under the Act?** Not necessarily.

   An organisation will be a provider if it has an AI system developed on its behalf and first makes it available on the EU market or first puts it into service under its own name or trade mark (for its own use or for another deployer). In short, a deployer (or other operator) cannot circumvent its regulatory obligations by asking someone else to build it.

   A deployer (and a distributor, importer or any other third party) will also be a provider if:

   - If it puts its name or trade mark on a *high-risk AI system* already placed on the market or put into service in the EU.
   - If it makes a substantial modification to a *high-risk AI system* already placed on the market or put into service in the EU, and it remains a *high-risk AI system.*
   - If it modifies the intended purpose of an AI system already placed on the market or put into service, which is not high-risk, such that it becomes a *high-risk AI system*.

   The Act is clear that it doesn't matter what the contract between organisations states with respect to regulatory responsibilities.

   Deployers (and other operators) will therefore need to consider carefully the risk-level of the AI system and, if high risk, any customisations, branding and the use cases, should they fall on the riskier-side of the fence and take on the more onerous provider-obligations under the Act.

7. **Does the Act apply to us if we only use the GPAI model or AI system for internal purposes?** It can do, depending upon the circumstances.

   The recitals of the Act explicitly state that GPAI models used only for purely internal processes, that are not essential for providing a product or service, and which do not affect the rights of individuals are not subject to the Act. However, if that provider integrated that GPAI model into its own AI system that is made available or put into service in the EU, then the GPAI model obligations would apply, even if that model is not provided to any third party.

   In addition, an organisation that develops its own AI system for internal use has not placed it on the EU market or put it into service. However, while not set out in the Act, taking inspiration from the GPAI model recital referred to above, if that AI system is essential to providing a product or service or poses a risk to individuals, it could potentially be caught). In any event, it could still be considered a deployer of the AI system e.g., if it is a high-risk AI system used internally for recruitment purposes.

THE WHERE (A.K.A. SCOPE)

8. **My organisation is based outside the EU; do we need to worry about the Act?** The Act has extra-territorial effect under Article 2, and so non-EU organisations could be subject to obligations under the Act. Broadly, there are two ways by which this could occur.

   Firstly, if a non-EU provider of an AI system (or GPAI model) first places on the market or puts it into service in the EU, then the Act applies. This is straightforward, e.g. a US entity that has no presence in the EU develops an AI system and then provides it to its clients (deployers) for use in the EU. That US entity will be subject to any applicable provider obligations under the Act.

   The Act will also apply to non-EU providers or deployers of AI systems, where the output of the AI system is intended to be used in the EU. This is primarily designed to prevent EU organisations deliberately circumventing the Act by outsourcing AI-related activities to outside the EU, and then using that output in the EU - for example, an EU organisation receiving job applications in the EU, sending these to a provider in the US to sift applications using an AI system who then informs the EU organisation, and the EU organisation then making recruitment decisions based on that information.

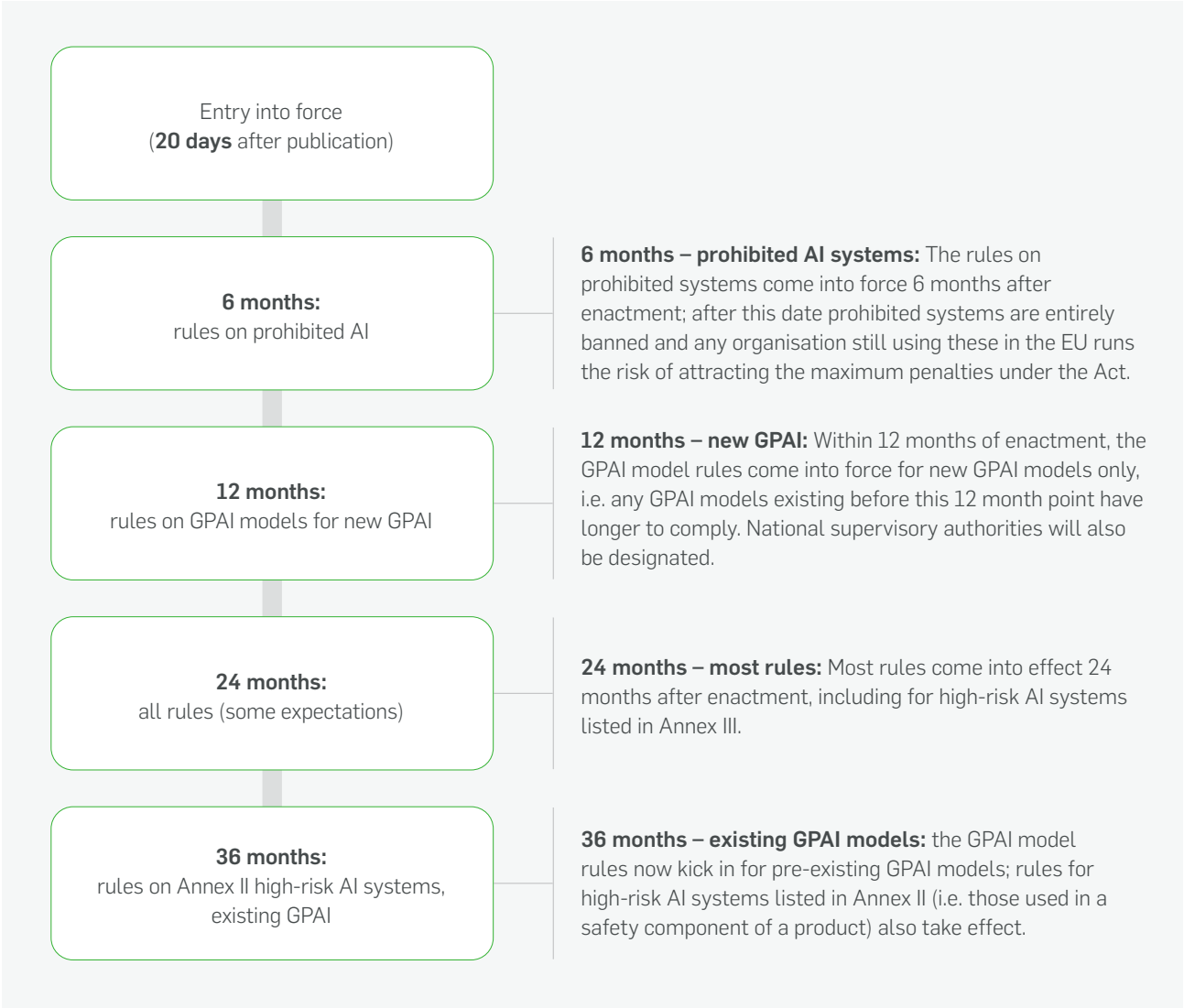
   Where the provider of a high-risk AI system is established outside the EU, it must appoint an authorised representative in the EU.

9. **What about a scenario where a US organisation (not established in the EU) develops and makes available a content-generation AI system under its trade mark on its website, which EU users are able to access. Is that US organisation subject to the Act in respect of the system?** Let's go back to the scope. If a non-EU provider of an AI system (or GPAI model) first places on the market or puts it into service in the EU, then the Act applies. In this scenario has the US organisation placed it on the market or put it into service in the EU? These are the key questions.

   Ultimately, it will depend upon the factual circumstances. However, if the organisation is not directing this at EU users, it is not intended for EU users (e.g. its website terms and conditions state that you must reside in the US to be able to use this feature), nor does the organisation tailor any of its offering to EU users in any other way (e.g. have a French language page),then there could be an argument that the Act doesn't apply as it is not placing the AI system on the market or putting it into service. Think along the same lines of the targeting criterion under the GDPR, where in order to be caught by the extra-territorial Article 3(2)(a) goods and services test, the individuals in the EU need to be targeted. However, how this plays out remains to be seen.

THE WHEN

10. Is there a transitional period under the Act? Yes, while the Act is generally enforceable 24 months after entry into force, there are some notable exceptions as implementation is phased in:



11. Can we expect to see other legislation or guidelines in the future? Yes. It does not stop at the Act. The Act allows the Commission to introduce delegated acts and implementing acts.

This includes delegated acts on the definition of AI system, high risk AI system exemptions and use cases, GPAI models with systemic risk thresholds and technical documentation requirements for high risk AI systems and GPAI models. It also includes implementing acts to approve codes of practice for GPAI and generative AI watermarking, and operational rules for AI regulatory sandboxes.

It does not stop there. The Commission can also provide guidance on specific areas, including practical guidance on determining if an AI system is high risk, the application of definition of an AI system, high risk AI system provider obligations, and the practical implementation of transparency obligations in relation to AI systems that present a transparency risk.

As for other regulators, the AI Office is expected to draw up codes of practice with respect to GPAI model provider obligations. National competent authorities will also likely publish guidance. So really it is watch this space.

THE ENFORCEMENT LANDSCAPE

12. How will the AI Act be enforced? Broadly, there are three prongs.

- Each Member States must designate a national supervisory authority and a market surveillance authority for the purposes of enforcing the Act. There is the question of who this will be – a new agency, the privacy regulator or another regulator? It is likely to vary across the EU, which coulld lead to differing enforcement approaches or priorities, for example, Denmark has appointed the Danish Digital Agency as its national supervisory authority, whereas Italy has stated it will appoint the Italian data protection authority.
- To help tackle this, while the Act has not followed the GDPR "one-stop shop" example, it sets up an AI Board, composed of one representative of each Member State, to help ensure consistent application of the Act through the provision of non-binding advice, recommendations, and sharing of technical expertise.
- The AI Office has also been assigned to police General-Purpose AI (GPAI) models and systems.

13. What are the potential penalties for breaches of the Act? Like the GDPR, not all breaches are treated the same. However, fines for the most egregious breach of the Act (using prohibited AI systems) are higher, being a maximum fine of is EUR 35 million or 7% of worldwide annual turnover, whichever is higher.

Non-compliance with prohibited AI
Up to €35 million or 7% worldwide annual turnover

Non-compliance with other obligations
Up to €15 million or 3% worldwide annual turnover

Supplying incorrect or misleading information to regulators
Up to €35 million or 7% worldwide annual turnover

14. What about private enforcement? While the Act does not explicitly provide for a private right of action, it is part of a package of EU legislation, supplemented by an amended Product Liability Directive and the new AI Liability Directive. Whereas the Act focusses on safety and the prevention of harm associated with AI systems. In contrast, these two Directives provide routes for redress following harm caused by AI systems. Think of it as a tripartite regime that will 'adapt liability rules to the digital age'.

The Product Liability Directive compromises of a strict liability regime giving redress for death, personal injury or property damage caused by defective products. This has been amended to make it clear that the rules cover AI systems and products that integrate AI systems.

The AI Liability Directive also provides rules for non-contractual fault-based liability for damage caused by AI, particularly high risk AI systems. One of the issues is that harm can be difficult to attribute to AI systems, what is known as the "black box" effect. Consumers or businesses may find it difficult to understand whether or not the damage resulted from the AI system, and to gather enough evidence to start proceedings. In short, the objective of this is to make it easier to sue the providers or deployers of an AI system for damages caused by that system.

THE PRACTICAL STEPS

15. What should organisations be practically thinking about?

- Identify your AI. Conduct an AI mapping exercise to understand what AI systems are being used in the organisation. Determine if the systems being used constitute an AI system.
- For organisations outside the EU, perform a scoping exercise. Assess whether and to which extent AI systems have a particular EU nexus that might trigger the Act.
- Assess risk. For AI systems in scope, determine which risk-level that AI system sits in.
- Determine your role, are you a provider, importer, distributor or deployer? Accordingly determine your compliance obligations. Map mitigations.
- Design and develop AI governance: focus on policies, process, people, resources, community. Ask yourself these questions: What teams need to be involved? What types of policies/ processes/ documentation are needed? Can you build from existing governance practices (e.g. privacy)? What are the technical and knowledge gaps you need to bridge? What types of additional tools are needed?
- Operationalise AI governance.

THE ANNEX

Risk Classification	Examples	Key Obligations	
		Providers	Deployers
Unacceptable Risk	▪ Behavioural manipulation ▪ Social scoring	Prohibited entirely.	Prohibited entirely.
High Risk	▪ Biometric emotion recognition systems ▪ Education (access and evaluation) ▪ Workplace AI/recruitment or candidate selection ▪ Credit scoring ▪ Life and health insurance pricing ▪ Safety components of certain products	▪ Quality management system ▪ Risk management ▪ Design requirements ▪ Data governance ▪ Documentation requirements ▪ Reporting and record requirements ▪ Conformity obligations ▪ AI literacy	▪ Comply with provider instructions (and use in DPIA) ▪ Inform individuals *(employees, decisions)* ▪ Input data (if have control) ▪ Human oversight ▪ Reporting ▪ Retention of logs ▪ AI literacy
Transparency Risk	▪ Chatbots ▪ AI systems generating/ manipulating content ▪ Deepfakes ▪ Emotion recognition systems	▪ Transparency *(if not obvious)* ▪ Identify AI-generated content (technical measures) ▪ AI literacy	▪ Transparency *(deepfakes, public interest text content, emotion recognition systems)* ▪ AI literacy
All other AI systems (minimal risk)	▪ Grammar-checking ▪ Shopping recommendations	▪ AI literacy	▪ AI literacy

FOR MORE INFORMATION

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

CHLOE KITE

+44 20 7903 1206
chloe.kite@weil.com

WEIL.COM

#97864250

Weil