Insights
June 2024

Skadden

The EU AI Act: What Businesses Need To Know

This article was published in the June 2024 issue of *Insights*.

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Simon Toms
Partner / London
44.20.7519.7085
simon.toms@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

Key Points

- On May 21, 2024, the European Council approved the Artificial Intelligence Act, which will be implemented over the next 36 months.
- The AI Act defines AI systems very broadly and outlines obligations for providers, deployers, importers and distributors — regardless of geographic location — if they market an AI system, serve persons using an AI system or utilize the “output” of the AI system, all within the EU.
- The law distinguishes four categories of AI systems based on the risks they pose, with higher obligations imposed where the risks are greater. Importers and distributors have separate, specific responsibilities.
- The law includes potentially significant fines comparable to those under the GDPR.
- The law creates a complex governance system, with member states required to nominate national supervising authorities.

The newly approved Artificial Intelligence Act (AI Act or the Act) aims to create a secure and trustworthy environment for the development and use of AI in the European Union.

The Act, which the European Council approved on May 21, 2024, is the first of its kind globally and may set a new standard for the regulation of AI, much as the General Data Protection Regulation (GDPR) did for privacy. Other jurisdictions are also enacting laws to govern AI, though they are more localized. Examples include the New York City AI Bias Law and the Colorado Artificial Intelligence Act in the U.S.

Businesses that use AI in some way should consider assessing the risk level of their use and preparing for the new law by satisfying its risk management, oversight and other obligations.

The EU AI Act: What Businesses Need To Know

Scope and Classification of AI Systems

Broad Scope

The AI Act defines AI systems broadly as "machine-based systems that are designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

The AI Act applies to providers, deployers, importers and distributors of AI systems, regardless of their location, if they do any of the following within the EU:

- Market an AI system.
- Serve AI system users.
- Utilize the "output" of the AI system.

There are some exceptions, such as AI systems used for scientific research and development, or for personal, nonprofessional activities. It will be particularly interesting in the health care, pharmaceutical and life sciences sectors to see how the scientific research exception is interpreted.

In addition, AI systems offered under free and open-source licenses are exempt from the AI Act, unless they are placed on the market as high-risk or unacceptable AI systems, or as certain AI systems that are subject to transparency obligations, *e.g.*, medical devices or AI systems used in law enforcement.

Risk-Based Classifications

The AI Act adopts a risk-based approach, classifying AI systems into four categories:

- **Unacceptable-risk:** Deemed to pose a threat to individuals and violate EU fundamental rights and values (such as the right to nondiscrimination, data protection and privacy). While the AI Act does not further define what an unacceptable-risk AI system means, it provides a few examples, such as social scoring systems (which classify individuals based on data relating to their social behavior), real-time biometric identification and systems that manipulate behavior. These systems are prohibited.
- **High-risk:** May pose a high risk to the safety, fundamental rights and freedoms of individuals or society, such as systems that are safety components of products or used in specific sectors like law enforcement, migration or education. This category includes, for example, employment tools used for recruitment, systems used to determine creditworthiness and medical devices. These systems are subject to a full and comprehensive set of requirements.
- **Limited-risk:** May cause confusion or deception for users. Examples are chatbots and deepfakes. These systems are subject to transparency obligations.
- **Low-risk:** Exempt from the AI Act, as they pose minimal or no risk. Text generators are an example.

Obligations for High-Risk AI Systems

The AI Act introduces significant obligations for high-risk AI systems, with different responsibilities depending on the role of the actor.

Providers of high-risk AI systems (defined as those who develop an AI system or have one developed with plans to place it on the market or put it into service under its own name or trademark, whether for payment or free of charge) bear the most responsibility, including:

- Establishing risk management systems.
- Ensuring data quality.
- Maintaining technical documentation.
- Implementing human oversight.
- Meeting standards for accuracy, robustness and cybersecurity.
- Setting up post-market monitoring.
- Registering the AI system.

Deployers of high-risk AI systems (defined as those who use an AI system under their authority, except where the system is used in the course of a personal nonprofessional activity) have fewer obligations, mainly concerning proper use and oversight.

Importers and distributors also have their own specific obligations. For example, they must verify that the product or software bears the required CE marking indicating that an AI system conforms with the AI Act and other applicable EU legislation.

If an importer, deployer or distributor places its trademark on an AI system, substantially modifies it or uses it for a high-risk purpose not anticipated by the provider, they will be classified as a provider themselves and bear the full set of obligations applicable to high-risk system providers under the Act.

Timing

The AI Act will come into force 20 days after its publication in the Official Journal of the EU, which is expected in June 2024. Specific provisions will take effect over the following three years.

Key stages and possible relevant dates after entry into force include:

- Six months (December 2024): Restrictions on prohibited AI practices will take effect.
- 12 months (June 2025): Regulations for general-purpose AI will be enforced.
- 24 months (June 2026): Requirements for high-risk AI systems will come into force.
- 36 months (June 2027): Rules for high-risk AI systems used as safety components in products will be implemented.

Governance

The AI Act establishes a complex framework for the supervision and enforcement of the AI Act, involving authorities at both the EU (*e.g.*, the European AI Office) and national levels (in particular, market surveillance authorities). As a result, an organization could face inquiries or enforcement actions in multiple EU jurisdictions simultaneously.

This stands in contrast to the GDPR, which generally allows organizations active in multiple EU countries to deal exclusively with a single lead supervisory authority.

Stiff Fines for Noncompliance

Noncompliance with the AI Act could result in substantial fines that vary based on the nature of the violation and the size of the organization. Infractions involving prohibited AI systems may incur fines of up to €35 million ($38.1 million) or 7% of global turnover. Other breaches of the AI Act's obligations may result in penalties of up to €15 million or 3% of global turnover.

Additionally, providing false information could lead to fines of up to €7.5 million or 1.5% of global turnover.

Unlike the GDPR, the AI Act does not contain a private right of action for individuals.

To-Dos

Given the breadth of requirements under the AI Act, organizations should consider starting to prepare for the day when the law becomes enforceable, even though that day is not imminent. Organizations may want to undertake several pivotal steps to navigate these changes adeptly.

- **Identify AI systems:** Begin by cataloging the software and hardware products used within or provided by your organization (both internally and externally) and assess which could fall under the definition of "AI systems."
- **Assess whether the Act applies:** For identified AI systems, ask if they are covered by the broad scope outlined in the AI Act, *e.g.*, if the system is offered to users in member states.
- **Classify the systems:** Classify AI systems according to their regulatory tier under the law, recognizing that only a subset may be categorized as prohibited or high-risk.
- **Determine organizational role:** Understand the specific requirements to which your organization must comply in relation to these AI systems. For high-risk systems, identify your organizational role — whether provider, deployer or other — in order to determine your obligations.
- **Develop a compliance plan:** A comprehensive plan will help ensure compliance with these obligations and seamlessly integrate them into your broader compliance framework.

While the AI Act does not encompass all AI systems, it is important to remember that those outside its scope remain regulated under other frameworks, such as the GDPR, as well as by consumer protection and intellectual property laws. Indeed, these laws also apply to AI systems that fall within the scope of the AI Act.

Additionally, the AI Act will likely be supplemented by the proposed AI Liability Directive (AILD) and the new Product Liability Directive (PLD).

- **AILD.** The AI Act contains no provisions addressing liability for damage claims, but the AILD gives more certainty around liability, creating a rebuttable presumption that any fault in an AI system is the fault of the developer. Critics have questioned, however, how it will be established that an AI system has malfunctioned and is at fault.
- **PLD.** The new PLD, which is intended to be adopted by the Council of the EU later this year, aims to modernize the existing rules on the strict liability of manufacturers for defective products. It gives individuals the right, on the basis of strict liability, to claim compensation from manufacturers for damage they have suffered as a result of a product defect. The new PLD thus creates a framework that makes it easier for individuals to assert and enforce such claims.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West / New York, NY 10001 / 212.735.3000