First Milestone in the Implementation of the EU AI Act

February 2, 2025 By Wim Nauwelaerts

The AI Act (*Regulation (EU) 2024/1689 of June 13, 2024, laying down harmonized rules on artificial intelligence*) is the European Union's comprehensive legal framework on AI, which aims to promote the responsible development and use of artificial intelligence in the EU.

The timeline for implementation of the AI Act follows a staggered approach: while the AI Act entered into force on **August 1, 2024**, most of its provisions will apply from **August 2, 2026**. However, the AI Act's requirements relating to (a) prohibited AI practices and (b) AI literacy are effective today, **February 2, 2025**.

(a) **Prohibited Practices under the AI Act.** Consistent with the AI Act's risk-based approach, the EU legislature has taken the position that certain types of AI use are so harmful – because they violate fundamental rights and EU values – that the risk is unacceptable and the use of AI must be prohibited. Accordingly, the AI Act prohibits the placing on the market, putting into service or use of AI systems that:

- Use subliminal techniques or purposefully manipulative/deceptive techniques, with the objective or the effect of materially distorting persons' behavior – thereby causing them to take decisions that they would not have otherwise taken.

For example, "neuromarketing", which uses neurodata to reveal and influence subconscious consumer decision-making processes;

- Exploit persons' vulnerabilities (relating to their age, disability or a specific social or economic situation), with the objective or the effect of materially distorting their behavior.
  For example, AI-powered content on social media that exploits typical vulnerabilities of children, such as their inexperience or lack of impulse control;

- Evaluate or classify persons over a certain period of time based on their social behavior or (personality) characteristics, with the 'social score' resulting in detrimental or unfavorable treatment of the person.
  For example, AI systems used by government agencies to evaluate the behavior of individuals on social media in order to derive adverse consequences for administrative decisions;

- Conduct risk assessments of persons in order to predict the risk of them committing a criminal offence, based solely on the profiling of the person or on an assessment of their personality traits and characteristics.
  For example, predictive policing AI used by law enforcement agencies to predict criminal activity based solely on personality traits or behavioral patterns;

- Create or expand facial recognition databases through the untargeted scraping of facial images (from the internet or CCTV footage).
  For example, AI systems that scrape images off the internet to create a database that can be used for biometric identification purposes;

- Infer a person's emotions in the workplace or at education institutions (except for medical or safety reasons).
  For example, AI systems that enable schools to monitor the performance and behavior of students and staff by analyzing their emotions.

In addition, the AI Act prohibits the following AI practices involving biometrics:

- Biometric categorization of individuals to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. However, the tagging or filtering of biometric datasets and the categorization of biometric data for law enforcement purposes will still be possible;

- The use of real-time remote biometric identification systems in publicly accessible areas for law enforcement purposes, subject to narrow exceptions (g., when searching for missing persons or investigating a terrorist threat).

The ban applies to anyone who provides or makes professional use of AI systems in the EU for any of the above purposes. Violations of the prohibition may result in fines of up to EUR 35 million or 7% of the company's worldwide annual turnover (whichever is higher). To the extent that the (prohibited) AI practice involves the processing of personal data, data protection authorities may also decide to take enforcement action under the EU General Data Protection Regulation (‘GDPR’).

Companies selling or using AI systems in the EU should review their systems and ensure that they are not prohibited by the AI Act.

(b) AI Literacy Requirements

The AI Act imposes an ‘AI literacy’ obligation on providers and deployers (i.e., professional users) of AI systems, regardless of the level of risk associated with the AI system. In other words, even the use of an AI system that is deemed to pose limited risk will require compliance with the AI literacy duty. It should be considered separately from the AI transparency requirements that the AI Act imposes in relation to certain (low-risk) AI applications, and the transparency obligation under the GDPR (for AI systems that involve personal data processing).

AI literacy refers to the skills, knowledge, and understanding needed to make informed use of AI systems while being aware of the opportunities and risks of AI and the potential harm it can cause.

Providers and deployers of AI systems within the scope of the AI Act will need to take measures to ensure, to the best of their ability, that their employees (and others who work with AI systems on their behalf) have a sufficient level of AI literacy. These measures should take into account the staff’s technical knowledge, experience, education and training, as well as the context in which the AI system will be used.

The AI Act does not explain what types of measures the EU legislature had in mind, but the European Commission is expected to issue guidance on the AI literacy obligation and how to comply with it. In the meantime, some EU member state regulators have already published AI literacy best practices to help companies design AI literacy programs that address their specific needs.

For most organizations, AI literacy measures may include the implementation of internal AI policies, guidelines and standards, as well as the roll-out of basic AI training courses (for all staff) and specialized training for specific target groups within the organization.

However, compliance with the AI Act’s AI literacy obligation will always require a contextual approach, meaning that effective compliance measures will need to be tailored to the organization’s specific circumstances, industry, and risks.

Providers and deployers of AI systems should also be able demonstrate to the relevant (EU member state) authorities that they are in compliance with the AI literacy requirement.

Filed Under: AI, Artificial Intelligence

Wim Nauwelaerts is a partner in the Brussels office, leading Alston & Bird’s European Privacy, Cyber & Data Strategy Team. Wim has over 20 years of experience working with global companies on their data protection, privacy, and cybersecurity needs, including General Data Protection Regulation (GDPR) readiness, data transfer, data security and breach requirements, and compliance training.