AI Act

The AI Act, which entered into force on 1 August 2024, marks a new era in AI regulation within the EU. This landmark legislation establishes a comprehensive framework designed to ensure that AI systems are safe, transparent and respectful of fundamental rights. Transparany rules and enforcement over GPAI providers took effect on 2 August 2026. The obligations for high-risk AI apply as of 2 December 2027 and 2 August 2028.

Scope

The AI Act applies to providers, deployers and other participants in the AI value chain, such as importers and distributors, when AI systems are placed on or used in the EU market. This includes situations where the output of an AI system is used in the EU or where individuals affected by an AI system are located in the EU, regardless of the location of the participants.

General-purpose AI (GPAI)

The AI Act also imposes specific requirements for the provision of GPAIs. GPAIs are AI systems that serve as versatile models, capable of being adapted for various applications, such as language processing for chatbots and translation services, image recognition for medical diagnostics and autonomous vehicles, and predictive analytics for financial forecasting and personalised marketing. All providers of GPAIs must comply with transparency obligations, including the provision of technical documentation and details about training data. Providers of 'systemic risk' GPAIs face additional requirements, such as implementing cybersecurity measures and reporting on energy efficiency and serious incidents (models with high-impact capabilities that could pose large-scale harms to e.g. health or democratic processes).

What is an AI system?

An AI system is a machine-based system that, for explicit or implicit purposes, infers from the input it receives how to generate output such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptability once deployed. For example, AI agents can independently make decisions and carry out tasks on behalf of a user or another system.

Note: Several key definitions in the AI Act, such as 'AI system', are both new and broad. Their precise scope will necessitate further clarification over time.

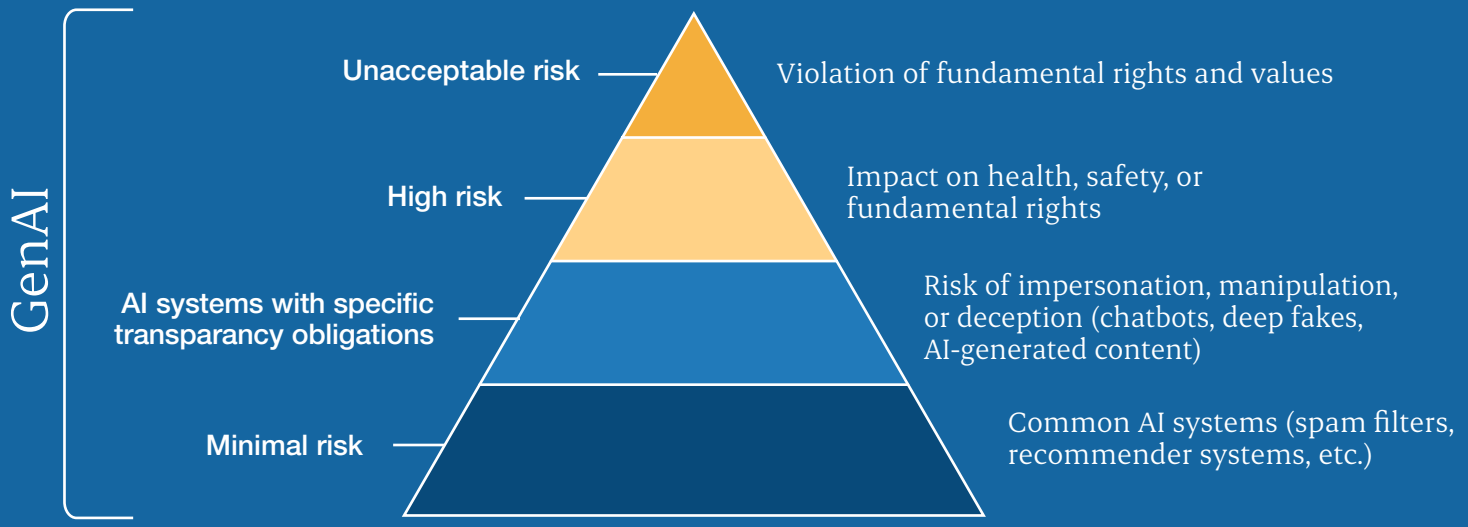
Generative AI (GenAI)

A subset of GPAI is Generative AI, which focuses specifically on creating new content, such as text, images or music based on its training data. The AI Act introduces additional requirements for this subset, including the disclosure of AI-generated content and copyrighted material used in training datasets, as well as designing the model so as to prevent generation of illegal content.

Risk classifications of AI systems

The AI Act sets out obligations for providers and deployers depending on the level of risk posed by AI, classifying AI systems into minimal risk, specific transparency risk, high-risk, and unacceptable risk categories.

Minimal risk AI is not subject to specific regulation. The AI Act introduces specific transparency obligations to ensure that users are informed when interacting with AI. High-risk AI must meet strict standards, including fundamental rights impact assessments and cybersecurity measures, while unacceptable risk AI is prohibited.



NautaDutilh

Enforcement

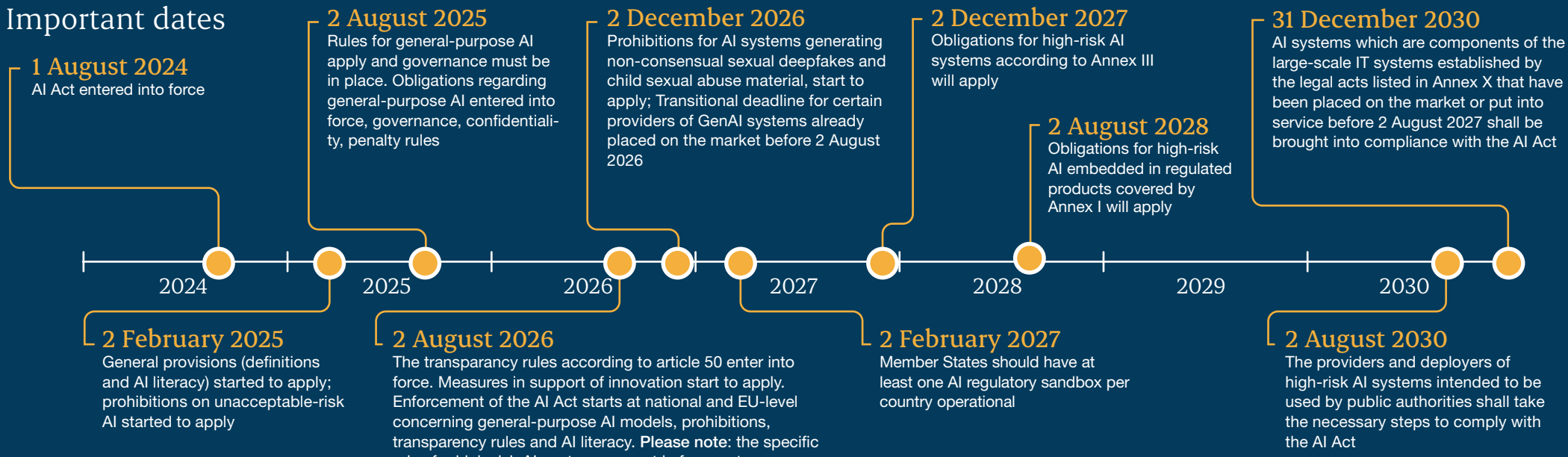
The AI Act relies on a two-tier enforcement mechanism:

- **EU level -** The European Commission plays a central role through the newly established AI Office, which coordinates policy at EU level and supports the development and use of trustworthy AI, while protecting against AI risks.
- **National level -** On 20 April 2026, the draft Dutch AI Implementation Act (*Uitvoeringswet AI-verordening*) opened for consultation until 1 June 2026. The draft designates nine sector regulators and the Dutch Data Protection Authority (DDPA) as coordinating authority.

Penalties

The AI Act allows for fines based on a percentage of the global annual turnover or a fixed amount, whichever is higher, with penalties ranging from EUR 7.5 million or 1.5% to EUR 35 million or 7%, depending on the infringement and company size. Proportional caps on fines for small and medium-sized enterprises (SMEs) and start-ups are included to avoid stifling innovation and to ensure a balanced governance framework.

Important dates



What this means for you

A comprehensive AI governance framework is essential to manage and mitigate the risks associated with AI. The following steps should be considered to ensure effective governance:

1. **Mapping** - Create a detailed overview of all AI systems within the organisation, including internal and third-party tools. Evaluate associated risks (ethical, legal, operational) and identify relevant stakeholders to understand their interests and concerns regarding AI.
2. **Policy development and governance** - Assign responsibilities and establish rules and guidelines for the use of AI within the organisation. This includes ethical guidelines to ensure transparency and accountability, data protection policies to safeguard data integrity and confidentiality, compliance with relevant laws and technical standards to ensure safe and ethical AI operations, and AI literacy. Governance over the use of AI is crucial to maintain trust, mitigate risks, and ensure responsible innovation.
3. **Communication** - Ensure employee AI literacy and awareness of AI policies through training sessions and updates. Communicate these policies to external stakeholders, such as customers and regulators, to build trust and mitigate reputational risk. Clearly inform users when they are interacting with AI-generated or AI-manipulated context.
4. **Compliance** - Ensure that all AI systems comply with established policies through regular audits. Integrate compliance into daily operations with staff training and control mechanisms and conduct regular assessments to verify ongoing compliance and identify emerging risks.

Contact

Our Technology group helps clients understand how AI legislation will affect them and offers tailored strategic advice.



Vincent Wellens | partner
T. +352 621 15 61 78
E. vincent.wellens@nautadutilh.com



Sven Uiterwijk | partner
T. +31 6 20 21 05 70
E. sven.uiterwijk@nautadutilh.com

NautaDutilh