Platis - Anastassiadis & Associates

The associate law firm of EY Greece

February 2025

Law Alert

# AI Act: Prohibited AI Practices Become Applicable

Regulation (EU) 2024/1689 ("Artificial Intelligence Act") represents a pivotal step in the European Union's regulation for artificial intelligence. Designed to address both the opportunities and risks posed by AI, the Act ensures compliance with fundamental rights, enshrined in the EU Charter of Fundamental Rights. Since its publication on 12 July 2024, the Act follows a phased implementation, with the critical section on prohibited practices under Article 5 becoming enforceable from 2 February 2025.

**Scope of Article 5**

Article 5 of the AI Act introduces an explicit prohibition of AI practices that pose significant risks to individuals, society, or EU values. This provision is designed to eliminate harmful AI applications, ensure the protection of fundamental rights, and promote trustworthiness and accountability in AI technologies. The prohibitions aim to address potential abuses, mitigate systemic risks, and set a clear legal standard for AI operations within the European Union.

The significance of Article 5 lies in its comprehensive approach to addressing emerging ethical and legal challenges posed by AI systems.

By delineating clear boundaries for acceptable practices, the provision fosters a regulatory environment that prioritizes human dignity, non-discrimination, and autonomy. This ensures alignment with the principles enshrined in the EU Charter, including the right to privacy, the prohibition of exploitation, and the safeguarding of vulnerable groups.

Furthermore, these prohibitions act as a deterrent to unethical innovation, compelling Providers and deployers to adhere to the highest standards of AI governance.

**Subliminal Manipulation**

Article 5(1)(a) of the AI Act explicitly prohibits AI systems that manipulate individuals through subliminal techniques, where the effects are imperceptible but materially distort behavior and cause harm. This restriction reflects the EU's commitment to ensuring AI systems do not undermine human autonomy or exploit cognitive vulnerabilities. Subliminal manipulation often involves imperceptible stimuli, such as micro-targeted messaging or audio-visual cues, designed to influence decisions without conscious awareness. Such practices are inherently coercive, depriving individuals of their ability to make informed choices.

From a legal perspective, this prohibition is rooted in the principles of autonomy and dignity as outlined in Articles 1 and 8 of the EU Charter. Recital 29 of the AI Act clarifies that such systems apply stimuli beyond human perception to significantly distort human behaviour. The Regulation imposes a duty on Providers to ensure transparency, requiring them to disclose the mechanisms and intent behind AI functionalities. Providers must implement safeguards to prevent unintended subliminal effects, ensuring compliance with the Act's overarching objective of protecting public welfare.

Examples of prohibited private sector applications include retail AI systems that employ subliminal advertising, such as online platforms using hidden visual cues to increase product engagement. Similarly, AI-driven gambling applications that leverage imperceptible stimuli to encourage prolonged betting behavior fall under this restriction.

**Exploitation of Vulnerabilities**

Article 5(1)(b) prohibits AI systems from exploiting vulnerabilities based on age, disability, or specific socio-economic circumstances. This provision targets practices that manipulate individuals in a manner that is inherently predatory and harmful. Examples include AI systems promoting high-interest credit products to financially desperate individuals or targeting children with addictive gaming mechanics.

This provision is underpinned by Articles 21 and 24 of the EU Charter, which protect against discrimination and uphold the rights of vulnerable groups. Recital 17 emphasizes that AI should not manipulate people who are particularly susceptible to undue influence due to personal conditions. The Act imposes strict compliance obligations on Providers, requiring them to conduct impact assessments that identify and mitigate potential risks to vulnerable populations. Providers must also demonstrate that their systems are designed with ethical considerations at the forefront, ensuring they do not disproportionately target or harm specific groups. For instance, AI-driven payday loan algorithms that exploit financially distressed individuals by recommending high-interest loans without adequate risk disclosure would be non-compliant. Similarly, children's applications that leverage AI to encourage excessive in-app purchases could fall under this restriction.

**Social Scoring Systems**

Under Article 5(1)(c), the Act prohibits public and private entities from implementing AI systems for social scoring purposes. Social scoring involves evaluating or classifying individuals based on their behavior, characteristics, or predicted attributes across different contexts. Such practices are inherently discriminatory, fostering exclusion and systemic inequality.

The legal basis for this prohibition is grounded in Articles 1 and 21 of the EU Charter, which safeguard human dignity and prohibit discrimination. Recital 31 states that social scoring leads to unjustified consequences and should not be permitted. Social scoring systems often lack transparency, relying on opaque algorithms that aggregate data from multiple sources to assign arbitrary scores. By banning social scoring, the EU aims to preserve the principles of equality and fairness in AI-driven decision-making processes.

Examples of non-compliant AI systems include AI-driven creditworthiness scoring models that aggregate social media data to determine loan eligibility, leading to discriminatory outcomes. Similarly, workplace AI that assigns performance scores based on non-work-related activities could be restricted under this article.

**Real-Time Biometric Identification in Public Spaces**

Article 5(1)(d) restricts AI systems used for real-time biometric identification in publicly accessible spaces, except under narrowly defined circumstances. Such systems, including facial recognition technologies, pose significant privacy risks and can facilitate mass surveillance. The regulation permits their use only for critical law enforcement purposes, such as preventing terrorist acts or locating missing persons, and requires prior judicial or administrative authorization.

This provision aligns with Articles 7 and 8 of the EU Charter, emphasizing the right to privacy and data protection.

Recital 30 clarifies that biometric categorization based on sensitive attributes such as political beliefs or sexual orientation is strictly prohibited. Organizations deploying biometric identification systems must adhere to stringent safeguards, including purpose limitation, data minimization, and accountability measures. For example, retail stores using facial recognition to monitor customer emotions and adjust pricing strategies could be in violation of this prohibition. Similarly, employers using AI-driven biometric attendance tracking without proper consent might face compliance challenges.

**Emotion Recognition in Sensitive Contexts**

Article 5(1)(e) bans AI systems used for emotion recognition in sensitive contexts, such as workplaces and educational institutions, except for narrowly defined therapeutic or safety applications.

Emotion recognition technologies, which analyze facial expressions, voice patterns, and physiological signals to infer emotions, carry significant risks of misuse and discrimination.

In sensitive environments, such systems can exacerbate power imbalances, leading to intrusive monitoring and unjustified profiling.

The prohibition is justified by the principles of dignity and privacy enshrined in the EU Charter. Recital 29 emphasizes that AI applications should not analyze emotions in settings where individuals may feel compelled to participate. Providers must ensure that any use of emotion recognition technologies is proportionate, transparent, and compliant with data protection regulations. The Act imposes strict conditions on permissible applications, requiring clear evidence of necessity and a commitment to mitigating potential harms.

Examples of prohibited AI applications include AI-driven hiring software that analyzes candidate emotions during job interviews. Similarly, classroom AI monitoring students' emotions to assess engagement levels would be non-compliant.

**Legal and Ethical Justifications for Prohibited Practices**

The prohibitions outlined in Article 5 are rooted in the principles and values of the EU as enshrined in the EU treaties and the European Charter of Fundamental Rights. The AI Act prioritizes human-centric AI, ensuring that AI applications do not result in discrimination, exploitation, or erosion of public trust. Recitals accompanying the prohibitions provide additional clarity, ensuring legal certainty and preventing regulatory fragmentation. The prohibitions serve as deterrents to unethical practices, promoting the development of AI systems that align with societal values and fundamental rights.

**AI Literacy Requirements**

From February 2, 2025, AI literacy becomes mandatory for Providers and deployers of AI systems, irrespective of their level of risk.

This means companies and public authorities must ensure their staff understands the technology they are using. The required competency directly relates to the specific purpose for which the AI system is being deployed.

For instance, when an online retailer uses AI for personalized customer recommendations, it requires a different level of literacy than a corporation using AI-powered recruitment management systems. The key is responsible assessment of the suitability, risks, and impacts of each AI system.

The goal of AI literacy is to provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement.

Especially, through AI literacy, deployers will be able to ensure that the persons assigned to implement the instructions for use and human oversight as set out in this Regulation have the necessary competence, in particular an adequate level of AI literacy, training and authority to properly fulfil those tasks.

**Enforcement and Penalties**

The provisions on prohibited practices become enforceable on 2 February 2025.

Non-compliance may result in substantial financial penalties, including fines of up to EUR 35 million or 7% of global annual turnover.

Member States are required to establish competent authorities for oversight and enforcement, ensuring compliance with the Act's requirements. These authorities will have the power to investigate breaches, impose sanctions, and provide guidance on best practices for AI governance.

**Stakeholder Responsibilities and Compliance Measures**

Stakeholders, including Providers, deployers, and legal counsels, must take proactive steps to align their operations with the requirements of Article 5 of the AI Act.

The compliance process begins with the identification and categorization of AI systems according to their intended use, risk level, and potential impact. Hence, entities of the public and the private sector using AI are strongly recommended to map down and monitor AI systems through the compilation and maintenance of a Register of AI Systems.

Next, Providers and deployers must conduct a comprehensive assessment to determine whether their AI system falls within the scope of Article 5. This involves analyzing the system's design, functionality, and potential interactions with end users. AI systems should then be categorized based on their risk level, in accordance with the AI Act's risk-based framework. Prohibited AI systems, such as those that manipulate individuals subliminally or exploit vulnerabilities, must be discontinued or redesigned to comply with regulatory standards.

Accordingly, Providers must integrate robust compliance measures into their system design processes, ensuring transparency, accountability, and adherence to ethical principles. This includes embedding safeguards against subliminal manipulation, social scoring, and biometric categorization. Deployers should conduct thorough legal and ethical assessments of their AI applications, particularly in high-risk contexts, ensuring that their use does not violate the prohibitions outlined in Article 5.

Especially, medium and large-sized enterprises must comply with obligations set forth in L. 4160/2022, which mandates the registration of AI systems in the national AI register and adherence to an AI Code of Conduct.

The AI Code of Conduct outlines best practices for responsible AI deployment, including risk mitigation strategies, transparency requirements, and mechanisms for ensuring ongoing compliance with EU regulations. Enterprises must maintain up-to-date records in the AI register, providing details on the purpose, scope, and impact of their AI systems to facilitate regulatory oversight.

Legal professionals must provide comprehensive guidance on compliance strategies, helping clients navigate the complex regulatory landscape and avoid potential liabilities. They should assist organizations in conducting AI impact assessments, ensuring that systems are evaluated against ethical standards and legal requirements. Legal teams should also support organizations in responding to regulatory inquiries and audits, ensuring that all necessary documentation is in place to demonstrate compliance.

By adhering to these structured steps, stakeholders can ensure that AI systems are developed and deployed in a manner that aligns with EU regulations while promoting ethical and responsible AI use. Failure to comply with these obligations may result in substantial penalties, as outlined in the AI Act and complementary national regulations.

**About Platis – Anastassiadis & Associates**

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 45 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis – Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:

**Eirinikos Platis**
Partner
eirinikos.platis@gr.ey.com

**Antonios Broumas**
Senior Manager
antonios.broumas@gr.ey.com

at the
**Platis - Anastassiadis & Associates Law Partnership**
Tel.: +30 210 2886 512
legaloffice@gr.ey.com



ey.com