Volume 1, Number 5 September–October 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 1, No. 5 September–October 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL (ISSN 2995-7486) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Leanne Battle
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

The photo on this journal's cover is by Gaël Gaborel—A Picture of the Earth on a Wall—on Unsplash

Cite this publication as:

The Global Regulatory Developments Journal (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Leanne Battle, Publisher, Full Court Press at leanne.battle@vlex.com or at 866.773.2782

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2995-7486

The European Union's Artificial Intelligence Act: Uncharted Territory for General Purpose AI Systems

Alexander Hendry, Paul Lugard, and Parker Hancock*

In this article, the authors provide an overview of some of the key issues raised by the EU's Artificial Intelligence Act's application to general purpose AI systems.

The European Union has officially adopted the final text of its comprehensive Artificial Intelligence Act (AI Act). The European Union has adopted a "risk-based approach," with specific provisions governing general purpose AI systems (GPAIs). These cutting-edge technologies have the potential to be revolutionary but have also caused considerable controversy in their relatively short time in the spotlight.

This article provides an overview of some of the key issues raised by the AI Act's application to GPAIs.

What Is a GPAI?

The AI Act defines a GPAI as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

Definitions are challenging for any technology-specific legislation, both for lawmakers and those attempting to interpret and comply with the law. Not least because technology frequently outpaces the legislative process. And while this definition applies to many AI systems on the market today (e.g., the leading large language models), there is scope for debate around its edges. For example, where should the lines be drawn in respect of phrases

The Global Regulatory Developments Journal / September–October 2024, Vol. 1, No. 5, pp. 325–330.

ISSN 2995-7486.

such as "large amount," "at scale," "significant generality," and "wide range"? Consider image, video, and audio generation AI based on diffusion models. Can these systems perform "a wide range of distinct tasks"? Or must an AI system be more versatile to be classified as a GPAI by the AI Act?

The complexity of these debates will only increase as the technology evolves; particularly as new systems are developed that do not conform to today's paradigms. AI providers should keep a watchful eye on the relevant authorities' application of this definition, as well as any forthcoming guidance, and regularly review whether their systems resemble a GPAI in the eyes of the European Union.

Systemic Risk

At the forefront of the AI Act's GPAI provisions is the concept of "systemic risk," meaning a risk "that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain."

To determine whether a GPAI system poses such systemic risk, the AI Act considers whether it has "high impact capabilities." A GPAI is presumed to have high-impact capabilities, and therefore systemic risk, when the number of floating-point operations (FLOPs) used in its training process is greater than 10^{25}. As a result, most, if not all, of the leading LLMs on the market today would be considered to pose systemic risk.

GPAIs deemed to have systemic risk are subject to a range of additional regulatory obligations, including mandatory model evaluations, adversarial testing, mitigations for potential risks, and minimum cybersecurity requirements. The European Commission will publish (and keep updated) a list of GPAIs with systemic risk. GPAIs on this list will likely be subject to considerable additional public and regulatory scrutiny.

Documentation Challenges

The AI Act imposes stringent documentation requirements on providers of GPAI systems. The term "provider" includes any

entity that develops a GPAI, as well as any entity that has a GPAI developed and puts it on the market or into service under its own name (whether for payment or free of charge).

The AI Act's documentation provisions include requiring GPAI providers to:

1. Create and maintain comprehensive documentation, including detailed information about model architecture, training methodologies and data, testing processes, and energy consumption. This documentation must be provided to the AI Office and competent national authorities upon request;
2. Provide downstream providers who integrate their systems with certain information, including information and documentation required to enable such downstream providers to have a "good understanding" of the capabilities and limitations of the GPAI, and to comply with their obligations under the AI Act;
3. Put in place a policy for complying with EU copyright law; and
4. Make publicly available a "sufficiently detailed summary" of the training data used, in a format to be determined by the AI Office.

Such requirements are likely to be met with consternation by GPAI providers. The information they must share may include highly sensitive proprietary information. And while the AI Act acknowledges the need to protect intellectual property, reconciling this with some of the AI Act's provisions will be a challenge. GPAI providers will need to carefully balance compliance with the AI Act with maintaining confidentiality and protecting their intellectual property rights.

Certain providers, who make their GPAIs accessible under a "free and open" license and who publish certain information about their model, may benefit from an exemption to some of the documentation requirements, but this exemption does not apply to any GPAI with systemic risks.

Transparency Obligations

In an effort to combat deepfakes and other deceptive content, the AI Act imposes transparency obligations on AI providers

requiring them to mark artificially created or manipulated content as such. However, implementing this requirement presents substantial technical hurdles—particularly for providers of GPAIs.

For rich media like images, audio, and video, most existing provenance marking technologies are easily circumvented by malicious actors. For example, if an image is marked using metadata, taking a screenshot can effectively un-mark it. If it is marked using a watermark, the watermark may be cropped out. Even more challenging is the requirement to mark AI-generated text content. Text can exist in a variety of formats, from plain text files to complex documents, and there is currently no robust way to reliably mark text as machine-generated.

These challenges are particularly daunting for GPAI providers due to the versatility of the systems, the scale of their adoption, and consequently, the potential for their misuse. GPAI providers will need to have in place technical solutions to mark each type of content that their GPAIs may generate. The AI Act requires providers to ensure that their technical solutions are "effective, interoperable, robust and reliable as far as this is technically feasible." Given the rate at which these and related technologies are evolving, this is likely to represent a fast-moving target.

The AI Act does not provide clear guidance on how to handle situations where AI-generated content is subsequently edited or modified by humans—a common workflow. Should such hybrid human-AI creations continue to bear the artificially generated mark? And if not, how much human intervention is required before a piece of artificially created content is no longer required to be marked as such? GPAI providers will need to be among the first entities to propose answers to these questions.

The AI Office

To oversee and facilitate the implementation and enforcement of the AI Act, the AI Act delegates numerous powers to the AI Office, a newly created body within the European Commission. The AI Office's responsibilities are extensive, and prominently among them are various powers in respect of GPAI, including the power to:

1. Enforce obligations under the AI Act on GPAI providers,
2. Monitor compliance of GPAI providers with the AI Act,

3. Request potentially sensitive information from GPAI providers, and
4. Conduct evaluations of GPAIs.

While the AI Act outlines these powers, along with the AI Office's broader responsibilities—such as developing guidelines, facilitating codes of practice, and promoting AI literacy—the specific scope and extent of the AI Office's powers, and how it will exercise them, remains to be seen. It will be crucial for GPAI providers to develop positive working relationships with the AI Office and engage in constructive dialogue to best understand how to comply with the AI Act while balancing the provider's commercial interests.

Key Takeaways

- The EU's AI Act introduces new regulations for GPAIs, including criteria for determining whether such systems present "systemic risks."
- Determining whether certain systems are classed as GPAIs for the purposes of the AI Act may be challenging.
- GPAIs with systemic risk are subject to considerable additional regulatory obligations.
- GPAI providers face stringent documentation requirements that may conflict with their business interests. Providers will be challenged to fulfill their obligations under the EU's AI Act while protecting confidential information and intellectual property.
- Implementing transparency obligations for AI-generated content presents substantial practical challenges; particularly for GPAI providers. Compliance with the AI Act by GPAI providers may not prevent malicious users from circumventing transparency measures.
- The AI Office will have a critical role in determining how the AI Act will affect GPAI, and much uncertainty remains around how this will play out.
- The AI Act will be fully applicable 24 months after its entry into force, but the provisions regarding GPAIs will become effective after 12 months. Fines for violations of the AI Act will depend on the type of AI system, size of the company, and severity of infringements, and may

reach €35 million or seven percent of a company's global turnover (whichever is higher).

Note

* The authors, attorneys with Baker Botts LLP, may be contacted at alexander.hendry@bakerbotts.com, paul.lugard@bakerbotts.com, and parker.hancock@bakerbotts.com, respectively.