WILLIAM FRY

The Time to (AI) Act is Now: A Practical Guide to the AI Act

July 16, 2024

The AI Act is a new European Union directive which regulates artificial intelligence (AI) within the EU. The main objective of the Act is to create a legal framework that ensures AI systems are safe, respects fundamental rights, and fosters innovation.

Published in the Official Journal on 12 July 2024, the AI Act introduces strict rules on the deployment and use of certain AI systems. This is a practical guide to assist businesses in navigating these regulations, focusing on AI systems compliance requirements and steps to ensure adherence.

A. Overview of the AI Act

The AI Act is a comprehensive legislative framework designed to regulate the use and development of AI systems within the European Union. It addresses several key areas, starting with the prohibition of certain AI practices due to their potential to cause significant harm or violate fundamental rights.

The Act bans manipulative or deceptive AI systems that use subliminal techniques to distort human behaviour and impair decision-making. This prohibition targets systems that employ imperceptible audio or visual stimuli to influence consumer choices unknowingly.

AI systems that exploit vulnerabilities based on age, disability, or socio-economic status are also prohibited. This includes systems targeting children, elderly individuals, or economically disadvantaged groups.

Social scoring is another prohibited practice under the AI Act. AI systems that evaluate or classify individuals based on their social behaviour or personal characteristics, leading to unjustified or disproportionate treatment, are banned. Such systems can result in discrimination and exclusion, violating fundamental rights.

The AI Act also prohibits predictive policing systems used solely for predicting criminal offences based on profiling or assessing personality traits. This prohibition ensures that AI systems do not unjustly target individuals based on profiling without objective and verifiable facts.

Untargeted facial recognition databases are restricted under the Act. AI systems that create or expand facial recognition databases through untargeted scraping of images from the internet or CCTV footage are prohibited to protect privacy and prevent misuse of biometric data.

Emotion recognition in workplaces and educational institutions is banned unless used for medical or safety reasons. This regulation prevents the potential misuse of AI systems to infer emotions in sensitive environments, where power imbalances could lead to exploitation.

Biometric categorisation is heavily regulated. AI systems that categorise individuals based on biometric data to infer sensitive characteristics such as race, political opinions, or sexual orientation are prohibited to avoid discrimination and privacy violations.

Real-time remote biometric identification systems are heavily restricted for law enforcement purposes, with strict conditions and safeguards to prevent misuse and protect individual rights.

In addition to prohibitions, the AI Act classifies certain AI systems as high-risk, necessitating stringent regulatory requirements. High-risk AI systems include those used in critical infrastructure, education, employment, essential services, law enforcement, migration, and the administration of justice. These systems require providers to maintain technical documentation, implement a quality management system, ensure data governance, and conduct conformity assessments. Deployers must ensure proper use, monitor performance, maintain records, and comply with data protection laws.

The AI Act also addresses general-purpose AI models and systems. These models are defined by their ability to perform various tasks across different applications. If these models possess high-impact capabilities, they are classified as having systemic risk. Providers of such models must ensure compliance with documentation, data protection, and transparency obligations. Deployers are responsible for ensuring proper use and reporting any substantial modifications that might change the AI system's risk classification.

AI literacy is another focus of the AI Act. AI literacy involves the skills and knowledge needed to make informed decisions regarding AI systems. Organisations must ensure their staff possess adequate AI literacy, supported by initiatives from the European AI Board. Measures to promote AI literacy include developing training programmes and collaborating with industry groups and regulatory bodies.

Regulatory sandboxes are established to allow providers to test innovative AI systems in real-world conditions. These frameworks, governed by a sandbox plan, are designed to foster innovation while ensuring regulatory compliance. Competent authorities provide guidance, supervision, and support, aiming to mitigate risks and enhance legal certainty. SMEs and start-ups receive priority access and tailored support services within these sandboxes.

B. Key Dates:

- 12 July 2024: The AI Act published in the Official Journal.
- 1 August 2024: The AI Act becomes law.
- 2 February 2025: Rules on Prohibited AI Systems come into effect.
- 2 August 2025: Rules on General-Purpose AI Models and Systems come into effect.
- 2 August 2026: Rules on Annex III High-Risk AI systems and establishment of regulatory sandboxes come into effect.
- 2 August 2027: Rules on Annex I High-Risk AI systems come into effect.

C. Enforcement and Penalties

- Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35 million or, if an undertaking, 7% of the offender's total worldwide annual turnover, whichever is higher. Non-compliant AI systems can also be taken off the EU market.

- For high-risk AI, non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).
- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7,500,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.
- For small and medium-sized enterprises (SMEs), including start-ups, each fine is capped at the lower of the specified percentages or amounts.

D. Steps to Compliance:

1. Conduct an AI Inventory
Create a comprehensive inventory of all AI systems in use. Categorise based on purpose, functionality, and data processed.

2. Assess AI Systems
Review AI systems to determine if they fall under prohibited or high-risk categories. Focus on customer interaction, marketing, decision-making, and sensitive data processing systems.

3. Implement Compliance Measures
Discontinue or modify non-compliant AI systems. Establish policies for ongoing monitoring and assessment.

4. Training and Awareness
Educate employees on regulations and compliance importance. Provide training on identifying and mitigating risks associated with AI practices.

5. Documentation and Reporting
Maintain detailed records of AI systems, assessments, and compliance measures. Prepare to provide documentation to regulatory authorities.

The AI Act represents a comprehensive effort by the EU to regulate AI technologies and protect fundamental rights. Compliance not only avoids penalties but also fosters trust and ethical AI practices. By proactively assessing and modifying AI systems, businesses can effectively navigate these regulations and maintain a competitive edge in the rapidly evolving technological landscape.

For further guidance and support on AI compliance, please contact Barry Scannell, Leo Moore, Rachel Hayes, or any member of the William Fry Technology Department.