THE EUROPEAN UNION'S AI ACT MAKES ITS MARK AND U.S. BUSINESSES ARE WITHIN ITS REACH

Caroline Mazurek Cozzi and **Joe Carlasare** Amundsen Davis, LLC

The European Union's Artificial Intelligence Act (AI Act) is more than a theoretical concept or distant regulation. It is the world's first comprehensive regulatory framework designed to shape AI governance and oversight. It provides rules related to the ethical use of AI and enhances consumer protection. Much like the effect of the General Data Protection Regulation (GDPR) on U.S. businesses related to data privacy, the AI Act forces companies to reassess how they build, deploy, and monitor artificial intelligence.

The Act supports innovation and market access and applies to almost every organization developing, deploying, or using AI systems. This includes American-based companies that develop or distribute AI products in the European Union (EU) market or those whose services produce outputs that affect EU residents. While the GDPR primarily impacted data flows, the AI Act targets systems. The Act's provisions create direct compliance obligations and legal risks that have an extraterritorial reach, regardless of industry or physical location.

TIMING AND APPLICABILITY OF THE ACT

The Act went into force on August 1, 2024, and the first two provisions took effect on February 2, 2025. In particular, Chapter I includes general provisions that outline the scope of the Act and provide key definitions. Article 4 within the chapter imposes AI literacy obligations to ensure companies have the skills, knowledge, and understanding to make informed decisions regarding AI deployment and gain awareness about potential harm. To meet the

AI literacy requirements, companies are tasked with promptly organizing training and education for their staff and all persons dealing with the operation and use of AI within their company.

Chapter II of the Act lists AI practices that are prohibited as of February 2, 2025. Examples of prohibited practices include the use of subliminal techniques, systems that exploit vulnerable groups, biometric categorization, social scoring, individual predictive policing, facial recognition systems using untargeted scraping, emotion recognition systems in workplaces and educational institutions, and "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement.

Additional provisions of the Act will continue to take effect on a rolling basis until all are in full force within a few years. Few exceptions apply and generally encompass the use of AI systems by the military, public authorities, or for research. The next compliance requirement of the Act takes effect on August 2, 2025, and creates transparency obligations, such as maintaining technical model and dataset documentation.

WHY SHOULD U.S. BUSINESSES CARE?

While the Act seems remote due to its international moniker, it can still affect U.S. businesses, even those that are not physically located within the European Union. The Act's applicability to U.S. businesses, however, depends on the company's role in the AI value chain. The Act defines key players within the chain, consisting of providers, developers, product manufacturers, importers, distributors, and authorized representatives.

For example, a U.S. company using an AI tool to recruit for a job in the EU falls within the scope of the Act because the AI tool's output is used in the European Union. The company is classified as a deployer and subject to the applicable provisions of the Act. Similarly, a U.S. auto manufacturer that embeds an AI system to support self-driving functionalities and distributes the vehicle under its own name or trademark in the EU falls within the scope of the Act. The auto manufacturer is classified as a product manufacturer because it has created and distributed a product containing an AI system in the European Union's market.

The scope of the Act's application further depends on the level of potential harm associated with the product or service. The Act previously identified four categories of potential harms ranging from the most extreme—systems that posed unacceptable risks—to those that posed minimal risks. The main focus is now on unacceptable-risk AI systems, which are completely banned, and high-risk AI systems that negatively affect safety or fundamental rights.

If the auto manufacturer's AI system in the previous example is classified as high-risk due to the system's effect on the safety component of the vehicle, the auto manufacturer assumes the role of an AI provider and is subject to heightened compliance obligations. Those include keeping technical documentation, ensuring the system undergoes the conformity assessment procedure, and complying with all EU regulations.

CORE ISSUES TO CONSIDER

U.S. companies face several issues under the Act, including regulatory exposure, operational risks, and reputational concerns. It is clear that a company can be held responsible for its own violations of the Act. Less clear, but also likely, is the concept that a company can be held responsible for violations caused by third-party AI vendors whose products or services touch the European Union. This complicates procurement, contracting, and vendor management.

When working with a third-party AI vendor, U.S. companies should take proactive steps by assessing the level of risk of the AI system and the compliance posture of the vendor. Inspecting technical documentation, requiring timely notification of regulatory inquiries or incidents, and overseeing audits can prevent major problems.

Another issue to consider is the misclassification of the AI system or the company's role. Although defined by the Act, the risk categories are often broader than assumed and require specific disclosures. Whether intentional or due to ignorance, misclassification can subject a company to enforcement actions, product bans, or customer lawsuits. Conducting a thorough analysis of all AI systems using cross-functional teams will ensure alignment.

COMPLIANCE OBLIGATIONS UNDER THE ACT

Compliance obligations under the Act depend on the risk level and the type of system. Providers and deployers of high-risk AI systems face the strictest requirements. These include documenting and disclosing significant incidents, implementing mitigation measures, and ensuring human oversight. Notably, compliance obligations are not limited to any particular industry. Software vendors, tech platforms, SaaS providers, and financial institutions can all be subjected to the Act's provisions.

In fact, many health care organizations are affected by the strictest requirements due to the sensitive and confidential nature of the information that they maintain and exchange. For example, patient identification systems that use biometric data to identify patients and their medical records are classified as high-risk under the Act. They are either banned or significantly restricted. Such systems require ongoing evaluation, auditing, and reporting to ensure full compliance.

Now is the time for U.S. businesses to adhere to compliance requirements. The first step is conducting a comprehensive inventory and identifying which AI models, tools, or features are deployed in or have outputs that affect the EU market. The next step is to classify each system by risk level and adhere to the corresponding obligations. This requires a living governance framework that evolves with changes to the AI system and adheres to regulatory guidance. Finally, establishing cross-functional AI compliance teams is crucial for monitoring systems before, during, and after deployment.

In the age of artificial intelligence, proactive steps are advised. This is particularly true because non-compliance with the provisions of the AI Act can trigger penalties of up to €35 million or 7 percent of global revenue, whichever is higher. These numbers are not hypothetical but rather mirror penalty provisions in other EU regulations concerning privacy and data protection. As the world trends towards automation and efficiency, the AI Act is no longer a European issue—it is a global compliance event.

Caroline Mazurek Cozzi is an associate attorney at Amundsen Davis. She is dedicated to servicing clients in a wide range of industries, including transportation and logistics, retail, and health care, while exploring the effect of artificial intelligence on legal issues.

Joe Carlasare is a partner in Amundsen Davis's Business Litigation Service Group. He defends clients in matters relating to commercial disputes, product liability, professional liability, premises liability, bad faith insurance defense, insurance coverage disputes, and election law.