wiley

ALERT

EU Adopts World's First Comprehensive AI Regulation

March 15, 2024

On March 13, 2024, the European Parliament passed the much-anticipated European AI Act, which is the first comprehensive attempt to regulate artificial intelligence (AI) globally. The AI Act – which is formally known as the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence – outlines a broad regulatory framework for AI and was first introduced by the European Commission in April 2021. Since then, the legislation has undergone rounds of revisions to reach the final version, which will go into effect thirty (30) days after it is published in the Official Journal of the European Union, with a staggered set of compliance deadlines for different provisions.

The AI Act generally adopts a risk-based approach to the deployment and use of AI systems. AI systems deemed to pose an "unacceptable" level of risk are outright banned and other AI systems are placed within a risk tier – with corresponding levels of compliance obligations. The obligations vary depending on whether the business is a provider (developer) or deployer of the system, with the majority of obligations falling on providers.

Additionally, the AI Act has a potentially broad, extraterritorial reach. Similar to the General Data Protection Regulation (GDPR), the AI Act covers any entity that is "placing on the market" or "putting into service" an AI system in the EU. The Act extends to "importers and distributors of AI systems," and providers and deployers of AI systems where "the output produced by the [AI] system is used" in the EU. The AI Act is also equipped with hefty penalties, making it important for a business to carefully evaluate whether its use of AI falls within the scope of the AI Act.

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

Artificial Intelligence (AI)

Privacy, Cyber & Data Governance

Below we provide a high-level overview of the AI Act's scope and obligations for each risk classification level.

Scope

After contentious debate, negotiators broadly defined an AI system as "a machine-based system 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."

Unacceptable Risk

AI systems that are deemed to pose an "unacceptable" risk are banned. If currently in use, these systems must be shutdown within six (6) months of the AI Act's effective date. AI systems pose an "unacceptable" risk by:

- deploying subliminal, manipulative, or deceptive techniques that distort behavior and impair informed decision-making;
- exploiting vulnerabilities relating to age, disability or socio-economic circumstances;
- utilizing biometric categorization systems that infer sensitive attributes (e.g., race, political opinions);
- utilizing social scoring;
- assessing the risk of an individual committing a crime solely based on profiling or personality traits (except when supplemented by human assessments based on certain criteria);
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV;
- inferring emotions in the workplace or education setting, except for medical or safety reasons;
- implementing "real-time" biometric information identification in public places for law enforcement purposes (subject to significant exceptions).

High-Risk

The next risk category includes AI systems that pose "high risks" to fundamental rights, public safety or public health, but the risk can be mitigated with the use of adequate safeguards. Systems classified as "high-risk" include those that use AI to:

- determine access to education or vocational training (e.g., grading);
- operate critical infrastructure, such as transportation systems;
- provide a safety component of a product;
- manage workers or evaluate employment, such as evaluating job applicants;
- assess eligibility for public or private benefits and services;

- research, interpret and apply the law to facts or in alternative dispute resolution;
- provide migration, asylum or border control services;
- perform law enforcement functions (e.g., evaluation of evidence).

High-risk systems are not banned, but their use in compliance with the AI Act requires providers to conduct complex and reoccurring assessments, and for certain systems, register them with EU authorities. Importantly, providers can demonstrate that a system that falls within the high-risk category does not create a significant risk to fundamental rights, public safety, or public health. The system must still be registered and assessed, but if the provider can prove that its AI system meets one of the following criteria, the system will not be designated as high risk:

- AI system is intended to perform only a narrow procedural task;
- AI system improves on an activity previously completed by a human;
- AI system analyzes decision-making patterns but does not influence or replace decisions made by humans; and/or
- AI system performs a preparatory task in a system meant to be used in a high-risk system.

General Purpose AI (GPAI) Model

The treatment of GPAI Models triggered extensive debate during negotiations. The final text adopted a tiered approach with varying compliance obligations. The AI Act defines a GPAI model as an "AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications." The AI Act notes "[a]lthough AI models are essential components of AI systems, they do not constitute AI systems on their own."

The Act generally provides rules for GPAI models with enhanced requirements for GPAI models that pose "systemic risks." These obligations will apply when the models are integrated into an AI system.

Generally, all GPAI Models must:

- implement transparency measures, including making public a summary of the content used to train the model;
- disclose to providers technical documentation of the model, including the training and testing process and the result of model evaluations; and
- adopt a policy to demonstrate compliance with copyright law.

Open GPAI Models are generally exempt from these requirements unless the model has systemic risks.

GPAI Models with "systemic risks" must also:

- perform model evaluation;
- assess and mitigate systemic risks; and
- ensure the model has adequate cybersecurity measures.

Limited Risk

Systems deemed to have "limited" risks have minimal obligations under the AI Act. Limited risk systems include those where the user may not realize they are interacting with AI, such as chatbots or AI-generated content. The obligations for these systems center around transparency to the end-user.

As the first comprehensive AI regulation combined with its potentially broad extraterritorial reach, the AI Act will have a significant impact on US-based businesses that operate globally. Businesses should carefully assess the scope of the Act to determine whether its use of AI systems will be governed by the Act's requirements.

***

Wiley's Artificial Intelligence practice counsel clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders in this quickly moving area. Please reach out to a member of our team with any questions.