GIBSON DUNN

European Parliament Adopts Its Negotiating Position on the EU AI Act

Client Alert | June 21, 2023

Related People

Kai Gesing

Joel Harrison

Vivek Mohan

Robert Spano

Frances Waldmann

Christoph Jacob

Yannick Oberacker

Since the European Commission first published its highly anticipated proposal for an AI regulation in April 2021,[1] EU institutions and lawmakers have been making significant strides towards passing what would be the first comprehensive legislative framework for AI, the EU Artificial Intelligence Act ("AI Act"). The AI Act seeks to deliver on EU institutions' promises to put forward a coordinated European regulatory approach on the human and ethical implications of AI, and once in force would be binding on all 27 EU Member States.[2]

Following on the heels of the European Commission's 2021 proposal, the Council of the European Union adopted its common position ("general approach") on the AI Act in December 2022.[3] Most notably, in its general approach the Council narrowed the definition of 'AI system' covered by the AI Act to focus on a measure of autonomy i.e., to ensure that simpler software systems were not inadvertently captured.

On June 14, 2023, the European Parliament voted to adopt its own negotiating position on the AI Act,[4] triggering discussions between the three branches of the European Union—the European Commission, the Council and the Parliament—to reconcile the three different versions of the AI Act, the so-called "trilogue" procedure. The Parliament's position expands the scope and reach of the AI Act in a number of ways, and press reports suggest contentious reconciliation meetings and further revisions to the draft AI Act lay ahead. In this client alert, we offer some key takeaways from the Parliament's negotiating position.

The AI Act Resonates Beyond the EU's Borders

The current draft regulation provides that businesses placing AI systems on the market or putting them into service in the EU will be subject to the AI Act, irrespective of whether those providers are established within the EU or in a third country. Given its status as the first comprehensive attempt to regulate AI systems and its extraterritorial effect, the AI Act has the potential to become the key international benchmark for regulating the fast-evolving AI space, much like the General Data Protection Regulation ("GDPR") in the realm of data privacy.

The regulation is intended to strike a much-debated balance between regulation and safety, citizens' rights, economic interests, and innovation. Reflecting concerns that an overly restrictive law would stifle AI innovation in the EU market, the Parliament has proposed exemptions for research activities and open-source AI components and promoted the use of so-called "regulatory sandboxes," or controlled environments, created by public authorities to test AI before its deployment.[5] Establishing harmonized standards for the implementation of the AI Act's provisions will be critical to ensure companies can prepare for the new regulatory requirements by, for example, building appropriate guardrails and governance processes into product development and deployment early in the design lifecycle.

The Definition of AI Is Aligned with OECD and NIST

The AI Act's definition of AI has consistently been a key threshold issue in defining the scope of the draft regulation and has undergone numerous changes over the past several years. Initially, the European Commission defined AI based on a series of techniques listed in the annex to the regulation, so that it could be updated as the technology developed. In the face of concerns that a broader definition could sweep in traditional computational processes or software, the EU Council and Parliament opted to move the definition to the body of the text and narrowed the language to focus on machine-learning capabilities, in alignment with the definition of the Organisation for Economic Co-operation and Development (OECD) and the U.S. National Institute of Standards and Technology ("NIST"):[6]

> "*a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments*."

In doing so, the Parliament is seeking to balance the need for uniformity and legal certainty against the "rapid technological developments in this field."[7] The draft text also indicates that AI systems "can be used as stand-alone software system, integrated into a physical product (embedded), used to serve the functionality of a physical product without being integrated therein (non-embedded) or used as an AI component of a larger system," in which case the entire larger system should be considered as one single AI system if it would not function without the AI component in question.[8]

The AI Act Generally Classifies Use Cases, Not Models or Tools

Like the Commission and Council, the Parliament has adopted a risk-based approach rather than a blanket technology ban. The AI Act classifies AI use by risk level (unacceptable, high, limited, and minimal or no risk) and imposes documentation, auditing, and process requirements on *providers* (a developer of an AI system with a view to placing it on the market or putting it into service) and *deployers* (a user of an AI system "under its authority," except where such use is in a "personal non-professional activity")[9] of AI systems.

The AI Act prohibits certain "unacceptable" AI use cases and contains some very onerous provisions targeting high-risk AI systems, which are subject to compliance requirements throughout their lifecycle, including pre-deployment conformity assessments, technical and auditing requirements, and monitoring requirements. Limited risk systems include those use cases where humans may interact directly with an AI system (such as chatbots), or that generate deepfakes, which trigger transparency and disclosure obligations.[10] Most other use cases will fall into the "minimal or no risk" category: companies must keep an inventory of such use cases, but these are not subject to any restrictions under the AI Act. Companies developing or deploying AI systems will therefore need to document and review use cases to identify the appropriate risk classification.

The AI Act Prohibits "Unacceptable" Risk AI Systems, Including Facial Recognition in Public Spaces, with Very Limited Exceptions

Under the AI Act, AI systems that carry "unacceptable risk" are per se prohibited. The Parliament's compromise text bans certain use cases entirely, notably real-time remote biometric identification in publicly accessible spaces, which is intended to include facial recognition tools and biometric categorization systems using sensitive characteristics, such as gender or ethnicity; predictive policing systems; AI systems that deploy subliminal techniques impacting individual or group decisions; emotion recognition systems in law enforcement, border management, the workplace and educational institutions; and scraping biometric data from CCTV footage or social media to create facial recognition databases. There is a limited exception for the use of "post" remote biometric identification systems (where identification occurs via pre-recorded footage after a significant delay) by law enforcement and subject to court approval.

Parliament’s negotiating position on real-time biometric identification is likely to be a point of contention in forthcoming talks with member states in the Council of the EU, many of which want to allow law enforcement use of real-time facial recognition, as did the European Commission in its original legislative proposal.

The Scope of High-Risk AI Systems Subject to Onerous Pre-Deployment and Ongoing Compliance Requirements Is Expanded

High risk AI systems are subject to the most stringent compliance requirements under the AI Act and the designation of high risk systems has been extensively debated during Parliamentary debates. Under the Commission’s proposal, an AI system is considered high risk if it falls within an enumerated critical area or use listed in Annex III to the AI Act. AI systems listed in Annex III include those used for biometrics; management of critical infrastructure; educational and vocational training; employment, workers management and access to self-employment tools; access to essential public and private services (such as life and health insurance); law enforcement; migration, asylum and border control management tools; and the administration of justice and democratic processes.

The Parliament’s proposal clarifies the scope of high-risk systems by adding a requirement that an AI system listed in Annex III shall be considered high-risk if it poses a “significant risk” to an individual’s health, safety, or fundamental rights. The Parliament also proposed additional AI systems to the high risk category, including AI systems intended to be used for influencing elections, and recommendation engines of social media platforms that have been designated as Very Large Online Platforms (VLOPs), as defined by the Digital Services Act (“DSA”).

High-risk AI systems would be subject to pre-deployment conformity assessments, informed by guidance to be prepared by the Commission with a view to certifying that the AI system is premised on an adequate risk assessment, proper guardrails and mitigation processes, and high-quality datasets. Conformity assessment would also be required to confirm the availability of appropriate compliance documentation, traceability of results, transparency, human oversight, accuracy and security.

A key challenge companies should anticipate when implementing the underlying governance structures for high risk AI systems is accounting for and tracking model changes that may necessitate a re-evaluation of risk, particularly for unsupervised or partially unsupervised models. In certain cases, independent third-party assessments may be necessary to obtain a certification that verifies the AI system’s compliance with regulatory standards.

The Parliament’s proposal also includes redress mechanisms to ensure harms are resolved promptly and adequately, and adds a new requirement for conducting “Fundamental Rights Impact Assessments” for high-risk systems to consider the potential negative impacts of an AI system on marginalized groups and the environment.

“General Purpose AI” and Generative AI Will Be Regulated

Due to the increasing availability of large language models (LLMs) and generative AI tools, recent discussions in Parliament focused on whether the AI Act should include specific rules for GPAI, foundation models, and generative AI.

The regulation of GPAI—an AI system that is adaptable to a wide range of applications for which it was not intentionally and specifically designed—posed a fundamental issue for EU lawmakers because of the prior focus on AI systems developed and deployed for specific use cases. As such, the Council’s approach had contemplated excluding GPAI from the scope of the AI Act, subject to a public consultation and impact assessment and future regulations proposed by the European Commission. Under the Parliament’s approach, GPAI systems are outside the AI Act's classification methodology, but will be subject to certain separate testing and transparency requirements, with most of the obligations falling on any deployer that substantially modifies a GPAI system for a specific use case.

Parliament also proposed a regime for regulating foundation models, consisting of models that "are trained on broad data at scale, are designed for generality of output, and can be adapted to a wide range of distinctive tasks," such as GPT-4.[11] The regime governing foundation models is similar to the one for high-risk AI applications and directs providers to integrate design, testing, data governance, cybersecurity, performance, and risk mitigation safeguards in their products before placing them on the market, mitigating foreseeable risks to health, safety, human rights, and democracy, and registering their applications in a database, which will be managed by the European Commission.

Even stricter transparency obligations are proposed for generative AI, a subcategory of foundation models, requiring that providers of such systems inform users when content is AI-generated, deploy adequate training and design safeguards, ensure that synthetic content generated is lawful, and publicly disclose a "sufficiently detailed summary" of copyrighted data used to train their models.[12]

The AI Act Has Teeth

The Parliament's proposal increases the potential penalties for violating the AI Act. Breaching a prohibited practice would be subject to penalties of up to €40 million, or 7% of a company's annual global revenue, whichever is higher, up from €30 million, or 6% of global annual revenue. This considerably exceeds the GDPR's fining range of up to 4% of a company's global revenue. Penalties for foundation model providers who breach the AI Act could amount to €?10 million or 2% annual revenue, whichever is higher.

What Happens Next?

Spain will take over the rotating presidency of the Council in July 2023 and has given every indication that finalizing the AI Act is a priority. Nonetheless, it remains unclear when the AI Act will come into force, given anticipated debate over a number of contentious issues, including biometrics and foundation models. If an agreement can be reached in the trilogues later this year on a consensus version to pass into law—likely buoyed by political momentum and seemingly omnipresent concerns about AI risks—the AI Act will be subject to a two-year implementation period during which its governance structures, e.g., the European Artificial Intelligence Office, would be set up before ultimately becoming applicable to all AI providers and deployers in late 2025, at the earliest.

In the meantime, other EU regulatory efforts could hold the fort until the AI Act comes into force. One example is the DSA, which comes fully into effect on February 17, 2024 and regulates content on online platforms, establishing specific obligations for platforms that have been designated as VLOPs and Very Large Online Search Engines (VLOSEs). Underscoring EU lawmakers' intent to establish a multi-pronged governance regime for generative models, the Commission also included generative AI in its recent draft rules on auditing algorithms under the DSA.[13] In particular, the draft rules reference a need to audit algorithmic systems' methodologies, including by mandating pre-deployment assessments, disclosure requirements, and comprehensive risk assessments.

Separately, Margrethe Vestager, Executive Vice-President of the European Commission for a Europe fit for the Digital Age, at the recent meeting of the US-EU Trade and Technology Council (TTC) promoted a voluntary "Code of Conduct" for generative AI products and raised expectations that such a code could be drafted "within weeks."[14]

We are closely monitoring the ongoing negotiations and developments regarding the AI Act and the fast-evolving EU legal regulatory regime for AI systems, and stand ready to assist our clients in their compliance efforts. As drafted, the proposed law is complex and promises to be challenging for companies deploying or operating AI tools, products and services in the EU to navigate—particularly alongside parallel legal obligations under the GDPR and the DSA.”

[1] EC, *Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence and amending certain Union Legislative Acts* (Artificial Intelligence Act), COM(2021) 206 (April 21, 2021), available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence. For more details, please see Gibson Dunn, Artificial Intelligence and Automated Systems Legal Update (1Q21), https://www.gibsondunn.com/artificial-intelligence-and-automated-systems-legal-update-1q21/#_EC_Publishes_Draft.

[2] If an agreement can be reached in the trilogues, the AI Act will be subject to a two-year implementation period before becoming applicable to companies. The AI Act would establish a distinct EU agency independent of the European Commission called the “European Artificial Intelligence Office.” Moreover, while the AI Act requires each member state to have a single overarching supervisory authority for the AI Act, there is no limit on the number of national authorities that could be involved in certifying AI systems.

[3] For more details, please see Gibson Dunn, Artificial Intelligence and Automated Systems 2022 Legal Review, https://www.gibsondunn.com/artificial-intelligence-and-automated-systems-2022-legal-review/

[4] European Parliament, *Draft European Parliament Legislative Resolution on the Proposal For a Regulation of the European Parliament and of the Council on Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (COM(2021)0206 – C9?0146/2021 – 2021/0106(COD)) (June 14, 2023), https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_EN.html#_section1; *see also the DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)) (May 9, 2023), https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence („Draft Compromise Agreement”).

[5] *See, e.g.,* Open Loop, *Open Loop Report “Artificial Intelligence Act: A Policy Prototyping Experiment” EU AI Regulatory Sandboxes* (April 2023), https://openloop.org/programs/open-loop-eu-ai-act-program/.

[6] *See* NIST, *AI Risk Management Framework 1.0* (Jan. 2023), https://www.nist.gov/itl/ai-risk-management-framework (defining an AI system as “an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments [and that] are designed to operate with varying levels of autonomy”). For more details, please see our client alert NIST Releases First Version of AI Risk Management Framework (Jan. 27, 2023), https://www.gibsondunn.com/nist-releases-first-version-of-ai-risk-management-framework/.

[7] Draft Compromise Agreement, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence, Art. 3(1)(6)-(6b).

[8] *Id*., Art. 3(1)(6(b).

[9] *Id*., Art 3(2)-(4).

[10] *Id*., Art. 52.

[11] *Id*., Art. 3(1c), Art. 28(b).

[12] *Id*., Art. 28(b)(4)(c).

[13] European Commission, *Digital Services Act – conducting independent audits, Commission Delegated Regulation supplementing Regulation* (EU) 2022/2065 (May 6, 2023), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en.

[14] Philip Blenkinsop, *EU tech chief sees draft voluntary AI code within weeks*, Reuters (May 31, 2023), https://www.reuters.com/technology/eu-tech-chief-calls-voluntary-ai-code-conduct-within-months-2023-05-31/.

Gibson, Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding these issues. Please contact the Gibson Dunn lawyer with whom you usually work, any member or leader of the firm's Artificial Intelligence practice group, or the following authors:

Kai Gesing – Munich (+49 89 189 33 180, kgesing@gibsondunn.com) Joel Harrison – London (+44 (0) 20 7071 4289, jharrison@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Robert Spano – London (+44 (0) 20 7071 4902, rspano@gibsondunn.com) Frances A. Waldmann – Los Angeles (+1 213-229-7914, fwaldmann@gibsondunn.com) Christoph Jacob – Munich (+49 89 1893 3281, cjacob@gibsondunn.com) Yannick Oberacker – Munich (+49 89 189 33-282, yoberacker@gibsondunn.com) Hayley Smith – London (+852 2214 3734, hsmith@gibsondunn.com)

Artificial Intelligence Group: Cassandra L. Gaedt-Sheckter – Co-Chair, Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com) Vivek Mohan – Co-Chair, Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Eric D. Vandevelde – Co-Chair, Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)

Related Capabilities

Artificial Intelligence