EU AI Act - what to do when

TaylorWessing

1 August 2024

AI Act in force: initial steps for compliance

The AI Act is now in force and the first chapters will apply from 2 February 2025.

Objectives

- Implement organisational measures for compliance.
- Clarify roles and responsibilities within the organisation, particularly in relation to Chapter I (Scope and Definitions).

Actions

- Review and update contracts to define roles and responsibilities for providers, deployers and importers in accordance with the AI Act definitions.
- Determine whether you are classified as a 'provider', 'deployer' or other regulated party under the AI Act.
- Develop a compliance programme that focuses on identifying prohibited AI practices and high-risk AI systems, and how to replace or modify the former and manage the latter.
- Start training employees, focusing on the specific requirements for each type of AI system including AI literacy as required by Article 4.
- Ensure that contracts include clauses that provide flexibility to adapt to new harmonised standards as they develop, and consider termination rights if compliance cannot be maintained.
- Assess whether your AI systems or GPAI models fall under the provisions of the Act.
- Begin to identify the necessary departments and stakeholders for compliance.
- Integrate transparency measures for AI systems designed for direct human interaction, ensuring that users are aware when they are interacting with AI.

Prepare for evolving standards

- Familiarise your team with existing international standards, such as EN ISO/IEC 22989:2023 (AI concepts and terminology) and EN ISO/IEC 23053:2023 (Framework for AI systems using machine learning). Start aligning your AI terminology and frameworks with these standards to ensure global consistency and compliance.

Transparency measures

- Develop a transparent stakeholder information system that communicates the purpose, capabilities and risks of your AI systems early in their lifecycle.

2 February 2025

Implementation of initial chapters (Chapters I and II)

Chapters I and II of the AI Act, including the scope, AI literacy requirements and prohibitions of certain AI practices, come into effect.

Objectives

- To ensure compliance with the scope and prohibited practices set out in Chapters I and II.

Actions

- Implement policies to avoid engaging in AI practices prohibited under Article 5, such as:

1. **Subliminal manipulation** (e.g. AI-driven dark patterns in digital interfaces).
2. **Exploitation of vulnerabilities** (e.g. targeting vulnerable groups with manipulative AI technologies).
3. **Social scoring** (e.g. using AI to create unwarranted classifications or rankings of individuals based on behaviour unrelated to the context in which it was collected).
4. **Predictive policing** (e.g. AI systems that predict individual criminal behaviour based solely on profiling).
5. **Scraping for facial recognition** (e.g. non-consensual collection of data from the internet for facial recognition databases).
6. **Emotion recognition in sensitive environments** (e.g. emotion-detecting AI in workplaces or educational settings); exceptions apply.
7. **Biometric categorisation** (e.g. classifying individuals by sensitive personal characteristics such as race or religion based on biometric data).
8. **Real-time biometric identification in public spaces** (e.g. facial recognition in public areas without explicit consent or lawful purpose).

- Use available guidance to assess and classify your AI systems, with a particular focus on identifying AI systems or practices that may be high-risk AI systems.
- Start developing documentation and transparency measures for AI systems used in the EU market.

Prepare for evolving standards

- Continue to familiarise your team with fundamental standards, including ISO/IEC 23894 (Guidance on Risk Management), to ensure that your AI systems are developed and managed with a robust risk management framework.

Transparency measures

- Implement transparency policies to inform users of potential biases and limitations in AI systems, particularly those that interact directly with humans. Consider the implications of over-transparency and apply the need-to-know principle to protect sensitive information.

2 May 2025

Finalisation of codes of conduct and guidelines

Additional provisions of the AI Act begin to apply, including obligations for general purpose artificial intelligence (GPAI) models and provisions on notified bodies and governance structure. Also provisions related to EU-level institutions under the AI Act come into effect.

Objectives

- To assess whether certain AI models or AI systems can be exempted from the AI Act, and to ensure compliance with applicable timelines.

Actions

- Implement procedures to comply with GPAI obligations as described in Chapter V of the AI Act.
- Use the grandfather clause (Article 111) to manage GPAI models and AI systems already placed on the market.
- Consider utilising other provisions of the grandfather clause as well: (other than large-scale IT systems referred to) placed on the market before 2 August 2026, the AI Act will only apply if these systems undergo significant design changes. However, for AI systems intended for public authorities, compliance with the AI Act must be ensured by 2 August 2030, regardless of any design changes.
- This means that while commercial high-risk AI systems are exempt from immediate compliance unless modified, public-sector systems face a hard deadline of full compliance by 2030, even if they remain unchanged.
- Start implementing a comprehensive risk management system for high-risk AI systems, including testing, validation and risk analysis.
- Ensure that data governance and quality management processes are in line with upcoming standards (e.g. ISO/IEC 5259), which will be crucial to ensure compliance and maintain system reliability.
- Implement regular monitoring and reporting systems for AI systems, with a focus on high-risk categories.
- Adjust contracts to include clauses addressing AI system transparency and termination rights if the system fails to comply.
- Use the provisions of Article 111 to manage compliance timelines effectively, particularly for AI systems and GPAI models placed on the market before specific deadlines.
- Ensure that systems producing or manipulating synthetic content are properly labelled, and that any are disclosed as required by Article 50.

Transparency and labelling

- For systems that generate synthetic content, such as those used in generative AI, implement mechanisms to label content as AI-generated (in accordance with Article 50 of the AI Act).

High-Risk AI to-do's

- Establish human oversight mechanisms for high-risk AI systems, ensuring that decisions made by the AI can be monitored and corrected by human operators if necessary.

Prepare for evolving standards

- Finalise preparations for logging and audit trails in line with prEN ISO/IEC 24970 (AI System Logging) to enhance traceability and accountability within your AI systems.

Transparency measures

- Incorporate ongoing monitoring and reporting into your transparency measures, ensuring that any issues related to the AI system's operation or data handling are promptly addressed and communicated to stakeholders.

Prepare for future compliance deadlines

- Providers of high-risk AI systems intended for government must ensure compliance by 2 August 2030, if placed on the market before 2 August 2026. GPAI models placed on the market before 2 August 2025 should be compliant by 2 August 2027, and those placed on the market thereafter must comply immediately.

Ensure correct classification

- Ensure that all GPAI models and high-risk AI systems are correctly classified when first placed on the market, and regularly updated if there are significant design changes.

2 August 2025

Enforcement of additional provisions begins

Develop and finalise internal codes of conduct and guidelines that align with the AI Act's requirements. Check for discrepancies with the codes of conduct and codes of practice developed by the AI Office.

Objectives

- Develop comprehensive codes of conduct (CoC) and codes of practice (CoP) to ensure compliance with the AI Act, particularly for high-risk AI systems.
- Prepare for full compliance, focusing on transparency, ethical guidelines, especially for high-risk AI systems.

Actions

- Review and adapt the CoC and CoP already drafted or developed at this time by the AI Office and relevant authorities.
- Where necessary, create internal guidelines that complement the CoC and CoP. These guidelines should focus on the specific obligations under the AI Act, especially for high-risk AI systems, and ensure that they are communicated effectively internally.

Some elements for a Coc or CoP

- Clear objectives and KPIs to measure compliance with the AI Act.
- Provisions for ethical AI, drawing on the Union's ethical guidelines for trustworthy AI.
- Consideration of environmental sustainability impacts of AI systems.
- Promotion of inclusivity and diversity in AI design and development, with a focus on protecting vulnerable groups.
- Regular reporting and monitoring of the implementation efforts.
- These CoC should be developed with flexibility to adapt to future changes in standards or legal requirements.
- Develop guidelines tailored to the needs and risks specific to SMEs. These should reflect the differing obligations for smaller providers and deployers under the AI Act, promoting the voluntary adoption of best practices and reducing administrative burdens.

Build in flexibility for evolving standards

- Ensure that contracts, CoC and CoP include mechanisms for adapting to future changes in harmonized standards. For example, incorporate adaptability clauses in contracts to manage evolving standards and requirements.

High-Risk AI systems documentation

- For high-risk AI systems, ensure that all technical documentation is detailed, up-to-date, and includes:
  - Descriptions of design and development processes.
  - Data sources and methodologies.
  - Algorithms and their decision-making frameworks.
  - Risk management measures and mitigation strategies.

This documentation must be ready for external audits and conformity assessments as required by the AI Act.

Prepare for evolving standards

- Get your team ready for evolving standards such as prEN ISO/IEC 24029-2 (Robustness of Neural Networks - Part 2). Establish protocols to regularly assess and ensure the robustness of neural networks and other AI models, meeting future expectations for AI reliability and safety.

Establish transparency frameworks

- Develop transparency frameworks to ensure clear communication of AI system capabilities, limitations, and potential biases, especially for high-risk systems or those with direct human interaction. This should include:
  - Clear disclosure of decision-making processes.
  - Transparent labeling of AI-generated content, in line with CoC requirements for the detection and labeling of synthetic content (e.g. deepfakes).
  - Reporting mechanisms for stakeholders to assess the system's fairness and impact.

Monitoring and enforcement

- Ensure compliance through regular internal audits and collaboration with the AI Office and other relevant authorities. Implement comprehensive risk management, employee and third-party training, and regular audits to ensure AI compliance and ethical conduct. Maintain flexibility for evolving standards, with continuous improvement and collaboration with regulators and industry partners for responsible AI development.

2 August 2026

Full application of the Act

The AI Act is fully applicable, with all aspects of the law being enforced, including new conformity assessments.

Objectives

- Ensure full compliance with the AI Act, including all necessary conformity assessments.

Actions

- Conduct comprehensive conformity assessments for all high-risk AI systems in line with the AI Act and the guide's recommendations.
- Establish documentation and audit trails to demonstrate compliance, as recommended in the guide.
- Prepare for external audits by training employees and setting up audit-ready documentation, ensuring readiness for the 2030 deadline for large IT systems as per Article 111.
- Reassess contracts for flexibility to adapt to new harmonised standards, and consider including opt-out clauses for updates to maintain the grandfathered status of certain systems.

High-Risk AI to-do's

- Finalise all technical documentation, establish a rigorous post-market monitoring system, and prepare for external audits to ensure continuous compliance.
- By this date, ensure that your AI systems align with the finalised prEN ISO/IEC 42001 (AI Management System) and prEN ISO/IEC 8183 (Data Life Cycle Framework). Ensure that your AI management systems and data lifecycle management meet the new standards to maintain compliance.

Transparency measures

- Ensure that transparency requirements are met by documenting AI decision-making processes, maintaining clear and accessible records, and providing users with explanations of AI-driven decisions where necessary.

Comment

- Be prepared for potential delays in the availability of harmonised standards, and consider alternative solutions such as common specifications or regulatory sandboxes if standards are not available by this date.

2 August 2027

Compliance required for high-risk AI systems and GPAI models placed on market before 2 August 2025

All high-risk AI systems and GPAI models must comply with the AI Act's requirements.

Objectives

- Ensure full compliance of GPAI models and all high-risk AI systems, particularly those subject to significant design changes.

Actions

- Conduct regular internal audits, with corrective actions for non-compliance.
- Ensure that any significant changes to the design of high-risk AI systems are re-assessed for conformity, as required by Article 111.
- Prepare for potential external audits by notified bodies by aligning internal processes with the applicable guidance.
- Ensure that all systems generating or manipulating synthetic content, particularly deepfakes, are properly labelled and disclosed, following the transparency obligations under Article 50.

High-Risk AI to-do's

- Operators of high-risk AI systems should verify if their systems fall under the grandfather clause (Art. 111(2)) based on the release date (before 2 August 2026).
- They must also check if any modifications disqualify the system from the grandfather clause due to significant design changes post-release.

Prepare for evolving standards

- Finalise integration harmonised standards like prEN ISO/IEC 24029-2 (Robustness of Neural Networks - Part 2) and prEN ISO/IEC 8183 (Data Life Cycle Framework) to ensure your AI systems are robust, reliable, and compliant with data lifecycle requirements.

Transparency measures

- Update and maintain transparency documentation regularly, particularly for high-risk AI systems, to ensure compliance with evolving standards and transparency obligations.

Comment

- Continue monitoring the progress of the JTC21 standardisation work and prepare for the possibility of further delays in the availability of harmonised standards. Ensure contracts are flexible enough to adapt to any interim solutions or alternative approaches that may arise due to these delays.

31 December 2030

End of the transition period for large IT systems

The transition period for large IT systems ends, requiring full compliance with the AI Act's standards and adaptability to future changes.

Objectives

- Achieve full compliance of large IT systems with the AI Act by the end of the transition period.

Actions

- Implement long-term strategies for maintaining compliance, particularly for large-scale IT systems, as recommended in the guidance.
- Establish continuous monitoring and regular technical audits to ensure systems' adaptability and compliance.
- Reevaluate contractual agreements to ensure flexibility in adapting to evolving harmonised standards, while protecting the ability to use the grandfather clause where applicable.

High-Risk AI to-do's

- Ensure ongoing compliance through continuous monitoring, regular updates, and technical audits for large IT systems that incorporate high-risk AI.

Prepare for evolving standards

- Align your large IT systems with finalised AI standards, such as the AI Trustworthiness Framework and the upcoming AI Cybersecurity Specifications, to maintain compliance and operational efficiency. Review and incorporate any additional requirements that may impact your systems.

Transparency measures

- Continue refining transparency practices, especially for large IT systems, by ensuring that all AI-related decisions and processes are clearly documented, communicated to stakeholders, and available for audit.