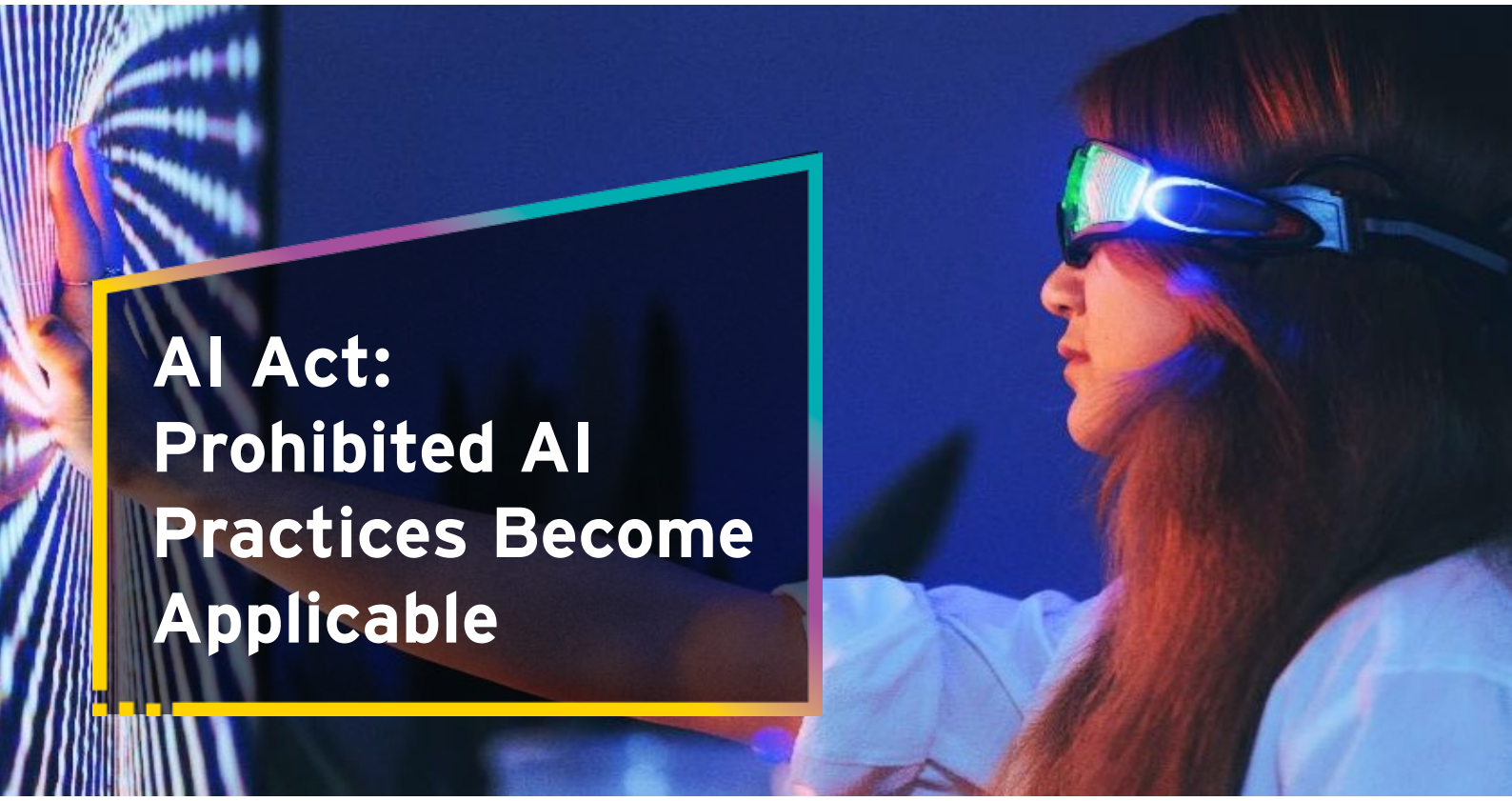
Platis - Anastassiadis & Associates

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 establishes a categorical prohibition on artificial intelligence (AI) practices that present significant risks to individuals, society, or the fundamental values of the European Union. This provision is specifically designed to eliminate AI applications deemed harmful, safeguard fundamental rights, and enhance the trustworthiness and accountability of AI technologies. By setting clear legal boundaries, Article 5 aims to mitigate systemic risks, prevent potential abuses, and establish a definitive regulatory framework for AI operations within the EU.

The legal significance of Article 5 lies in its comprehensive approach to addressing the ethical and legal challenges posed by AI systems. By explicitly delineating prohibited practices, it ensures regulatory clarity while reinforcing the protection of human dignity, non-discrimination, and personal autonomy. The provision aligns with the principles enshrined in the EU Charter of Fundamental Rights, including the right to privacy and the prohibition of exploitation of vulnerable groups. Additionally, these prohibitions serve as a deterrent against unethical AI innovations, compelling providers and deployers to uphold the highest standards of AI governance and ethical compliance.

Further guidance on the implementation of Article 5 is provided by the ***Commission Guidelines issued on 4 February 2025***. These guidelines extend beyond the AI Act by defining vague legal concepts, establishing enforcement principles, introducing compliance mechanisms, clarifying permissible and prohibited AI applications, and outlining judicial oversight measures. These provisions strengthen legal certainty and ensure the consistent application of the AI Act across all Member States, fostering uniform enforcement and regulatory harmonization within the European Union.

Subliminal Manipulation

Article 5(1)(a) of the AI Act categorically prohibits the placing on the market, putting into service, or use of AI systems that deploy subliminal techniques, purposefully manipulative methods, or deceptive mechanisms designed to distort an individual's behavior. Subliminal techniques, as defined in the AI Act, involve imperceptible influences such as visual, auditory, or cognitive manipulations, which operate covertly beyond an individual's conscious awareness. This prohibition is contingent upon the demonstration that such techniques materially distort behavior, impair the ability to make informed decisions, and cause or are likely to cause significant harm (Commission Guidelines, Section 3.2).

This prohibition aligns with the EU's broader commitment to safeguarding human dignity and autonomy, principles enshrined in Articles 1 and 8 of the EU Charter of Fundamental Rights. Recital 29 of the AI Act further underscores that the application of stimuli beyond human perception constitutes a significant distortion of behavior, undermining the EU's core values of individual autonomy and informed decision-making (Commission Guidelines, Section 3.1). Such manipulation is inherently coercive, depriving individuals of their capacity for self-determination and informed choice.

From a legal perspective, this prohibition imposes a dual responsibility on providers and deployers of AI systems. Providers are obligated to ensure that their systems do not include mechanisms capable of deploying subliminal or manipulative techniques. They must demonstrate transparency in the design and intent of these systems, as mandated by the AI Act, and implement safeguards to prevent both intentional and inadvertent subliminal effects (Commission Guidelines, Section 3.2.3). Deployers, in turn, are responsible for ensuring that these systems are used in accordance with the limitations set forth in the Act, including refraining from deploying AI systems in ways that exploit cognitive vulnerabilities or undermine individual autonomy.

This prohibition reflects a high standard of accountability and risk management required under the Regulation. Examples of violations include AI systems designed for subliminal advertising, where imperceptible visual cues are embedded to influence consumer behavior, or gambling platforms that use imperceptible stimuli to manipulate betting behavior and increase user engagement. Both scenarios fall squarely within the scope of prohibited practices as they involve the deliberate distortion of behavior, causing harm in a manner that undermines individual autonomy and consumer protection (Commission Guidelines, Section 3.2.1 and 3.2.3).

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) of the AI Act, the prohibition of social scoring is broadly applicable to both public and private entities that implement AI systems for evaluating or classifying individuals based on their social behavior or personal characteristics across a certain period of time. This prohibition is designed to prevent harmful practices that result in detrimental or unfavorable treatment in unrelated social contexts or treatment that is unjustified or disproportionate to the social behavior evaluated. These practices are seen as inherently discriminatory, fostering social exclusion and systemic inequality (Guidelines, Section 4.2).

The legal basis for this prohibition is anchored in Articles 1 and 21 of the EU Charter of Fundamental Rights, which enshrine human dignity and non-discrimination. Recital 31 of the AI Act reinforces the rationale for this provision, emphasizing that social scoring practices often lack transparency, rely on arbitrary data sources, and result in harmful treatment that is inconsistent with the principles of fairness and equality. Such scoring practices are incompatible with Union values, including democracy and equality, and are deemed incompatible with fundamental rights, including the right to private and family life and data protection (Guidelines, Section 4.1)

To fall under the prohibition in Article 5(1)(c), the following cumulative conditions must be met: the AI system must be placed on the market, put into service, or used; it must be intended for the evaluation or classification of individuals based on their social behavior or personal characteristics; and the scoring must result in or be capable of resulting in detrimental or unfavorable treatment either in unrelated social contexts or in ways that are unjustified or disproportionate to the behavior evaluated (Guidelines, Section 4.2.2).

Examples of prohibited practices include AI systems that combine data from unrelated contexts, such as a bad driving record being used to deny access to financial services, or the scoring of individuals based on inferred or predicted traits, leading to discriminatory or exclusionary treatment. These practices are expressly forbidden when they lack transparency or procedural safeguards, such as mechanisms for individuals to challenge their assigned scores (Guidelines, Section 4.2.3).The AI Act does, however, distinguish prohibited social scoring from lawful evaluation practices that comply with specific Union and national laws. For example, credit scoring based on financial history or AI-driven fraud detection systems that rely on verifiable data are outside the scope of the prohibition provided they adhere to the principles of transparency, relevance, and proportionality in their design and use (Guidelines, Section 4.3).

This prohibition under Article 5(1)(c) reflects the EU's broader objective to ensure trustworthy and human-centric AI systems that uphold fundamental rights while preventing societal harm and systemic discrimination. It imposes obligations on both providers and deployers to ensure their AI systems do not engage in practices that contravene the prohibition, while emphasizing the importance of fairness, accountability, and the rule of law in AI applications (Guidelines, Section 4.1).

Predictive Policing

Under Article 5(1)(d) of the AI Act, the use of AI systems for predictive policing is prohibited when such systems assess or predict the risk of a natural person committing a criminal offense solely on the basis of profiling, personality traits, or behavioral characteristics. This prohibition reflects the EU's commitment to safeguarding fundamental rights, including the right to privacy, non-discrimination, and due process, as guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights. Recital 39 clarifies that such predictive practices are impermissible when they rely on profiling disconnected from verifiable facts or use sensitive attributes, such as race, socio-economic status, or political beliefs, as predictive factors (Commission Guidelines, Section 5.2.1) .

The guidelines distinguish between lawful and prohibited applications of predictive policing. AI systems are prohibited when they generate "risk scores" for individuals based solely on their inferred behavioral profiles or personality traits without a demonstrable link to specific criminal activity. For instance, a system that categorizes individuals as high-risk based on socio-economic or demographic data violates Article 5(1)(d) because it lacks the evidentiary basis required under the Act. Similarly, predictive systems that rely on unverified correlations, such as those using familial or social connections, perpetuate systemic biases and stigmatization, rendering them unlawful (Commission Guidelines, Section 5.2.2) .

Permitted uses of predictive policing AI systems are clearly outlined in the guidelines. AI-enabled crime mapping, which identifies high-crime areas based on historical crime data, is lawful because it is focused on geographic patterns rather than individual profiling. Additionally, AI systems designed to assist human police assessments are permissible when they serve as tools to support decision-making, provided that human oversight is maintained, and the AI does not autonomously make final decisions. Such systems must incorporate verifiable evidence directly linked to specific criminal behaviors and adhere to principles of accountability, transparency, and proportionality (Commission Guidelines, Section 5.3).

This prohibition reflects the broader objectives of the AI Act to prevent misuse of AI technologies in ways that undermine fairness, legal certainty, and individual autonomy. Providers and deployers of AI systems must ensure compliance with Article 5(1)(d) by implementing safeguards such as transparency, human oversight, and adherence to principles of purpose limitation and data minimization. The guidelines further emphasize that any deviation from these obligations, particularly reliance on profiling or sensitive attributes for predictive purposes, constitutes a violation of the Act and exposes violators to significant penalties (Commission Guidelines, Section 5.4).

Facial Recognition Databases

Under Article 5(1)(e) of the AI Act, the placing on the market, putting into service, or use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage is strictly prohibited. This prohibition is rooted in the principles of privacy, data protection, and the prevention of mass surveillance as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights. Recital 43 of the AI Act underscores the significant risks posed by such practices, highlighting that untargeted scraping undermines the right to anonymity and contributes to a pervasive feeling of mass surveillance.

For this prohibition to apply, four cumulative conditions must be met: the practice must involve the placement, service, or use of an AI system; the purpose must be to create or expand facial recognition databases; the method must involve untargeted scraping of facial images; and the data sources must be the Internet or CCTV footage. If these conditions are satisfied, the activity is considered unlawful under the Act.

The guidelines define "facial recognition databases" as collections of human facial images used to enable identification through AI-based recognition systems. "Untargeted scraping" refers to the indiscriminate use of automated tools, such as web crawlers or bots, to extract facial images without targeting specific individuals. These images are typically obtained from publicly accessible platforms like social media or CCTV footage in public spaces. The indiscriminate nature of such scraping breaches data protection principles, as it does not provide for informed consent or targeted use of the data (Commission Guidelines, Section 6.2.2)

Prohibited examples include AI systems that gather facial images from social media platforms using automated scrapers and integrate these images into commercial facial recognition systems for identification purposes. By contrast, targeted scraping, such as a police tool designed to identify a known criminal suspect, does not fall under this prohibition, as it involves specific and verifiable use cases. Similarly, the scraping of biometric data other than facial images or the use of synthetic facial images for AI training purposes does not fall within the scope of this restriction (Commission Guidelines, Section 6.3) .

The untargeted scraping of facial images also violates existing EU data protection laws, including the GDPR, EUDPR, and LED, rendering it unlawful and devoid of legal justification. The prohibition reinforces the EU's commitment to ensuring that AI systems respect fundamental rights and prevent mass surveillance or invasive data collection practices. Providers and deployers are required to implement strict safeguards, including purpose limitation, data minimization, and adherence to accountability principles, to ensure compliance with these legal standards (Commission Guidelines, Section 6.4) .

Emotion Recognition in Workplaces and Educational Institutions

In accordance with Article 5(1)(f) of the AI Act and Recital 44, the placing on the market, putting into service, or use of artificial intelligence (AI) systems designed to infer the emotions of a natural person is expressly prohibited within workplace and educational institution settings. This prohibition is grounded in significant concerns regarding the scientific validity and reliability of such AI systems, as emotional expressions vary considerably across cultures, social contexts, and even within the same individual over time. The inherent limitations of these AI systems—such as their lack of specificity, limited generalizability, and potential for discriminatory outcomes—raise serious ethical and legal concerns.

Furthermore, the use of AI systems to infer emotions in these contexts is considered highly intrusive and risks creating an imbalance of power between employers and employees, or educators and students. Such AI-driven emotional analysis may lead to unfavorable or prejudicial treatment of individuals or entire groups, potentially infringing upon fundamental rights and freedoms.

However, the AI Act provides for a narrowly defined exemption to this prohibition. AI systems designed to detect emotions for strictly medical or safety reasons may be placed on the market or put into service, provided their use is justified by legitimate therapeutic or safety-related objectives. Such systems must still comply with applicable regulations, including data protection and fundamental rights safeguards, ensuring that their deployment does not result in undue harm or discrimination.

Therefore, outside the permitted exceptions, any entity Engaging in the commercialization, implementation, or use of AI-driven emotion recognition systems in workplace and educational settings will be in violation of the AI Act, subject to regulatory enforcement and penalties as prescribed by the applicable legal framework.

Legal and Ethical Justifications for Prohibited Practices

The prohibitions outlined in Article 5 of the AI Act are firmly rooted in the principles and values of the European Union, as enshrined in the EU Treaties and the European Charter of Fundamental Rights, including the rights to dignity, privacy, and non-discrimination. These prohibitions aim to ensure that AI systems are human-centric and do not result in harm, exploitation, or erosion of public trust. Practices such as subliminal manipulation, untargeted scraping of facial data, and discriminatory social scoring are explicitly prohibited to safeguard against systemic risks to individuals and society. The prohibitions also reflect the EU's broader commitment to fostering trust and transparency in AI technologies while ensuring their compatibility with fundamental rights.

The legal basis for these prohibitions is supported by Recitals such as Recital 29, which addresses the risks of subliminal manipulation, and Recital 43, which highlights the dangers of untargeted scraping contributing to mass surveillance. These Recitals provide essential legal clarity, ensuring harmonized enforcement across the EU and preventing regulatory fragmentation. They reinforce the principles of accountability, proportionality, and transparency, which are central to the regulation.

The Commission Guidelines further emphasize the legal and ethical justifications for these prohibitions. They stress the importance of protecting fundamental rights by preventing practices that undermine human autonomy, dignity, and equality. For instance, untargeted scraping of facial data violates privacy rights and contributes to a sense of mass surveillance, while discriminatory social scoring fosters systemic exclusion and inequality. These justifications underscore the need to address AI practices that lack transparency or rely on unverifiable data, which could lead to significant harm or undermine public confidence in AI systems.

By prohibiting these harmful practices, the AI Act acts as a deterrent to unethical AI development, promoting the creation of systems aligned with societal values and the Union's democratic principles. These prohibitions ensure that AI innovation does not come at the expense of fundamental rights, establishing a robust legal framework to foster trust, fairness, and accountability in AI technologies across the EU.

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 42 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

EY @EY_Greece EY Greece eygreece EY Greece