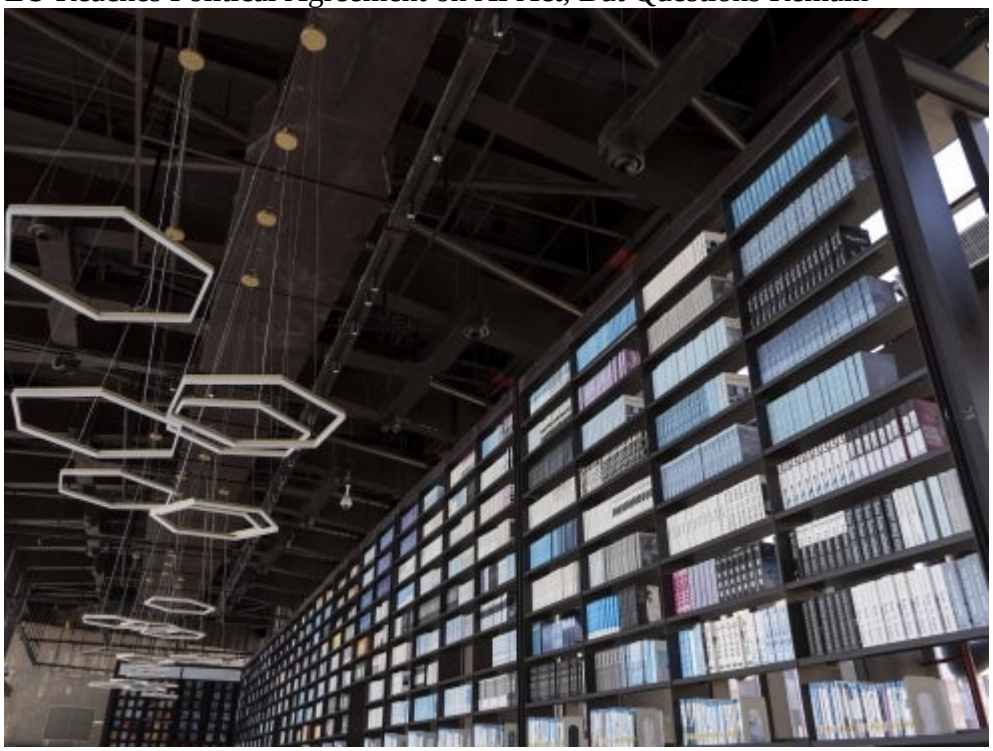
Updates
December 22, 2023
EU Reaches Political Agreement on AI Act, But Questions Remain



After a series of intensive negotiations among representatives of the European Union's three governing bodies (the European Commission, the European Parliament, and the European Council), the EU has concluded its "trilogue" meetings with a "political agreement" on the terms of its forthcoming Artificial Intelligence Act (AI Act).

This milestone marks a pivotal step towards establishing the world's first comprehensive legal framework on artificial intelligence, with the potential to influence international norms and standards for AI, much like how the EU's General Data Protection Regulation (GDPR) influenced the approach to data privacy regulation in many jurisdictions.

The final text of the AI Act, detailing the comprehensive regulations, will likely not be approved and made available until February 2024. For now, important elements of the AI Act await clarification. Nonetheless, summaries issued by EU governing bodies and tech reporters present at the trilogue negotiations shed light on what we can expect from the AI Act.

Overview of the Political Agreement

Following the trilogue negotiations, the European Commission published a "Questions and Answers" document that provides reliable insights into the political agreement's terms. Overall, the political agreement reflects the 11th hour influence of the EU's political leadership through the European Council that appears to have moderated the earlier version favored by the European Parliament.

The Commission's summary includes the following information on what will be included in the forthcoming AI Act:

- **To whom the AI Act will apply.** The AI Act will apply to both public and private entities (including those outside the EU) with AI systems placed or put into service in the EU market or affecting EU residents. The extraterritorial reach of the law tracks the similar approach of the EU's GDPR. The AI Act will apply to providers and deployers of "high-risk AI systems" and "general-purpose AI models," with importers responsible for ensuring foreign systems comply with EU standards. Exceptions will include:
    - Providers of free and open-source AI models, except general purpose models (e.g., generative AI models) with systemic risks.
    - Use for military, defense, and national security purposes.
    - Research, development, and prototyping activities.
- **Risk-based approach.** The AI Act will implement a risk-based regulatory approach with four levels:
    - Minimal risk (most AI systems, subject to existing laws, with optional adherence to trustworthy AI standards).
    - Specific transparency risk (certain AI systems requiring explicit user awareness of AI interaction, such as with a chatbot).
    - High risk (limited AI systems with potential adverse impacts on safety or fundamental rights, requiring strict compliance).
        - Reports from negotiations suggest that the following will be considered "high risk" use cases: education, employment, critical infrastructure, public services (e.g., healthcare and governmental benefits), creditworthiness evaluation, law enforcement, border control, administration of justice, and certain biometric systems that are not prohibited (see below).
        - There will reportedly be some exemptions for systems that do not pose a significant risk to fundamental rights, such as those intended for narrow procedural or preparatory tasks.
        - Despite the efforts of Parliament negotiators, the AI Act will not include "recommender systems of social media" in the list of high risk uses. The Commission states that these systems are excluded because they are already covered by other EU legislation, including the Digital Markets Act and Digital Services Act.
    - Unacceptable risk (banned uses contravening EU values or violating fundamental rights). Use cases with "unacceptable" risk will reportedly include:
        - Public and private uses of "social scoring" systems (defined in previous drafts as the use of AI systems to classify or evaluate people based on social behavior or known or predicted personal characteristics, resulting in a social score to the detriment of such people).
        - Exploitation of the vulnerabilities of persons or use of subliminal techniques to manipulate behavior.
        - Real-time remote biometric identification in publicly accessible spaces by law enforcement (with exceptions for specific crimes).
        - Biometric categorization (i.e., although the text has not been released yet, prior versions of the AI Act suggest this will concern the use of biometric data to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, or sexual orientation and categorizing persons as a result).
        - Individual predictive policing.
        - Emotion recognition in the workplace and education institutions (with medical and safety exceptions).
        - Untargeted or bulk scraping of faces for databases from the internet or CCTV.
- **General purpose AI models.** The AI Act will also consider potential systemic risk from general purpose AI models with high impact capabilities. (The term "general purpose AI models" replaces the term "foundation models," which the Parliament used in its draft). Initially, general purpose AI models include those trained over a specific threshold of computing power,[1] a standard which likely only a handful of models (e.g., GPT-4 and Gemini) meet today, though the Commission's AI Office may update this threshold or identify other models as a general purpose AI model based on further criteria. A new title of

the AI Act will be dedicated to these types of models, with definitions, classification rules, and obligations for providers. Generally, providers of general purpose AI models will be required to provide technical documentation and disclose vital information to "downstream service providers," adhere to copyright laws, and manage systemic risks, with some exceptions for open-sourced models that do not propose systemic risks. Providers will be asked to engage with the European AI Office to "draw up Codes of Conduct" for general purpose AI models.

- **Regulatory sandbox.** The AI Act will include a regulatory sandbox and may allow for real-world testing of certain AI systems, though few details are currently available for what that will entail. Importantly, the AI Act includes no funding for the sandbox.
- **Penalties.** Potential penalties are quite severe and even greater than the GDPR's penalties: up to €35 million or 7% of annual global revenue for violations of bans under the AI Act; up to €15 million or 3% of annual global revenue for violating other obligations; and up to €7.5m or 1.5% of annual global revenue for failing to provide accurate information.
- **Implementation timeline.** Adoption of the AI Act will require supermajority approval from the EU member states, which reports suggest may not be simple in light of the contentious debate over key terms. The AI Act will come into force 20 days after its publication in the Official Journal of the European Union and then become fully applicable thereafter in phases:
    - 6 months after implementation. Phase out prohibited systems.
    - 12 months after implementation. Obligations for general purpose AI governance apply.
    - 24 months after implementation. All rules of the AI Act become applicable.
    - 36 months after implementation. Obligations for high-risk systems for which EU harmonization legislation is necessary.

Notably, reporting from the negotiations suggests that an export ban on AI technologies that could carry out banned activities will not be included in the AI Act.

Further, reports suggest that some enforcement of the AI Act will be carried out and separately funded by each of the EU's member states.

Early Reactions from Stakeholders

The political agreement on the EU AI Act is largely a compromise between earlier, stricter, consumer protection-focused versions favored by the Parliament and Commission and more lenient, industry-friendly terms favored by the Council. The reported compromises of the political agreement have caused stakeholders across the spectrum to raise concerns about the forthcoming AI Act:

- **Concerns about exceptions.** Those who favored the earlier, stricter version of the legislation expressed alarm over the exceptions included in the political agreement, such as the national security and open-source exemptions, arguing they are too broad, potentially undermining the highly debated biometric identification ban.
- **Premature regulation and slow implementation.** Some express a general concern that, while the AI Act gives the Commission amending authority, the regulation may be largely obsolescent before it is fully effective two years after adoption due to the rapid evolution of AI, particularly given the rise of generative AI models. But even this issue is something of a Rorschach test reflecting the stakeholders' appetite for regulation; some fear the law will stifle innovation, while others believe it will be unable to keep up with AI innovations.
- **Inconsistent enforcement.** Some critics argue that delegating significant enforcement responsibilities to individual member states might lead to inconsistent application and enforcement of the AI Act across the EU, potentially undermining its effectiveness and uniformity. The reasons for the inconsistency include

how economic challenges and political ideology could create varying levels of commitment to enforcement among the 27 EU member states.
- **Pushback from certain member states.** France, Germany, and Italy (with support from Hungary, Finland, and Poland) reportedly prefer a lighter regulatory touch for AI and have pushed back throughout the negotiations. These countries generally advocate for self-regulation and are concerned that implementing strict regulations will hamper AI innovation and divert investment away from the EU. These six countries could potentially act collectively to influence the interpretation of the political agreement during the typically routine process of approving the final text of the AI Act in early 2024.

Takeaways and Next Steps

If adopted as final, the EU's AI Act will mark a significant shift in the regulatory landscape of AI. While the final text could still contain some surprises, there is currently enough information available about what the AI Act will entail (including reports on the political agreement and past drafts of the AI Act) to allow regulated entities to begin taking preparatory steps.

Providers and deployers of AI systems could proactively assess their systems against the AI Act's risk categories, particularly for potential bans and obligations, and whether possible exceptions to those requirements may apply. Potentially regulated entities might also consider the implementation timelines, especially considering that the ban on prohibited systems will apply six months following the implementation of the AI Act.

Endnotes

[1] 10^25 floating point operations per second (FLOPs).

© 2023 Perkins Coie LLP

Authors

Explore more in

Technology Transactions & Privacy Law Government Contracts Privacy & Security Communications Artificial Intelligence & Machine Learning Advertising, Marketing & Promotions

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law

Update

February Tip of the Month: Federal Court Issues Nationwide Injunction Against Trump Executive Orders on DEI Initiatives