Decoding the AI Act: Key Elements

The European Union's Artificial Intelligence Act (AI Act), one of the first and likely the most comprehensive regulation of AI systems in the world, entered into force on 1 August 2024. The AI Act will affect an incredibly wide range of AI systems used in the EU, and subject AI system providers to a range of compliance and transparency obligations reflecting a risk-based approach.

Certain high-risk AI applications will be prohibited outright, while other AI systems will be subject to obligations that vary depending on the risk associated with them. The AI Act, despite the concern that its strict rules may stifle AI development in the EU, is expected to exert a strong influence on the development of the regulation of AI around the world.

We will decode the the AI Act and its likely impact for affected businesses in a series of client alerts. This first alert provides a general introduction to the AI Act, highlighting:

(i) the AI Act's broad definition of AI systems;

(ii) the obligations that providers and deployers of AI systems that can affect EU citizens must comply with;

(iii) the risk-classification of AI systems; and

(iv) the AI Act transition periods.

The reach and complexity of the AI Act and the tight transition periods suggest that businesses should already now start considering compliance measures, including the classification of their AI systems, to minimise the risk of hefty fines.

AI systems in scope

The Act covers all "AI systems" which it defines with the help of four parameters: autonomy; adaptiveness; inference (which can cover logic or knowledge-based approaches as well as machine learning); and the ability to influence physical or virtual environments.

This definition is aligned with the definition used by the OECD to "*ensure legal certainty*" and "*facilitate international convergence*". Still, the definition is broad and technology changes rapidly, which will make it challenging for businesses to identify all stand-alone systems or AI components of their products or services that fall within the scope of the AI Act. For instance, the definition of AI system includes machine-based systems that "*may*" exhibit adaptiveness. If adaptiveness is not a mandatory characteristic, does that imply that the AI Act will also cover non-adaptive AI systems, such as rule-based chatbots or static pricing mechanisms? Further guidance will be required to provide greater legal certainty on the systems that are covered.

The AI Act separately defines "General Purpose AI" (**GPAI**) , which includes large generative AI models, as AI systems characterized by their generality and capability to competently perform a wide range of distinct tasks. As GPAIs are subject to additional rules and obligations, this vague definition is bound to raise many borderline questions which, again, will have to be resolved by future guidance or enforcement practice.

Applications out of scope

The AI Act excludes specific AI applications from its scope. Free, open-source AI systems are excluded if they do not qualify as high-risk AI systems (see below). In addition, the AI Act does not apply to AI systems designed exclusively for military or defence purposes or for scientific research and development.

A tiered approach based on risk

The EU legislator classifies AI systems based on their perceived potential of inflicting harm: the higher the risk, the stricter the obligations.

The AI Act classifies systems into four categories:

- Prohibited AI systems are banned for posing risks to fundamental rights. These include AI systems performing biometric categorization and social scoring, with exceptions for law enforcement.
- High-risk AI systems, which are subject to the most stringent rules, are those integrated into safety-critical products or used in sensitive areas like education, employment, and healthcare.
- Low-risk AI systems, which are all systems which do not fall under the other categories. This includes, e.g. most types of chatbots.
- Minimal or no risk AI systems, which are permitted without restrictions.
- GPAI systems with "systemic risks" or "high impact capabilities" face enhanced regulation, including evaluations and cybersecurity measures.

Wide range of compliance obligations

The AI Act uses an expansive toolset of risk-regulation mechanisms that range from outright bans (for Prohibited AI systems) to conditional access subject and prior approval (for high-risk systems). The AI Act also envisages the deployment of regulatory sandboxes and soft regulation through the use of codes of conduct to contribute to safe uses of AI systems.

Reflecting the AI Act's risk-based approach, the most comprehensive obligations apply to high-risk systems:

- **High-risk systems** are subject to the most stringent requirements, including risk management systems, technical documentation, instructions for use, conformity assessments, transparency obligations, human oversight, accuracy requirements, robustness, cybersecurity, post-market monitoring, and incident reporting.
- **GPAI systems** must comply with general requirements based on their intended use. Deployers of such systems are responsible for using the GPAI systems in compliance with the established guidelines and ensuring that their implementation aligns with the intended purpose and ethical standards.
- **Low-risk systems** are primarily subject to transparency obligations and are encouraged to adopt codes of conduct.
- **Minimal or no risk AI systems**: refers to systems where risk is particularly unlikely (such as spam filters), which are generally exempt from most obligations.

All AI operators must ensure compliance

The Act imposes compliance obligations on all operators in the AI value chain, from AI system developers to users and market players commercialising AI systems on a stand-alone basis or when integrated into another product or service. We will look at the obligations applicable to different stakeholders in a subsequent alert.

Extra-territorial reach

As with other instruments forming part of the EU's Digital Strategy, the AI Act applies not only to businesses established or located in the EU. What matters is whether the AI system can have an impact on EU citizens, from wherever it is deployed. Accordingly, even if an AI system is operated outside the EU but its output is used within the EU, the system falls within the scope of the AI Act.

Sanctions for non-compliance

The AI Act sets out different maximum fining levels for non-compliance. These range from fines of up to EUR 35 million or 7% of worldwide turnover for use of prohibited AI systems, to fines of up to the higher of EUR 7.5 million or 1% of worldwide turnover for information notification breaches.

Timing

The Act formally entered into force on 1 August 2024. However, it will be applied in phases, with the following compliance deadlines:

February 2025	August 2025	August 2026	August 2027
Enforcement of prohibited AI systems .	Obligations of GPAI systems will take effect, with the exception of GPAI models that were placed on the market prior to this date.	Most other obligations of the AI Act will take effect from this date.	High-risk AI systems, not defined in Annex III but used as safety components or standalone products, must undergo third-party conformity assessments.

Key takeways

- Developers should ensure that new AI tools are built to comply with the new rules. Similarly, businesses that commission or procure AI tools (including tools with AI components) should screen these tools for compliance with the AI Act. Any contracts that are concluded should clearly allocate compliance responsibilities.
- Businesses should review their existing AI systems (whether stand-alone or integrated in products or services) and identify those that may fall within the scope of the Act, and if so, whether they qualify as high-risk. This will allow the determination of future obligations under the AI Act.
- Businesses are advised to leverage, where possible, existing legal, technical or organisational measures required by other rules (e.g., data protection, DSA) to comply with the AI Act's requirements.
- Businesses should educate staff and anyone involved in designing or operating AI systems on the requirements of the Act and implement adequate policies and procedures to ensure compliance.

KEY CONTACTS

Andreas Reindl
Partner
areindl@vbb.com
+32 (0)2 647 73 50

Thibaut D'Hulst
Counsel
tdhulst@vbb.com
+32 (0)2 647 73 50

Malik Aouadi
Associate
maoudi@vbb.com
+32 (0)2 647 73 50