Volume 1, Number 3 May–June 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 1, No. 3

May–June 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. Copyright 2024 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner.

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: Morgan Morrissette Wright
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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

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.

This publication is designed to be accurate and authoritative, but the publisher, the editors and the authors are not rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

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

Morgan Morrissette Wright, Publisher, Full Court Press at morgan.wright@vlex.com or at 202.999.4878

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

Final Form of the EU's Artificial Intelligence Act Endorsed by Member States

Huw Beverley-Smith and Charlotte H N Perowne*

In this article, the authors discuss the EU's long-awaited Artificial Intelligence Act.

The long-awaited EU's Artificial Intelligence (AI) Act,[1] once enacted, will be a comprehensive cross-sectoral regulatory framework for AI. Its aim is to regulate the development and use of AI by providing a framework of obligations for parties involved across the entire AI supply chain. As with the General Data Protection Regulation (GDPR), the European Union is seeking, through its first-mover advantage, to set the new global standard for AI regulation.

Affected Entities

The AI Act is designed to cover the whole AI supply chain. There are a broad range of "operators," defined as the providers, product manufacturers, deployers, authorized representatives, importers, or distributors. The AI Act has wide extraterritorial scope, therefore, a number of U.S. businesses will be within scope, depending on their exact role in the supply chain.

Scope and Definition of AI

The AI Act defines an "AI system" as a "machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

The European Union has adopted the definition promulgated by the Organisation for Economic Co-operation and Development

The Global Regulatory Developments Journal / May–June 2024, Vol. 1, No. 3, pp. 177–182.

ISSN 2995-7486.

(OECD). Unlike the Commission's original proposal, where an AI system was limited to software acting for human-defined objectives, this now also seeks to encompass the metaverses through the explicit inclusion of virtual environments.

Risk Classification

The AI Act classifies AI systems into several risk categories, with different degrees of regulation applying to each one. Most AI systems will fall into the lower-risk categories, although there will be significant procedural and transparency obligations relating to their use, which businesses throughout the supply chain will have to understand.

Prohibited: AI Systems Posing Unacceptable Risks

While some of these are focused on the activities of governments and public authorities, many will apply more broadly. The prohibited AI include:

- Use of subliminal techniques to modify or distort an individual's behavior (for example, using subvisual cues that cannot be detected by the human eye in sales or advertising),
- Targeting and exploiting the vulnerabilities of specific groups (for example, toys using voice assistants that encourage dangerous behavior),
- Biometric categorization systems (except for labelling or filtering of lawfully acquired biometric data sets, or for law enforcement purposes where biometric data sets have been lawfully acquired),
- Social scoring (for example, through algorithms determining a person's ability to access social benefits, services, or opportunities),
- Real-time remote biometric identification systems in publicly accessible spaces for law enforcement (subject to specific exceptions such as the detection of serious crimes),
- Predictive policing,
- Facial recognition databases compiled through untargeted scraping of the internet or closed-circuit television footage, and

- Emotion recognition systems in educational or workplace settings (except where this is intended for medical or safety reasons).

High-Risk Systems

The bulk of the obligations under the AI Act apply to systems deemed "high risk" (estimated by the European Commission to be roughly 5-15 percent of AI systems). These are divided into two categories: (1) safety components or products that are already subject to EU safety legislation and that require third-party conformity assessments under such laws, and (2) stand-alone AI systems expressly designated by the European Commission as "high risk," including AI systems used:

- To determine access to or outcomes in education and training;
- In employment for recruitment or selection, promotion, or termination;
- To determine access to essential private and public services, like health care or credit (although there are exceptions for fraud detection);
- In managing critical infrastructure;
- For non-banned biometric identification systems, including systems inferring protected characteristics, emotion recognition systems and remote biometric identification systems (excluding biometric verification of individuals);
- In managing migration, asylum and border controls; and
- In the administration of justice and democratic processes (provided that final rulings are made by humans).

Stand-alone AI systems will not be deemed high risk if they do not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. Prior to placing on the market an AI system, which falls under Annex III but is deemed not to be high risk, the provider must document its assessment of the risk, as well as registering the system in the EU database. Such assessment should take into account both the severity of the possible harm and its probability of occurrence. An AI system may be found not to be high risk if the AI system meets certain criteria, for example, if it is only intended to perform a narrow procedural task or improve the result of a previously completed human activity. However, an AI system will always be considered high risk if the AI system performs profiling of natural persons.

AI systems that do not fall into the "prohibited" or "high-risk" categories are permitted, but with transparency obligations—for example, ensuring that users know that they are interacting with an AI system in a chatbot.

General Purpose AI

The AI Act has had a relatively long legislative process and has been overtaken by technology developments, particularly the recent rise of generative AI systems, such as ChatGPT. One of the key issues in the final stages of negotiations was the extent to which providers of general purpose AI (GPAI) models, on which a number of downstream applications are based, should be subject to specific rules.

The final draft sets out specific requirements of GPAI models, including classification of models with systemic risk, procedural requirements, and obligations for providers of both regular GPAI models and those classified with systemic risk.

A GPAI model will be classified as a GPAI model with systemic risk if it meets any of the following criteria: (1) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks, or (2) based on a decision of the European Commission, including following an alert by a scientific panel that a GPAI model has equivalent capabilities or impact equivalent to those of point (1).

High-impact capabilities (under point 1) will be assumed for high-powered AI, where the cumulative amount of computation used for training a model measured in floating point operations is greater than 10^25.

Providers of GPAI models must:

- Draw up and keep up-to-date technical documentation of the model (including training and testing);
- Provide information to downstream providers of AI systems who intend to integrate the GPAI model into their AI system, containing sufficient information to enable

providers of AI systems to understand the GPAI model and comply with their own obligations;
- Put in place a policy to respect copyright law (especially with regard to reservation of rights);
- Draw up and make publicly available a sufficiently detailed summary of the content used for training the GPAI model (according to a template to be provided by the AI Office); and
- Cooperate with the European Commission and national competent authorities.

Providers of GPAIs with systemic risk will also be required to:

- Perform model evaluation in accordance with standardized protocols and tools, including conducting and documenting adversarial testing of the model to identify and mitigate systemic risk;
- Assess and mitigate possible systemic risks, including their sources, that may stem from the development, placing on the market or use of GPAI models with systemic risk;
- Report serious incidents and possible corrective measures to address them to the AI Office; and
- Ensure an adequate level of cybersecurity protection.

Except for GPAI models with systemic risks (which must comply with all of the above), AI models that are made available to the public under free and open licenses meeting certain requirements are not required to provide the technical documentation and information set out in the first two points above.

Timeline

The final text of the AI Act is expected to be formally adopted in the of summer 2024. However, the leaked final drafts give a sufficient indication of the ultimate requirements for businesses to start planning and integrating the AI Act's requirements in their product development and procurement processes.

Assuming that the text is adopted in June 2024, the AI Act would be effective 24 months after entry into force (i.e., June/July 2026). However, some provisions, such prohibitions on unacceptable-risk

AI systems, will apply six months after entry into force (i.e., late 2024).

Similarly, regulation of GPAI systems will apply after 12 months (or 24 months if they are already on the market).

In Summary

In summary, the EU Artificial Intelligence Act will provide the following:

- A broad definition of AI that applies to many different entities, including providers, deployers, importers, and distributors of AI systems, and will have a wide extraterritorial scope;
- A cross-sectoral, risk-based classification system with an outright prohibition on certain AI practices deemed to impose unacceptable risk;
- New obligations largely targeting AI systems deemed "high risk" and obligations on providers of GPAI systems, including generative AI systems like ChatGPT; and
- Significant fines similar to the GDPR of up to 7 percent of annual global turnover for certain offenses.

Notes

* The authors, attorneys in the London office of Faegre Drinker Biddle & Reath LLP, may be contacted at huw.beverley-smith@faegredrinker.com and charlotte.perowne@faegredrinker.com, respectively.

[1] https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf.