TaylorWessing

AI Act step plan

Overview

- The EU Artificial Intelligence Act (AI Act) represents a significant step forward in the regulation of AI.
- It introduces a risk-based approach. This means that it applies different requirements to AI systems and general-purpose AI (GPAI) models depending on the risks they pose to health, safety, and fundamental rights.
- The AI Act will enter into force in stages, starting on 1 August 2024.

From 1 August 2024	■ Entry into force
From 2 February 2025	■ Ban on prohibited AI practices & introduction of AI literacy requirements
From 2 August 2025	■ Obligations relating to GPAI models ■ Notification procedure, EU governance and appointment of national regulators
From 2 August 2026	■ Obligations relating to high-risk AI systems under Annex III ■ All other rules unless otherwise specified
From 2 August 2027	■ Obligations relating to high-risk AI systems that are products or safety components of products covered by legislation in Annex I ■ Obligations for GPAI models placed on the market before 2 August 2025
From 2 August 2030	■ Duties for high-risk AI systems that are used by certain public authorities and were put into circulation before the start of application 2 August 2025
From 31 December 2030	■ Obligations relating to AI systems in European information systems in the areas of freedom, justice and securit placed on the market or used before 2 August 2027

For other AI systems that were placed on the market or put into operation before the start of applicability, the AI Act will only apply where significant changes are made.

- The AI Act will also apply to entities outside the EU where the output by the AI system is used in the EU, or when the provider places an AI system on the EU market.
- Fines differ depending on violations but may reach up to EUR 35 million or 7% of a company's annual turnover, whichever is higher.

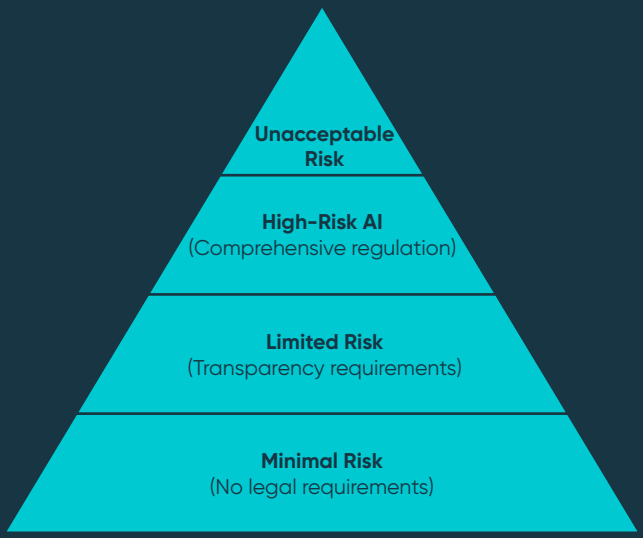
We recommend the following five steps to help you achieve compliance with the AI Act and other EU digital regulation:

STEP 1
AI mapping

- Carry out a **gap analysis** between the current status of compliance and the obligations deriving from the AI Act.
- As a first step, map your current and prospective use or development of AI by asking questions including:
  - which entities / departments use or develop what kind of AI systems and if so, for what purposes?
  - is there an AI policy in place already regarding development, distribution and use?
  - are internal responsibilities clearly assigned?
  - what are foreseeable risks for health, safety, fundamental rights?
  - what security measures are in place?

STEP 2
Risk assessment

- Assess which AI Act requirements apply. This requires a detailed analysis of the risk category of each AI system or model and the company's role for example, whether they are a provider, deployer, importer, distributor or product manufacturer in relation to relevant AI.
- The gap analysis and risk assessment will inform your governance requirements (STEP 4).
- Remember: you may have a lot to do in order to comply with the AI Act so focus on the areas of greatest risk.



Risk category: it is important to understand that the AI Act follows a risk-based approach. It divides AI systems into four groups and sets out rules for general-purpose AI (GPAI) models. GPAI models, also known as foundation models such as GPT-4, are AI models that are trained with a large amount of data and can be integrated into a variety of downstream applications.

Company's role: Most of the AI Act's obligations apply to providers of AI systems. However, users (deployers) are also regulated. Other addressees of the AI Act are importers, distributors, product manufacturers and authorized representatives of providers.

STEP 3
Resource and budget planning

- **Assign project responsibilities** to key personnel and have buy-in from the executive board.
- Allocate adequate resources. This should cover: additional personnel and administration, legal and IT costs (eg for data governance, technical documentation, record-keeping and cyber security). Legal costs as well as IT costs (e.g. for data governance, technical documentation, record-keeping, cybersecurity).
- **Integration with other compliance management systems is essential**. This means that it is important to consider existing approaches with regard to:
  - information security and risk management
  - outsourcing and vendor management
  - GDPR compliance and other data governance management, as well as
  - a company's code of conduct and ethics compliance

STEP 4
Implementation of an AI governance scheme

- Implement a targeted AI governance scheme based on the outcomes of steps 1 and 2. The higher the level of risk and subject to your role, the more obligations will apply. For example, for high-risk AI systems, obligations may include:

AI literacy	**Quality management system**
Risk management system	**Transparency obligations**
Technical documentation	**Data requirements**
Reporting	**Human oversight**
Registration	**Cooperation with authorities**
Conformity assessment	**Cybersecurity, accuracy and robustness**
Automatic recording of events	**Post-market monitoring**

- For deployers less intensive obligations apply including AI literacy, human oversight, data governance and transparency.

STEP 5
Stay up-to-date

- The requirements under the AI Act make it necessary for companies to continuously monitor regulatory developments, their AI system and model landscape and readjust their AI governance.
  - This means you will need to go through the **5 step** cycle on a regular basis.
  - The European Commission will adopt delegating and implementing acts, and develop guidelines to adjust the scope and refine specific requirements under the AI Act. It is **crucial for companies to keep track of these changes** and consider future guidelines and codes of practices from the new established AI Office and competent national authorities.
- Please note that the **AI Act is only one important piece of a cluster of horizontal and sectoral regulations regarding AI**.

  Other relevant legal acts that must be considered are the **General Data Protection Regulation** e.g. for AI training, the **Cyber Resilience Act** regarding AI cybersecurity requirements, the **Data Act** for AI-based IoT-devices or to train third-party AI, the **AI/Product Liability Directive** when AI systems cause damages, the **Digital Services Act** e.g. for AI content moderation and the **Directive on Copyright on the Digital Single Market** for licensing and compensation for rightsholders.

Your Contacts

Thanos Rammos, LL.M.
Partner, Berlin
+49 30 885636-118
t.rammos@taylorwessing.com

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Partner, Berlin
+49 30 885636-408
p.voigt@taylorwessing.com

Richard Gläser
Associate, Berlin
+49 30 885636-159
r.glaeser@taylorwessing.com

© Taylor Wessing 2024

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at www.taylorwessing.com/regulatory