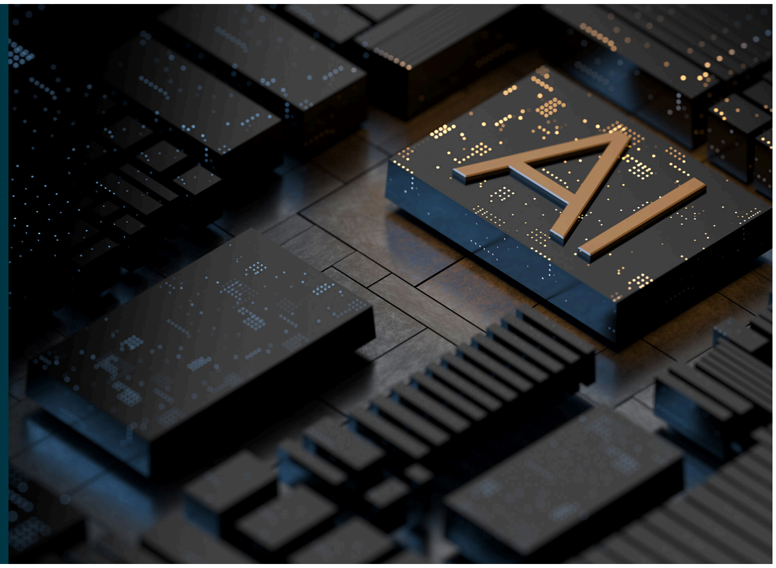
WILSON SONSINI



EU AI Act Enforcement Phase Begins

CONTRIBUTORS

Cédric Burton

Maneesha Mithal

Roberto Yunquera Sehwani

Karol Piwonski

Yaron Moszynski

ALERTS

August 3, 2026

On August 2, 2026, the European Commission (EC), acting through its European AI Office (EU AI Office), became formally entitled to exercise its powers to investigate and enforce the EU AI Act obligations imposed on providers of general-purpose artificial intelligence (GPAI) models, as well as rules on prohibited AI practices. These powers are significant and include requesting information and documentation, obtaining access to models for evaluation, requiring corrective or risk-mitigation measures, and imposing fines of up to the higher of €15 million or 3 percent of the provider's worldwide annual turnover.

Additionally, businesses providing or deploying certain AI systems are now required to comply with new transparency requirements under Article 50 of the EU AI Act. Those AI systems are required to disclose to users when they are interacting with AI and include provenance signals (e.g., watermarks or metadata) to flag when content has been generated or altered by them.

The recently adopted AI Omnibus postponed the EU AI Act's principal requirements for high-risk AI systems but does not affect these August 2, 2026, developments.

EU AI Office Enforcement Powers Take Effect

The substantive obligations for providers of GPAI models placed on the market on or after August 2, 2025, have been applicable since that date, although the EU AI Office lacked the powers to enforce these requirements. Providers of models placed on the market before then generally have until August 2, 2027, to comply.

Over the past year, the EU AI Office has focused on supporting implementation, receiving information from providers, and conducting technical compliance dialogues. As of August 2, 2026, the substantive obligations for GPAI providers are backed by the EU AI Office's formal investigative and enforcement powers.

It is difficult to predict how the EU AI Office will use its enforcement powers, but several European bodies—including the European Data Protection Board and the EU Agency for Fundamental Rights—have advocated for strong and effective enforcement of AI rules. At the same time, in a recently published FAQ, the EU AI Office described "technical compliance dialogues" as its preferred initial tool for assessing compliance and clarifying questions. According to the EU AI Office, those dialogues will continue, and may intensify, after August 2, 2026. Where technical compliance dialogues do not adequately resolve its concerns, the EU AI Office may turn to exercising its formal powers.

Among its enforcement powers, the EU AI Office may:

1. request information and documentation;
2. obtain access to models for evaluation;
3. require corrective or risk-mitigation measures;
4. in serious cases, request that a provider restrict, withdraw, or recall a model from the market;
5. impose fines of up to the higher of €15 million or 3 percent of the provider's worldwide annual turnover.

Considering the transitional period for GPAI models placed on the market before August 2, 2025, providers should confirm which models are currently subject to the requirements and to EU AI Office enforcement, and document the basis for their analysis.

New Transparency Requirements Start to Apply

In addition, as of August 2, 2026, businesses must comply with the following transparency requirements:

- Businesses providing AI systems intended to interact directly with individuals, such as chatbots, must ensure that individuals are notified that they are interacting with AI (unless this is obvious from the circumstances).
- Businesses providing AI systems that generate synthetic audio, image, video, or text content must ensure that relevant outputs are marked in a machine-readable format and detectable as artificially generated or manipulated (e.g., by implementing metadata or invisible watermarks).
- Businesses deploying AI systems that generate or manipulate image, audio, or video content constituting a deepfake must disclose that the content has been artificially generated or manipulated. The same applies to AI-generated or manipulated text published for the purpose of informing the public on matters of public interest.
- Businesses deploying emotion-recognition or biometric-categorization systems must inform individuals exposed to those systems.

The EC recently published final guidelines on the scope and application of these requirements. It has also endorsed a voluntary Code of Practice on Transparency of AI-Generated Content (the Code) as an adequate means of supporting compliance with the marking and labeling obligations (see our client alert for more information). Businesses that do not adhere to the Code may use alternative measures but should be able to explain and document how those measures comply with Article 50.

The AI Omnibus provides a limited transition period for the machine-readable marking requirement under Article 50(2). Providers of systems that generate synthetic audio, image, video, or text content and were placed on the market before August 2, 2026, have until December 2, 2026, to comply with that requirement. The transition does not extend to the other Article 50 transparency requirements.

Next Steps

Given these developments, businesses should consider:

- *Confirming the applicable compliance timeline for each GPAI model.* Determine which models are currently subject to GPAI obligations, and which benefit from the transition for models placed on the market before August 2, 2025.
- *Preparing for EU AI Office scrutiny.* Confirm that the required compliance documentation—including the technical documentation, the information for downstream providers, the copyright compliance policy, and the training data summary—is complete, up to date, and internally consistent. Providers of GPAI models with systemic risk should also review their compliance with the additional obligations concerning model evaluations, the assessment and mitigation of systemic risks, the tracking and reporting of serious incidents, and cybersecurity protection.
- *Preparing for formal requests.* Establish procedures for responding to requests for information, documentation, or model access, including clear internal ownership, escalation, legal review, and accuracy checks. Failure to comply with a request, to provide accurate information, or to provide required model access may itself trigger enforcement action and fines.
- *Confirming compliance with Article 50.* Identify AI systems subject to the transparency obligations and determine whether the business acts as provider, deployer, or both. Review notices concerning interaction with AI, machine-readable markings, and disclosures relating to emotion recognition, biometric categorization, deepfakes, and qualifying public-interest content.
- *Considering adherence to the Code.* Businesses that do not adhere to the Code should document how their alternative measures satisfy the relevant Article 50 requirements.
- *Preparing for the high-risk AI requirements.* The AI Omnibus postponed the application of the key high-risk AI requirements to December 2, 2027 (for Annex III systems) and August 2, 2028 (for AI systems embedded in products covered by certain EU legislation). Businesses should continue

preparing for compliance with the applicable requirements in advance of those dates (for more detail, see our client alert here).

For more information or if you have any questions regarding the EU AI Act, please contact Cédric Burton, Laura De Boel, Yann Padova, or Nikolaos Theodorakis from Wilson Sonsini's Data, Privacy, and Cybersecurity practice.

Wilson Sonsini's AI Working Group assists clients with AI-related matters. Please contact Laura De Boel, Maneesha Mithal, Manja Sachet, or Scott McKinney for more information.

Roberto Yunquera Sehwani, Karol Piwonski, and Yaron Moszynski contributed to the preparation of this alert.