

April 2025

Follow us on [LinkedIn](#) 

Attorney Authored

European Commission and AI: Guidelines on Prohibited Practices

By [Camille Paulhac](#)

- ⇒ As artificial intelligence (AI) continues to transform industries across the globe, the EU has taken significant strides to regulate its deployment, use and implementation and to mitigate associated risks.
- ⇒ The 2024 AI Act ([Regulation \(EU\) 2024/1689](#)), presented by the European Commission (EC) as “the first-ever comprehensive legal framework on AI worldwide,” creates a set of risk-based rules regarding specific uses of AI. It came into effect on August 1, 2024, and will be fully enforceable in August 2026.
- ⇒ Certain provisions (mostly prohibition on use) took effect in advance, on February 2, 2025. On February 4 and 6, 2025, the European Commission (EC) published guidelines on prohibited AI practices ([here](#)) and guidelines on AI system definition ([here](#)).
- ⇒ At the same time, the EC withdrew its proposed AI liability directive ([February 11, 2025](#)).
- ⇒ This alert highlights the key aspects of prohibited practices under Article 5 of the AI Act, identifies critical risks, offers actionable compliance insights and highlights enforcement mechanisms to ensure businesses remain ahead in this ever-evolving regulatory landscape.

Understanding the Scope of Prohibited AI Practices

The AI Act defines four different levels of risk:

1. **Unacceptable risk.** Practices involving AI systems which are deemed to pose unacceptable risks on the basis that they are incompatible with fundamental rights and EU values are prohibited.
2. **High risk.** AI systems posing high risks to health, safety and fundamental rights can be placed on the market, put into service or used, subject to fulfilling certain requirements and obligations.
3. **Limited risk.** AI systems which are subject to transparency requirements (i.e., AI systems which perform autonomous tasks, are intended to interact directly with an individual or create content viewed by an individual, but which do not qualify as “high risk”).
4. **Minimal risk.** AI systems posing minimal to no risk are not regulated. Providers can adhere to voluntary codes of conduct

The guidelines published by the EC on February 4, 2025, focus on the first category. Separate guidelines are expected for the second and third categories.

Prohibited Practices

The AI Act prohibits “manipulative, exploitative, social control or surveillance” AI-enabled practices, which by nature “violate fundamental rights and Union values.” Eight types of practices are identified, and sometimes illustrated by examples:

Harmful manipulation and deception: AI systems cannot deploy subliminal or deceptive techniques when they have the objective or the effect of materially distorting the behavior of a person or a group of persons.

Harmful exploitation of vulnerabilities: AI systems cannot exploit vulnerabilities inherent to certain individuals or groups of persons (e.g., age, disability, specific socio-economic situation) that make them particularly susceptible to manipulative and exploitative practices.

Social scoring: AI-enabled “social scoring” practices that assess or classify individuals or groups based on their social behavior or personal characteristics, and lead to detrimental or unfavorable treatment particularly when data comes from unrelated social contexts, are prohibited.

Individual risk assessment and prediction of criminal offences: AI systems cannot assess or predict the risk of a natural person committing a criminal offense based solely on profiling or personality traits and characteristics.

Untargeted scraping to develop facial recognition databases: AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or closed-circuit television (CCTV) footage (including images from surveillance cameras operated in airports, streets, parks, etc.) are prohibited.

Emotion recognition: AI systems cannot infer emotions of individuals in the workplace and in educational institutions, except if intended for medical or safety reasons.

Biometric categorization for certain “sensitive” characteristics: Biometric categorization systems that categorize individuals based on their biometric data to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation are prohibited.

Real-Time Biometric Identification for law enforcement purposes: The use of Real-Time Biometric Identification (RBI) systems in public spaces for law enforcement purposes (subject to limited exceptions exhaustively set out in the AI Act) is not allowed.

Responsible Actors

The AI Act distinguishes five categories of operators in AI systems: providers, deployers, importers, distributors and product manufacturers. The guidelines only focus on providers (i.e., developers of AI systems) and deployers (i.e., users of AI systems).

Exclusions

The AI Act does not cover:

- **National security and defense.** AI systems exclusively used for military or national security purposes are excluded.
- **Judicial and law enforcement cooperation with third countries.** Third-country public authorities or international organizations using AI for law enforcement or judicial cooperation, as long as they protect individual rights, are excluded.
- **Research and development (R&D).** Activities related to R&D on AI systems or models before market placement or before placement into service are excluded.
- **Personal nonprofessional activity.** AI systems deployed in purely personal, nonprofessional contexts are excluded (e.g., home security systems).

- **AI systems released under free and open-source licenses.** Open-source AI systems (unless displaying unacceptable risk, high risk or being subject to limited risk rules) are excluded.

However, “dual-use” systems (e.g., systems designed for both civilian and military use) and testing in real-world conditions (i.e., temporary testing of an AI system in real-world conditions to assess and verify its conformity with the AI Act) are **within the scope**.

Enforcement and Penalties

Compliance with the AI Act will be overseen by 27 national market surveillance authorities designated by member states and the European data protection supervisor. Member states must designate their national market surveillance authority by August 2, 2025.

Key enforcement measures include:

- Fines (not applicable before August 2, 2025) — **for providers and deployers**, violations can result in penalties up to €35 million or 7% of annual worldwide turnover, whichever is higher.
- Withdrawal of the AI system from the market.
- Restriction of the AI system’s availability.
- Corrective actions to ensure the AI system is compliant.

Challenges

While a number of stakeholders have welcomed the AI Act and guidelines, viewing them as a step toward safeguarding fundamental rights in AI deployment, industry representatives have expressed concerns that complying with this additional complex regulation will necessitate important resources and could stifle innovation and competitiveness.

Key Actionable Compliance Steps for Providers and Deployers

1. **Risk assessment.** Conduct thorough risk assessments of AI systems used, deployed and/or developed.
2. **Internal audits.** Establish internal controls and regular audits to verify compliance.
3. **Training and awareness.** Educate employees and stakeholders.
4. **Responsible data governance.** Ensure lawful collection, processing and storage of data, particularly biometric and sensitive personal data.
5. **Responsible data personalization.** Ensure that AI-driven personalization respects fairness principles and avoids exploiting vulnerabilities inherent to certain individuals.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact the following Paul Hastings lawyers:

Camille Paulhac
+33-1-42-99-04-10 / +32-2-641-7460
camillepaulhac@paulhastings.com