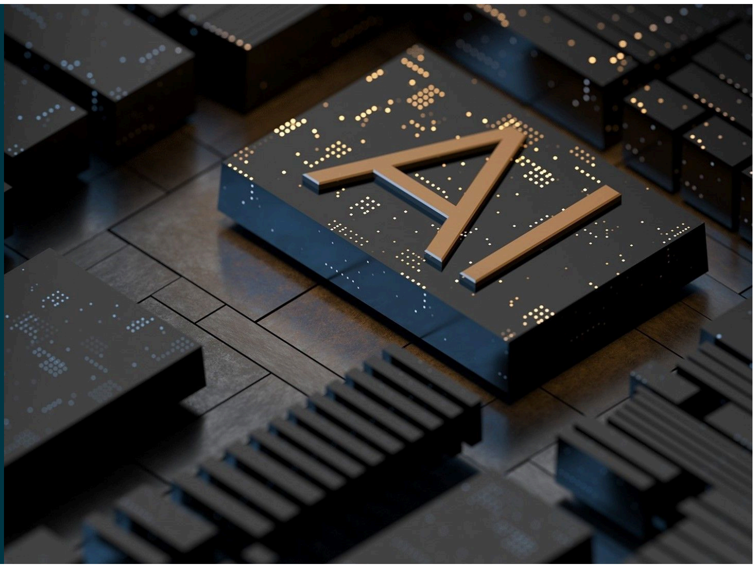
WILSON
SONSINI

EU Releases Final Code of Practice for General-Purpose AI Models



CONTRIBUTORS

Laura De Boel

Roberto Yunquera Sehwani

Karol Piwonski

Hattie Watson

ALERTS

July 21, 2025

On July 10, 2025, the European Commission (EC) published the final version of the General-Purpose AI Code of Practice (Code). This voluntary instrument provides guidance on how providers of general-purpose AI models (GPAI), including those posing systemic risks (GPAI-SR), can comply with their obligations under the AI Act, which become applicable on August 2, 2025. The Code is structured around three key areas: transparency, copyright, and safety and security. Adherence to the Code is voluntary, but providers who decide not to comply with it may face heightened scrutiny from regulators, as they will be expected to demonstrate AI Act compliance through alternative means.

Background

The EU Artificial Intelligence Act (AI Act) was adopted last year, and it is becoming applicable in phases. As of February 2, 2025, certain AI practices are prohibited in the EU (as we explain here). From August 2, 2025, all GPAI models released after this date will need to comply with the AI Act's regime for GPAI models.

The Code is designed to offer practical ways of complying with the obligations for providers of GPAI models, which are set out only at a high level in the AI Act. A multi-stakeholder group of experts drafted the Code under the supervision of the EU AI Office, incorporating feedback from industry, government bodies, civil society, and academia. Although the Code was initially expected by May 2, 2025, it was finalized only on July 10, 2025, just ahead of the August 2, 2025, deadline when the relevant GPAI obligations under the AI Act take effect.

What Is GPAI and GPAI-SR?

GPAI models are models that i) display significant generality, ii) are capable of competently performing a wide range of distinct tasks, and iii) can be integrated into a variety of downstream AI systems or applications. Large-scale generative AI models typically fall within this category. Providers of GPAI models must draw up technical documentation, publish a summary of the data used for training, and implement a policy for compliance with EU copyright rules. GPAI-SR are the most powerful GPAI models and are subject to additional risk management and reporting requirements under the AI Act. To learn more about the AI Act's rules for GPAI models, please see our AI Act FAQs.

Key Points in the Code

The Code is split into three separate chapters: transparency, copyright, and safety and security:

1. *Transparency.* Under the AI Act, providers of GPAI models must draw up technical documentation about the model to provide to the AI Office upon request. GPAI providers must

also make information available to downstream providers, i.e., providers of AI systems that integrate the GPAI model.

   The AI Act outlines the types of information that must be included in such documentation—such as information on model characteristics, distribution methods, licensing, and training—but it does not prescribe a specific format for presenting this information. The Code expands on the documentation requirement and provides a template form that signatories can use. The form has not changed significantly compared to the previous draft of the Code, although it now allows companies to avoid reporting on energy used for training where this information is not available "*due to the lack of critical information from a compute or hardware provider.*"

   In addition, the Code introduces obligations such as updating the documentation when relevant changes occur, retaining previous versions for at least 10 years, and publishing contact details to enable the AI Office and downstream providers to request information from the model provider.

2. *Copyright.* The AI Act requires GPAI providers to adopt a policy to comply with EU copyright and related rights. The Code outlines specific commitments that signatories must implement to fulfil this obligation. In particular, signatories must ensure that web crawlers:

   a. do not circumvent technological protection measures, such as paywalls or subscription controls;
   b. do not crawl websites that are included on lists, published by the EU, of websites recognized as persistently and repeatedly infringing copyright and related rights on a commercial scale; and
   c. respect rights reservations communicated through machine-readable signals, including the Robot Exclusion Protocol (robots.txt) and other recognized standards. Signatories must publish information about the web crawlers that they employ and enable affected rightsholders to be automatically notified when such information is updated.

   Signatories must also mitigate the risk of their models producing copyright-infringing output (e.g., by implementing technical safeguards and contractually prohibiting copyright-infringing uses of the model).

   The Code further states that signatories are encouraged to make publicly available and keep up to date a summary of their copyright policy.

3. *Safety and security.* Under the AI Act, GPAI-SR providers are subject to enhanced obligations. The Code sets out how signatories can meet these requirements by establishing a comprehensive Safety and Security Framework (Framework) to manage systemic risks throughout the model lifecycle. The final version of the Code takes a higher-level approach to the Framework than the previous draft, removing some of the highly prescriptive provisions found in the previous draft. Under the Code, signatories must:

   a. assess and monitor systemic risks. Providers must identify and analyze systemic risks associated with their models, including potential misuse scenarios (e.g., facilitation of chemical or biological weapon development, loss of model control). For each risk, providers must estimate its likelihood and severity and determine whether the residual risk is acceptable. These determinations must inform key decisions, such as whether to proceed with releasing or deploying the model in the EU.
   b. implement safety and security. Signatories will need to implement appropriate safety mitigations, such as filtering and cleaning training data, monitoring and filtering the model's inputs and/or outputs, or fine-tuning the model to refuse certain requests or provide unhelpful responses. They are also required to adopt adequate cybersecurity protections for the models and their physical infrastructure throughout the model's lifecycle.
   c. report to the AI Office. Signatories must provide the AI Office with access to their Framework. In addition, before offering the GPAI-SR model in the EU, signatories must submit to the AI Office a "Model Report" including details such as a description of the model and its behavior, justifications of why systemic risks stemming from the model are appropriate, and documentation of the systemic risk identification, analysis, and mitigation process. Signatories must keep the Model Report up to date and notify the AI Office of any changes they make. The final version of the Code introduces new elements to be included in the Model Report, such as information about systemic risk modeling, and listing five random samples of inputs and outputs for each model evaluation to facilitate independent interpretation of the model evaluation results.
   d. implement the Framework and manage risks throughout the model lifecycle. As part of managing systemic risks, signatories must allocate responsibilities and suitably resource personnel (e.g., an independent committee or members of the management body) to manage systemic risks at all levels of the organization and promote a healthy risk culture (e.g., informing staff of the Framework). In addition, signatories must implement processes and

measures to monitor and document relevant information about serious incidents and possible corrective measures.

The Code also details the obligation for GPAI-SR providers to report serious incidents. The Code lists the information that needs to be reported to the AI Office (and national regulators, if applicable) and provides reporting timelines.

Next Steps

The Code has not yet been formally adopted. It will be reviewed by the AI Office and the AI Board. If deemed adequate, the EC will endorse it. If approved, the Code will obtain general validity in the EU, meaning that adherence to the Code would be a means to demonstrate compliance with the AI Act. It does not, however, provide a presumption of conformity with the AI Act.

To complement the Code, the EC also published guidelines on key concepts related to GPAI models (see details of the draft guidelines here). The AI Office is also due to publish the template that GPAI providers must use to publish the summary of training data, which they must do in addition to the obligations mentioned above.

The AI Act's requirements for GPAI and GPAI-SR will start to apply on August 2, 2025. The EC updated its FAQs on the Code, clarifying that companies signing the Code will not be considered to infringe the AI Act if they do not implement the Code's requirements immediately after signing. The FAQs also mention a one-year grace period for the signatories, meaning that from August 2, 2026, the requirements of the Code will be fully applicable and enforceable with fines, and the AI Office will hold signatories to the standard set out in the Code.

For more information on how to ensure your AI systems and models comply with 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 Hattie Watson contributed to the preparation of this alert.