WILSON SONSINI

Council of the EU Proposes Amendments to Draft AI Act

ALERTS

December 22, 2022

On December 6, 2022, the European Union's (EU) Regulation on Artificial Intelligence ("AI Act") progressed one step towards becoming law when the Council of the EU (the Council) adopted its amendments to the draft act ("Council General Approach"). The European Parliament (Parliament) must now finalize their common position before interinstitutional negotiations can begin.

The Council General Approach concludes months of internal Council negotiations and broadly offers a more business-friendly approach to artificial intelligence (AI) regulation than the European Commission's (EC's) proposal. The definition of an AI system and the scope of the AI Act are slightly narrowed, and a supplementary layer is added to the classification of high-risk AI so that systems that would otherwise be high risk but are only used as accessories to relevant decision making, are excluded. Obligations on providers of high-risk AI systems remain similar, but some requirements are made more technically feasible and less burdensome. The list of prohibited systems is both expanded and narrowed in different areas, and penalties are tweaked in favor of small- to medium-sized enterprises (SMEs).[1]

Background

AI and its regulation are a top priority for the EU. Following the publication of the Ethics Guidelines for Trustworthy AI in 2019, the EC initiated a three-pronged legal approach to regulating AI. Together with the AI Act, new and revised civil liability rules,[2] and revised sectoral legislation, such as the General Product Safety Regulation,[3] seek to offer a legislative framework to support trustworthy AI in the EU. The AI Act will also operate alongside other existing and proposed data-related regulations including the General Data Protection Regulation,[4] the Digital Services Act,[5] the proposed Data Act,[6] and the proposed Cyber Resilience Act.[7]

Commission Proposal

The EC published a proposal for the AI Act (the Proposal) in April 2021. The Proposal adopts a cross-sector and risk-based approach that applies to all providers and users of AI systems that are on the EU market, regardless of where they are established. Applications of AI that are perceived to be most harmful will be banned, while a defined list of "high-risk" AI systems will need to comply with strict requirements. The majority of the Proposal's obligations fall on providers of high-risk AI systems. Transparency requirements will apply to AI systems with limited risks, while those that are of low or minimal risk will not be subject to any obligations. National regulators will be tasked with enforcement, which will be overseen by a newly established "EU AI Board." Companies could face fines of up to the higher of €30 million or six percent total worldwide annual turnover.

For a summary of the EC proposal, please refer to our visual Fact Sheet on Draft EU AI Act.

Key Changes Made by the Council

- **Scope is limited.**[8]AI systems exclusively developed for research and development, and for defense and national security purposes are excluded from scope. AI systems that are used for purely personal, non-professional activities will only be subject to some transparency requirements.

- **New definition of "AI System."**[9]The Council offers a new, slightly narrower definition of AI systems, which requires the system to operate with "elements of autonomy" that infers how to achieve a given set of objectives using "machine learning and/or logic and knowledge based approaches." The EC may adopt further regulation to specify the technical elements of "logic and knowledge based approaches."[10]

- **Some prohibited AI practices are narrowed, while others are broadened.**[11]AI systems that deploy harmful manipulative "subliminal techniques" or exploit the vulnerabilities of a defined list of particular groups continue to be banned. The Council adds specific social and economic groups to the list of vulnerable groups and expands the prohibition of social scoring to cover use by private sector organizations. The Council also broadens exceptions to the prohibition of real-time facial recognition systems by law enforcement in publicly accessible spaces.

- **Exclusion from high-risk classification for purely accessory AI systems.**[12]AI systems that would otherwise be high-risk but are purely accessory to relevant decisions or actions will be excluded from the high-risk classification. Within a year of the AI Act entering into force, the EC will clarify circumstances when AI systems are purely accessory.

- **Amended list of high-risk AI categories.**[13]AI systems will be classified as high-risk if they relate to products that already require a third-party conformity assessment under EU health and safety law (e.g., medical devices, radio equipment, and cars) or are used for a purpose defined in the Act. The Council builds on the purposes proposed by the EC, such as remote biometric identification, recruitment, evaluating creditworthiness, and adds AI systems used in critical digital infrastructure, or that assess risks and pricing in relation to life and health insurance. Meanwhile, the detection of deep fakes by law enforcement, crime analytics, and authentication of travel documents have been removed from the list of high-risk AI.

- **Tweaks to transparency and accountability obligations associated with high-risk AI.** The Council fine-tunes record-keeping provisions,[14]details of the information to be offered to users of high-risk AI,[15]and adds some flexibility for SMEs for demonstrating technical documentation.[16]Requirements for risk management systems are adjusted so that companies must identify risks to individuals' health, safety, and fundamental rights which are most likely to arise when the AI system is used for its intended purpose.[17]Risks that could arise from "reasonably foreseeable misuse" of the AI system are excluded. High-risk AI systems that are also subject to quality management obligations under other EU laws may use parts of their current compliance programs to comply with the AI Act requirements.[18]

- **Adjustments to the requirements for training data and detecting bias.** Providers of high-risk AI will need to ensure "to the best extent possible" that their systems' training data is complete, relevant, representative, and error-free.[19]The Council also limits the biases that must be examined to those that are likely to affect the health and safety of individuals or lead to discrimination.[20]Providers of high-risk AI must eliminate or reduce as far as possible the risk of biased output influencing feedback loops.[21]

- **New fines threshold for small and medium businesses and expanded scope of the EU AI Board.** The Council maintains the maximum fine threshold, at the higher of €30 million or six percent worldwide annual turnover, for companies with over 250 employees and a turnover of €50 million or more.[22]Circumstances in which maximum fines could be issued are limited to cases of non-compliance with respect to prohibited AI systems.[23]A separate threshold, of up to three percent annual worldwide turnover, is created for SMEs.[24]These fines will be imposed by national regulators, with a new EU AI Board ensuring consistency and coordination in enforcement. The activities and powers of the new EU AI Board are scaled to include creating expert groups in relevant fields and advising the EC on international aspects of AI regulation.[25]

Next Step

The Parliament must now finalize their amendments to the Proposal before the next phase of the legislative process, the interinstitutional negotiations (so-called "trilogues"), can begin. More than 3,000 amendments are currently being debated by members of the Parliament. They are expected to vote on the amendments in the first half of 2023, and trilogues could begin shortly after. It is possible that the law could enter into force by the end of 2023, prior to the next Parliament elections in 2024. Once the text passes into law, companies will likely have two-to-three years to comply.[26]

Meanwhile, advancements in AI technology are making headlines. In particular, Open AI's ChatGPT chatbot and Dall.e 2 art generator were recently published[27] and have already attracted millions of curious users. As the potential and challenges associated with AI come to the fore of public discourse, it will be interesting to see how recent developments shape negotiations in the Parliament and trilogues.

We will publish updates on the legislative progress of the AI Act as they occur.

For more information on the EU AI Act and other matters related to AI and machine learning, please contact Cédric Burton, Laura De Boel, Maneesha Mithal, or any other attorney from Wilson Sonsini's privacy and cybersecurity practice or AI and machine learning practice.

Laura De Boel, Maneesha Mithal, Rossana Fol, and Hattie Watson contributed to the preparation of this client alert.