ARTIFICIAL INTELLIGENCE
INFORMATION MEMO
JUNE 12, 2025

The EU AI Act: What U.S. Companies Need to Know

By: Mario Ayoub, Jessica Copeland and Summer Associate Sarah Jiva*

The European Union's ("EU") Artificial Intelligence Act (the "AI Act" or "Act"), enacted in Aug. 2024, is the first comprehensive legal framework governing artificial intelligence having global reach. The Act aims to ensure that AI systems are human-centric, trustworthy and safe, with particular emphasis on impacts to health, safety and fundamental human rights. The Act takes a risk based approach, with obligations varying based on whether an AI system is considered to pose minimal, limited, high or unacceptable risk. Integral aims of the AI Act include transparency and accountability in all stages and uses of AI systems. Organizations both located within and outside the EU Area must adopt new or preserve existing practices to ensure data quality, reduce bias and protect user privacy.

Once Again EU Regulation Has Extraterritorial Impact

Having déjà vu moments related to GDPR? Just like the EU's groundbreaking data privacy regulation, their AI Act applies to organizations based in the EU, as well as the U.S. and other non-EU organizations if AI systems or outputs are used within the EU. Relevant to U.S. business, this includes AI services hosted in the U.S. but accessible to EU users and systems where automated outputs are used in the EU. In short, organizations based in New York and other states in the U.S. are not necessarily exempt from compliance just because they are not physically within the EU's borders.

In Feb. 2025, the European Commission issued additional clarifying guidance on the definition of "AI system" and prohibited AI practices. Additional guidance and technical standards are forthcoming.

- Definition of "AI System": While the European Commission acknowledges that the definition will evolve over time, it breaks down the definition as set forth by Article 3(1) of the AI Act into the following elements: "(1) a machine based system; (2) that is designed to operate with varying levels of autonomy; (3) that may exhibit adaptiveness after deployment; (4) and that, for explicit or implicit objectives; (5) infers, from the input it receives, how to generate outputs (6) such as predictions, content, recommendations, or decisions (7) that can influence physical or virtual environments."
- Prohibited AI practices: AI systems that pose unacceptable risks to fundamental rights and are therefore prohibited include those with the following functions: manipulation or deception, exploitation of vulnerable groups, social scoring based on traits, predictive policing based on profiling, untargeted scraping of facial images for recognition, emotion recognition in workplaces and schools, biometric categorization and real time remote biometric identification.

Categorical Risk Breakdown

The AI Act adopts a tiered, risk based approach to regulation of AI development, use and deployment.

1. Unacceptable Risk: Certain AI applications are banned outright, such as real time biometric

surveillance in public spaces, social scoring, manipulative behavioral targeting and exploitative tools that harm vulnerable groups (e.g., minors).

2. High Risk: Systems deemed high-risk include those used in education, employment, healthcare, law enforcement and critical infrastructure—fields and contexts in which socioeconomic decisions are routinely made. Because these systems process sensitive data, they must meet rigorous requirements around risk management, transparency, data quality, non-discrimination, technical documentation and human oversight. They are subject to continuous monitoring after meeting a conformity assessment.

3. Limited Risk: These AI systems must meet transparency obligations, including disclosures when users interact with AI (e.g., chatbots or deepfake generators). Content generated by AI must be labeled as such.

4. Minimal or No Risk: Most AI systems (like email spam filters) fall into this category and are not subject to new obligations.

Implementation and Enforcement Timeline

Implementation and enforcement of the AI Act is already underway with key dates still on the horizon and subject to change:

- Feb. 2, 2025: Ban on unacceptable risk systems took effect.
- Aug. 2, 2025: Transparency rules for general purpose AI systems take effect.
- Aug. 2025: Expected publication of code of practices governing general purpose AI systems.
- Feb. 2, 2026: Expected publication of guidelines governing high risk AI systems.
- Aug. 2, 2026: High risk AI systems must comply with core obligations.
- Aug. 2, 2027: Providers of general purpose AI models that have been put on the market prior to Aug. 2, 2025, will need to be compliant with the AI Act by Aug. 2, 2027. Extended compliance deadline for AI embedded in other regulated products like medical devices or vehicles.

Industry Impacts for U.S. Organizations

- Healthcare: AI diagnostic tools, clinical support systems, and software embedded in medical devices will likely be high risk. U.S. healthcare companies must audit their systems for fairness and bias, implement strong risk controls and maintain detailed documentation to retain access to the EU market.
- Manufacturing: AI used in machinery, robotics or vehicles—particularly where safety is involved—will require compliance with the Act's technical and transparency standards. Manufacturers must begin aligning product development and conformity assessments with the AI Act now.
- Financial Services: Credit scoring, fraud detection and AI underwriting systems fall under high risk use. U.S. financial institutions must ensure their models are explainable, fair and secure. Algorithmic impact assessments and transparency measures will be essential.
- Education: AI tools used to score exams, screen applicants or evaluate performance are high risk. Education and EdTech companies must ensure their systems are accurate, non-discriminatory and overseen by humans. Disclosures to users and recordkeeping will be necessary.

How can your organization stay ahead of compliance deadlines?

While the world awaits further EU guidance that specifically spells out what organizations must do to fulfill their obligations under the AI Act, here are some actions you can take now:

- Inventory Your AI Tools: Identify all AI systems that might touch the EU market and assess their risk classification.
- Avoid Banned Uses: Immediately cease or modify any systems that could fall into the unacceptable risk category.
- Prepare for Compliance: Begin collecting technical documentation, conducting risk assessments, and assigning accountability within your organization. Develop an internal AI governance framework, including an AI Code of Conduct or AI Responsible Use Policy.
- Stay Informed: Follow EU guidance and emerging standards. Compliance with harmonized technical standards will help demonstrate conformity.
- Train Your Teams: Ensure product, legal, and compliance teams understand the AI Act and embed it into development processes. Consider creating a cross-disciplinary team responsible for AI compliance and governance.

Looking Beyond Europe

Much like how the GDPR transformed global data privacy, the EU AI Act is likely to influence U.S. regulations as well. States like California, Colorado and New York have already enacted AI specific regulations, some of which mirror the EU's risk based approach. U.S. businesses that proactively align with the AI Act's principles will be well positioned to comply with future domestic laws and maintain competitive access to the global market.

The EU AI Act is a landmark regulation that reshapes the landscape for AI use and deployment. U.S. companies, particularly those in health care, manufacturing, financial services and education, must begin evaluating and updating their AI governance programs now. With steep financial penalties for noncompliance and broad extraterritorial reach, early and decisive action is imperative.

For more information or assistance with AI governance and privacy compliance, contact Bond Schoeneck & King PLLC's artificial intelligence or cybersecurity and data privacy practices.

*Special thanks to Summer Law Clerk Sarah Jiva for her assistance in the preparation of this memo.

BOND SCHOENECK & KING ATTORNEYS