Overview

EU AI Act Implementation: A Guide to Risks & Timeline

Laura De Boel and Marie-Catherine Ducharme, Wilson Sonsini

Bloomberg
Law

Read Professional Perspectives | Become a Contributor

EU AI Act Implementation: A Guide to Risks & Timeline

Contributed by ***Laura De Boel*** *and* ***Marie-Catherine Ducharme****, Wilson Sonsini*

The European Union's (EU) long awaited Artificial Intelligence Act (**AI Act**) was approved by vote of the European Parliament in March 2024, sending it into the final stages of the EU's legislative process towards its entry into force. So now is a good time for companies to start assessing how the new rules will affect their use of AI and which new requirements they will need to comply with.

The AI Act is a complex piece of legislation imposing different obligations for different types and uses of AI. In a nutshell, the AI Act will ban certain AI systems that are considered to create unacceptable risks for individuals and impose strict obligations for AI systems that qualify as "high-risk". Additionally, certain AI systems are deemed to create transparency risks, which the AI Act addresses by imposing specific notice requirements. Rules on general purpose AI (GPAI) models were added during the legislative process, with a specific focus on GPAI raising "systemic risks".

The promise is that the above approach will impose requirements that are proportionate to the level of risk of AI systems, with more stringent obligations applying to systems which have a higher risk level. By doing so, the EU aims to strike a balance between its desire to be an AI champion and to protect the rights of individuals.

Adding GPAI to a Risk-Based Approach

When the European Commission (Commission) proposed the AI Act in 2021, it presented a risk-based structure that categorized AI systems based on risk levels, from minimal risk to unacceptable risk, imposing different obligations for each category. This risk-based structure is also at the core of the current version of the text.

However, the current version adds onto this structure a separate set of obligations for providers of GPAI models. This was not foreseen in the Commission's proposal, but after the generative AI model ChatGPT was launched in Europe, the gap in the Commission's proposal became obvious. EU legislators extensively debated how to bridge this gap.

While the European Parliament favored regulation for GPAI models, countries like France, Germany and Italy were pressured by local AI companies to push against regulation for GPAI. During marathon negotiations at the end of 2023, EU legislators finally agreed to include in the AI Act a set of obligations specifically addressing concerns with GPAI models.

The **latest draft** of the AI Act, which was approved by the European Parliament on March 13, 2024, organizes risk levels as follows:

- **Unacceptable Risks:** a limited set of harmful AI practices which pose unacceptable risks are prohibited.
- **High Risks**: certain AI systems are identified as "high risk" and specific, onerous, obligations apply to them.
- **Transparency Risks:** certain AI systems (whether high-risk or not) are subject to specific transparency obligations.
- **Minimal Risks**: AI systems with limited risks that do not fit in the categories listed above are not subject to obligations pursuant to the AI Act.

In addition, GPAI models (which are distinct from "AI systems") are subject to specific obligations and those which could pose "systemic risks" are subject to additional, more stringent, requirements.

Unacceptable Risks

The AI Act lists a series of harmful AI practices which are prohibited as they are not compatible with EU values. Prohibited AI practices include:

- Social scoring leading to unfavorable or detrimental treatment;
- Deployment of subliminal techniques to manipulate behavior by encouraging individuals to make decisions they would not have made otherwise, in a harmful manner;
- Exploitation of vulnerabilities of individuals;

- Certain applications of predictive policing;
- Biometric categorization of individuals to infer sensitive data e.g., sexual orientation or religious beliefs;
- Facial recognition for law enforcement purposes in publicly accessible areas, subject to narrow exceptions;
- Creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; and
- Emotion recognition systems in the workplace and educational institutions, subject to narrow exceptions.

High Risks

High-risk AI systems include AI systems intended for the purposes listed in Annex III of the AI Act, such as AI systems intended to be used to influence the outcome of an election or the voting behavior of individuals, as safety components in the management and operation of critical infrastructure (e.g., digital infrastructure and road traffic), and for recruitment decisions (e.g., placing job ads or filtering job applications). In addition, high-risk AI systems include any AI system that is a safety component of a regulated product or that is itself a regulated product (e.g., cars, toys).

The majority of the obligations of the AI Act apply to providers of high-risk AI systems. These obligations can be broadly classified into two categories:

Policies, Procedures & Other Internal Documentation

The key requirement for providers of high-risk AI systems is to set up a "quality management system", which is a set of written policies and procedures covering a range of requirements that are set out in Article 17 of the AI Act. The quality management system should include, for instance, procedures for quality controls, testing, data management, risk management, and post-market monitoring. Providers should also carry out a conformity assessment, which is the process of verifying that the high-risk AI system is compliant before placing it on the EU market. Compliance documentation should be kept on file, including automatically generated logs.

Registration, Notices & Other External Documentation

Providers need to register their high-risk AI system in a public EU database and, if the provider is not established in the EU, appoint a representative in the EU. Providers also need to report serious incidents to local authorities.

Deployers of high-risk AI systems also have some obligations under the AI Act, unless they use the AI system for personal non-professional purposes. Deployers need to use the AI system in accordance with its instructions, and only provide data to the AI system that is relevant and sufficiently representative. They will also need to monitor the functioning of the AI system. In case of a serious incident, they need to notify the provider.

Transparency Risks

Certain AI systems are considered to pose specific transparency risks. Such AI systems will be subject to transparency obligations, such as informing individuals that they are interacting with an AI system (e.g., that they are communicating with a chatbot, not a human). Individuals should also be informed whether an AI system generates 'deep fakes', and whether they are exposed to an emotion recognition system or a biometric categorization system.

Generative AI systems may need to undergo design changes to comply with the AI Act, since their output will need to be marked in a machine-readable format and be detectable as artificially generated or manipulated.

GPAI & Systemic Risks

The term "GPAI model" refers to an AI model that displays significant generality, is capable of performing a wide range of tasks and can be integrated in a variety of other systems or applications (e.g., large generative AI models that can perform a wide range of tasks). A GPAI model can become an AI system through the addition of other components, such as a user interface. The AI Act includes a special section devoted to these models.

Providers of GPAI models are subject to obligations which are distinct from those applicable to AI systems. These include information and documentation requirements, putting in place a policy to comply with copyright law and making publicly available information about the content used for the training of the model.

Some GPAI models are considered as posing "systemic risks", meaning risks that can be propagated at scale across the value chain and that could have a significant impact on the EU market due to their reach or negative effects on public health, safety, public security, fundamental rights or the society as a whole. GPAI models will be presumed to pose systemic risks when the amount of computation used for its training exceeds a certain threshold (i.e., greater than 10^25 floating point operations).

Providers of such GPAI with systemic risks are subject to a set of additional obligations, including to perform model evaluations, assessing and mitigating risks, keeping track and reporting serious incidents and ensuring an adequate level of cybersecurity protection.

Risk-Based Enforcement Regime

The AI Act's risk-based structure is reflected in the levels of fines that can apply in case of violation of the AI Act. Non-compliance with the provision that bans certain AI practices triggers the highest level of fines: up to 35,000,000 euros or 7% of the organization's total worldwide turnover (whichever is higher). Other violations can be subject to fines up to 15,000,000 euros or 3% of the organization's total worldwide turnover (whichever is higher). These levels of fines also apply to small organizations (e.g., start-ups), but they are capped by whichever of the amounts or percentages is *lower*.

While enforcement of the AI Act was initially foreseen only at the national level, the **latest draft** of the AI Act provides enforcement powers to a new **AI Office**—which will be part of the European Commission's Directorate-General for Communications Networks, Content and Technology (**DG CNECT**)—in relation to the GPAI models. AI systems will be supervised by local regulators in each EU country. Regulators will be able to impose fines, but also other sanctions such as ordering the withdrawal of an AI system from the EU market.

Risk-Based Entry Into Application

Following a final vote in its favor by the Council of the EU, the AI Act will start to apply in phases, following a risk-based approach. The provisions on prohibited AI will apply 6 months after the law enters into force, so likely before the end of 2024. Interestingly, the next set of rules to enter into force is not the regime for "high-risk AI", but the regime for GPAI, which will apply one year after the AI Act's entry into force (likely Q2 2025).

The new rules for most "high-risk AI systems" will apply only two years after the AI Act enters into force (likely Q2 2026). Moreover, the new rules will only apply to high-risk AI systems that were already in the EU market in the event of a significant design change (unless the AI system is intended to be used by public authorities). The European Data Protection Supervisor already **flagged** that this could lead to situations where AI systems that pose a high risk for individuals may not fall within the scope of the AI Act. This creates a potential incentive for organizations offering high-risk AI systems to place them on the EU market before Q2 2026 (and a competitive disadvantage for start-ups launching their business after this date).

A carve-out is also created for providers of GPAI already offered in the EU market: they will have an additional two years to comply with the new requirements (meaning they will likely only be subject to the new requirements by Q2 2027). The rules on AI systems with specific transparency risks will apply two years after the AI Act enters into force.

Next Steps

Taking into account the phased entry into application of the AI Act, organizations should take the following steps during the coming 12 months:

By Q3 2024: Map the organization's AI activities to determine whether and how the AI Act will apply.

By Q4 2024: Identify the obligations of the AI Act that would affect the organization's activities/business, and prepare a strategy for compliance (e.g., consider leveraging compliance documentation created for other EU regulations such as the **General Data Protection Regulation** (GDPR)).

By Q1 2025: Implement policies, procedures, and other documentation required for GPAI models, if applicable.

By Q2 2025: Implement full AI Act compliance plan, including allocation of responsibilities and resources for compliance.

As organizations take these steps, they should monitor the development of guidance, standards, and market practices. As with the GDPR, the AI Act introduces a complex set of new requirements that will impact organizations globally. It remains to be seen if, similar to the GDPR, the AI Act will also set new standards for how organizations globally operate and innovate.