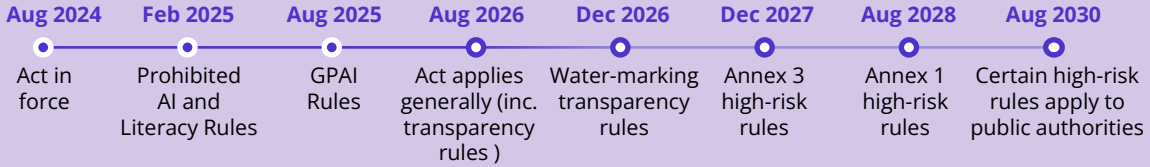
Digital Regulation Essentials: *The EU AI Act*

The EU AI Act entered into force on 1 August 2024. It has a phased transition and has generally applied since 2 August 2026. Here we highlight some of the key aspects of the EU AI Act (the Act).

Timing

The Act entered into force on 1 August 2024. As a Regulation, it is directly applicable in Member States. The Act has a phased transition, although it has applied generally since 2 August 2026. N.B.: The AI Omnibus delayed some of the original timings.



Overview – how the Act works

Applies to providers and users of AI:

Applies across the AI supply chain, whether you provide, use (deploy), distribute or import AI. Applies to all sectors (subject to some exceptions – e.g. military, R&D & some open source).

High fines:

The Act has a range of enforcement provisions including high fines which range from €35 million or 7% of worldwide annual turnover to €7.5 million or 1.5% (depending on the infringement).

Multi-level exposure:

In-scope organisations must consider a range of issues, from ongoing compliance adjustments to strategic decision-making on product development and launches within the EU.

Risk based rules:

Different rules apply depending on the risks posed by the AI. Some AI is prohibited, some is high-risk (attracting substantial obligations) and some have additional transparency rules. Many AI Systems have minimal or no obligations.

Specific GPAI rules:

General purpose AI (GPAI) models have their own rules under the Act which are enforced by the Commission (via the AI Office) rather than Member States. Powerful models posing a systemic risk face additional rules.

AI omnibus put regime under review :

The AI Omnibus changed parts of the Act. This was part of a wider Digital Omnibus review - a simplification package produced in part due to pressure on the Commission to lighten the EU's regulatory burden to help it remain competitive.

Who is in scope?

Providers

A developer of an AI system or GPAI model (or someone who has it developed) who places that AI on the market or puts it into service in the EU under its own name or trademark (whether for payment of free). Also in scope where the output from its AI is used in the EU.

Deployers

An EU based user of an AI System (where use is under its authority and not in a personal capacity). Also in scope where the output from its AI is used in the EU.

Others in scope

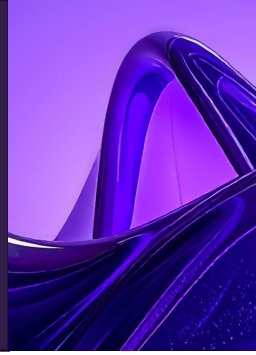
The Act impacts many in the AI supply chain. Some importers, distributors and manufacturers therefore also face obligations under the Act.

What does this mean in practice?

One AI product may be regulated in different ways under the Act:

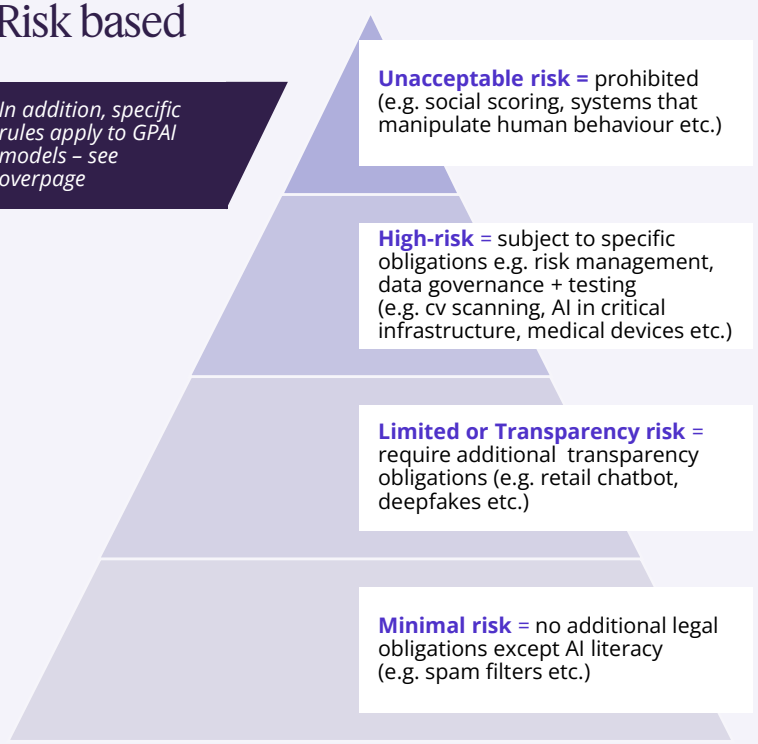
- **Multiple parties may be involved:** An AI product may be an AI System based on a GPAI model that has been configured by the user/customer.
- **Different obligations under the Act may apply simultaneously:** Depending on the type of AI and its use case, one product may trigger the GPAI, high-risk, transparency and literacy rules (although the latter have changed under the AI Digital Omnibus).
- **Actions can change roles and obligations under the Act:** E.g. a deployer of a high-risk AI System who heavily modifies that system or attaches its own brand could become a provider.
- **KEY TAKEAWAY:** Carefully check your role, actions and whether any exemptions are relevant before confirming which obligations apply.

Digital Regulation Essentials: *The EU AI Act*



Risk based

In addition, specific rules apply to GPAI models – see overpage



AI Omnibus

The AI Omnibus made changes to the Act, including delays to the application of the high-risk rules and (some) transparency provisions, narrowing what is in scope for Annex 1 high-risk AI, removing duplication with sector rules, giving more authority to the AI Office and helping SMEs. See our blog for more details.

What does the Act target?

AI Systems posing unacceptable risk

Some AI practices carry so much risk they are banned. Prohibited AI includes AI which:

- Deploys subliminal or deceptive techniques to materially distort behaviour and impair ability to make an informed decision (likely to cause significant harm)
- Exploits the vulnerabilities of people (due to their age, disability, social or economic situation) to affect their behaviour (reasonably likely to cause significant harm)
- Social scoring based on social behaviour or personal characteristics
- Certain biometric categorisation systems and real-time biometric use in publicly accessible spaces for law enforcement unless strictly necessary for specific listed purposes and subject to conditions
- Untargeted scraping of facial images from the internet or CCTV footage to create or expand facial recognition databases
- Infers emotions in certain circumstances (work, education) except if for medical or safety reasons

Check the codes and guidance

The Act envisages a range of codes of practice, guidance and standards to assist with compliance. A number of these are now in agreed form.

High-risk AI Systems

Some AI Systems have high-risk uses cases and are heavily regulated. These include AI Systems which are:

1. products (or safety components of products) falling under the EU's product safety legislation (e.g. toys, aviation, cars, medical devices, lifts etc.) listed in Annex 1 and which require a third-party conformity assessment. The AI Digital Omnibus changes narrow down what qualifies as a safety component; or
2. in the areas listed in Annex 3 and which pose a significant risk of harm to the health, safety or fundamental rights of natural persons. The list includes biometrics (where permitted), safety components in critical infrastructure, education, employment, essential services (both public e.g. welfare, and private e.g. credit scoring and life insurance), law enforcement, migration, judiciary etc.

Exemptions: Exemptions apply where the AI System was already on the market before the rules started to apply.

Obligations: Providers, deployers, importers and distributors of high-risk AI Systems are all subject to a wide range of obligations, with providers facing the most onerous obligations. Key provider provisions include obligations relating to:

- risk management and quality management systems;
- ensuring data used to train, validate or test the AI System are relevant, representative and (to the extent possible) free of errors and complete;
- technical documentation, record-keeping and event logs;
- transparency, human oversight, accuracy, robustness and cybersecurity; and
- conformity assessments

More details on the high-risk obligations, including the high-risk guidance, are available here and here.

Could you be an accidental provider? Deployers and other third parties should avoid actions which mean they would be classified as a provider. Examples include putting their name/mark on a high-risk AI System or making substantial modifications to it.

Digital Regulation Essentials: *The EU AI Act*

What does the Act target?

AI creating transparency risks:

Some AI Systems present particular risks which require additional transparency obligations, although different triggers and obligations apply to providers and deployers. It is also important to check if an exemption applies.

- **Provider obligations:** Providers must build transparency into their AI Systems. It must be clear when people interact directly with an AI System (e.g. chatbots) and AI generated synthetic audio, image, video or text content must be marked (e.g. watermarked).
- **Deployer obligations:** Deployers must tell people where AI is used for emotion recognition or biometric categorisation, to generate or manipulate text published to inform the public on matters or public interest or if there are deepfakes.

The Commission has published both guidance and a Code of Practice to help organisations comply with the transparency rules. Organisations can voluntarily sign up to the code.

More information

For more information on the Act, see our general AI Act briefing, our briefing for AI providers and our AI blogs.

GPAI Models:

- The GPAI model rules were a late addition to the Act and proved controversial. They are intended to cover the most powerful AI models including large language models like ChatGPT.
- There are specific obligations on providers of GPAI models and their authorised representatives.
- For example, providers must draw up technical documents, comply with EU copyright law and disseminate summaries about content used for training etc. (although some exemptions do apply for free publicly available open source models)
- GPAI models with systemic risk (meaning they have high impact capabilities – where cumulative computing power used for training is greater than 10^25 flops) have more stringent obligations.
- These include notification to the Commission (who keep a list), model evaluations, obligations to assess/mitigate systemic risks, conduct adversarial testing, report serious incidents and ensure the cybersecurity of the model and its physical infrastructure.
- The Commission has published a Voluntary Code of Practice which a number of organisations have signed. The Code has been designed to aid compliance. The Commission has also published guidance and templates to aid compliance. For more information see our blogs here and here.

Digital Regulation at Slaughter and May

Our Digital Regulation practice covers the full spectrum of digital rules, from AI regulation competition-focused platform regulation, online harms and content regulation, to data access and portability. Clients look to us to offer practical, risk-adjusted advice that helps them navigate this ever more complex landscape – and to innovate at speed.

For more information, see our *Digital Regulation Practice* page or digital Blog *The Lens*.

Laura Houston
Partner
+44 (0)20 7090 4230
laura.houston@slaughterandmay.com

Will Manley
Head of Digital Regulation
+32 (0)2 737 9431
will.manley@slaughterandmay.com

Jordan Ellison
Partner
com+32 (0)2 737 9414
jordan.ellison@slaughterandmay.com

Natalie Donovan
Head of Knowledge, Tech and Digital
+44 (0)20 7090 4058
natalie.donovan@slaughterandmay.com

5 key questions to ask

01
Do I understand how my organisation and its key suppliers are using AI?

02
Where do I sit in the AI supply chain? Do I understand my dependencies, obligations and areas of exposure?

03
How am I assessing my AI partners, suppliers and third-party technologies? What due diligence, piloting and/or testing am I carrying out?

04
Does the Act impact my longer-term product planning?

05
What is my compliance approach, and does it fit with my wider risk appetite? Do I need a global approach?

SLAUGHTER AND MAY

This material is for general information only and is not intended to provide legal advice. 2026 © Slaughter and May