Volume 1, Number 6 November–December 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

Editor's Note: From Climate Change and Gambling to Foreign Subsidies and Data Export
Victoria Prussen Spears

International Tribunal on the Law of the Sea Issues Landmark Advisory Opinion on Climate Change
Paul A. Davies, Sophie J. Lamb, Michael D. Green, and Stephanie Forrest

Finland Proposes Sweeping Reform of Gaming Market with Open Licensing System
Johnny P. ElHachem

German Federal Government Lays Foundation for Carbon Capture and Storage in Germany
Alexander "Stefan" Rieger, John-Patrick Sweny, Jean-Philippe Brisson, and Joachim Grittmann

The European Union's Industrial Carbon Management Strategy: Building a CO_2 Market to Meet Climate Goals
François-Charles Laprévote, Camilla Cozzani, Sebastian Kummler, and Consuelo Pollonara

The European Union's ESG Ratings Regulation: Ten Questions (and Answers!)
Marc Schubert, Hannah Laurie, Bryony Pearson and Amy Waddington

What Are High-Risk Artificial Intelligence Systems Within the Meaning of the European Union's Artificial Intelligence Act and What Requirements Apply to Them?
Martin Braun, Anne Vallery, and Itsiq Benizri

The European Union Foreign Subsidies Regulation in Practice: First Cases and Enforcement Trends
François-Charles Laprévote, Wanjie Lin, and Francesco Iodice

Unlocking a Mystery of China Compliance: Fapiaos
Helen Hwang, Eric Carlson, Ping An, and Huanhuan Zhang

From Regulating to Facilitating: Key Developments in China's Safe Harbor Rules—Part II
Amigo L. Xie, Dan Wu, and Enzo Wu

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 1, No. 6 November–December 2024

393 **Editor's Note: From Climate Change and Gambling to Foreign Subsidies and Data Export**
Victoria Prussen Spears

397 **International Tribunal on the Law of the Sea Issues Landmark Advisory Opinion on Climate Change**
Paul A. Davies, Sophie J. Lamb, Michael D. Green, and Stephanie Forrest

405 **Finland Proposes Sweeping Reform of Gaming Market with Open Licensing System**
Johnny P. ElHachem

409 **German Federal Government Lays Foundation for Carbon Capture and Storage in Germany**
Alexander "Stefan" Rieger, John-Patrick Sweny, Jean-Philippe Brisson, and Joachim Grittmann

415 **The European Union's Industrial Carbon Management Strategy: Building a CO_2 Market to Meet Climate Goals**
François-Charles Laprévote, Camilla Cozzani, Sebastian Kummler, and Consuelo Pollonara

421 **The European Union's ESG Ratings Regulation: Ten Questions (and Answers!)**
Marc Schubert, Hannah Laurie, Bryony Pearson and Amy Waddington

429 **What Are High-Risk Artificial Intelligence Systems Within the Meaning of the European Union's Artificial Intelligence Act and What Requirements Apply to Them?**
Martin Braun, Anne Vallery, and Itsiq Benizri

437 **The European Union Foreign Subsidies Regulation in Practice: First Cases and Enforcement Trends**
François-Charles Laprévote, Wanjie Lin, and Francesco Iodice

447 **Unlocking a Mystery of China Compliance: Fapiaos**
Helen Hwang, Eric Carlson, Ping An, and Huanhuan Zhang

465 **From Regulating to Facilitating: Key Developments in China's Safe Harbor Rules—Part II**
Amigo L. Xie, Dan Wu, and Enzo Wu

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Paulo Fernando Campana Filho
Partner
Campana Pacca

Hei Zuqing
Distinguished Researcher
International Business School, Zhejiang University

Justin Herring
Partner
Mayer Brown LLP

Lisa Peets
Partner
Covington & Burling LLP

Joan Stewart
Partner
Wiley Rein LLP

William D. Wright
Partner
Fisher Phillips

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: 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)

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.

Copyright © 2024 Full Court Press, an imprint of Fastcase, Inc.
All Rights Reserved.
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.

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:

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

What Are High-Risk Artificial Intelligence Systems Within the Meaning of the European Union's Artificial Intelligence Act and What Requirements Apply to Them?

Martin Braun, Anne Vallery, and Itsiq Benizri*

In this article, the authors focus on the identification of "high-risk AI systems" under the EU's artificial intelligence law and the requirements applying to such systems.

The overall risk-based approach of the EU's artificial intelligence law (the AI Act)[1] means that, depending on the level of risk, different requirements apply. In total, there are four levels of risk:

1. Unacceptable, in which case AI systems are prohibited;
2. High risk, in which case AI systems are subject to extensive requirements, including regarding transparency;
3. Limited risk, which triggers only transparency requirements; and
4. Minimal risk, which does not trigger any obligations.

Identifying High-Risk AI Systems

Article 6 of the AI Act describes the thresholds that lead to an AI system being "high risk." Either such system meets the criteria in Article 6(1) AI Act, or it falls into a category referred to in Article 6(2) AI Act.

The Global Regulatory Developments Journal / November–December 2024, Vol. 1, No. 6, pp. 429–435.
© 2024 Full Court Press. All rights reserved.
ISSN 2995-7486.

Article 6(1) AI Act

An AI system will be considered high-risk if two cumulative conditions are fulfilled:

1. The AI system is intended to be used as a safety component of a product (or is a product) covered by specific EU's harmonization legislation listed in Annex I of the AI Act. This list contains more than 30 Directives and Regulations, examples include legislation regarding the safety of toys, vehicles, civil aviation, lifts, radio equipment, and medical devices; and
2. The same harmonization legislation mandates that the product, which incorporates the AI system as a safety component, or the AI system itself as a standalone product, must undergo a third-party conformity assessment before being placed on the EU market or put into service within the European Union.

Article 6(2) AI Act—Specific List

In addition, the AI Act contains, in its Annex III, a list of AI systems that must be considered high risk. This list currently contains AI systems in eight different categories. Examples include, subject to specific conditions and exemptions, biometrics, critical infrastructures, education and vocational training, employment, workers management, and access to self-employment. The European Commission (EC) has the power to amend this list.

The AI systems identified in Annex III will not be considered high risk if they do not pose a significant risk of harm to individuals' health, safety, or fundamental rights, including by not materially influencing the outcome of decision-making. This exemption applies where one of the following conditions is met:

- The AI system is intended to perform a narrow procedural task;
- The AI system is intended to improve the result of a previously completed human activity;
- The AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously

completed human assessment without proper human review; or
- The AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases that are listed as high risk.

However, the exemption never applies if the AI system performs profiling of natural persons. Profiling is defined by reference to Article 4(4) of the General Data Protection Regulation as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

If a provider considers that an AI system benefits from the exemption, it must document its assessment before placing that system or putting it into service in the European Union. The provider must also register the system in an EU database for high-risk AI systems set up and maintained by the EC.

The EC will provide guidelines no later than 18 months from the date of entry into force of the AI Act to specify the practical implementation of classification rules for high-risk AI systems, including the conditions for exceptions.

Requirements for High-Risk AI Systems

High-risk AI systems must comply with a significant number of requirements, considering their intended purposes, the generally acknowledged state of the art, and the risk management system put in place. The applicable requirements are as follows:

- *Risk Management System*. High-risk AI systems require a risk management system running throughout the entire life cycle of the system. The objective is to identify foreseeable risks to health, safety, or fundamental rights when the system is used in accordance with its intended purpose and to adopt appropriate and targeted measures to address those risks; to estimate and evaluate the risks that may emerge when the system is used in accordance with its intended purpose, and under conditions or reasonably foreseeable

misuse; and to evaluate other risks possibly arising based on a post-market monitoring analysis. Importantly, the risk management system only concerns risks that may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.

- *Data and Data Governance*. The training, validation, and testing data used to develop high-risk AI systems must be subject to appropriate data governance and management practices appropriate for the intended purpose of the system.
  - Examples include relevant design choices; appropriate data collection processes; relevant data preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment, and aggregation; the formulation of relevant assumptions; prior assessment of the availability, quantity, and suitability of the data sets needed; examination in view of possible biases likely to affect individuals' health and safety, negatively impact fundamental rights, or lead to discrimination prohibited under EU law; appropriate measures to detect, prevent, and mitigate those biases; and identification of relevant data gaps or shortcomings that prevent compliance, and how they can be addressed.
  - Training, validation, and testing data sets must be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They must have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof. In addition, data sets must consider, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioral, or functional setting within which the AI system is intended to be used.
  - For AI systems that are not developed based on AI model training, those requirements only apply to the testing data sets.

- *Technical Documentation*. Technical documentation for high-risk AI systems must be drawn up before placing the system or putting it into service in the European Union. Such documentation must demonstrate that the system complies with the requirements set out in the AI Act.
  - The AI Act provides a list of the minimum information that the technical documentation must include, such as a description of the system, its elements and the process for its development; information about the monitoring, functioning, and control of the system; a description of the appropriateness of the performance metrics for the system; a description of the risk management system; the relevant changes made by the provider through the life cycle of the system; the technical standards applied; the declaration of conformity; and the system in place to evaluate the system performance.
  - Small and medium-sized enterprises, including start-ups, may provide the elements of the technical documentation in a simplified manner. The EC will publish a simplified form to that end.
- *Recordkeeping*. High-risk AI systems must allow for the automatic recording of events (logs) over their lifetime. The objective is to ensure the traceability of the functioning of the system that is appropriate to its intended purpose. To that end, logging capabilities must enable the recording of events relevant for identifying situations that may result in the system presenting a substantial modification or having the potential to adversely affect individuals' health, safety, or fundamental rights to a degree that goes beyond that considered reasonable and acceptable in relation to its intended purpose, or under normal or reasonably foreseeable conditions of use; facilitating post-market monitoring; and monitoring the operation of the systems deployed by financial institutions.
- *Transparency and Provision of Information to Deployers*. Deployers must be provided with sufficiently transparent information to interpret the system's output and use it appropriately. The system must be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, correct, and clear information that is

relevant, accessible, and comprehensible. The instructions for use must contain at least the following information: the providers' identity and contact details; the system characteristics, capabilities, and limitations of performance; changes to the system and its performance; human oversight measures; the computational and hardware resources needed; and, where relevant, the mechanisms included within the system that allows users to properly collect, store, and interpret the logs.

- *Human Oversight*. High-risk AI systems must be designed and developed in such a way that they can be effectively overseen by humans. Human oversight must aim at preventing or minimizing the risks to health, safety, or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. The oversight measures must be commensurate to the risks, level of autonomy, and context of use.
  - Human oversight must be achieved through at least one of the following types of measures:
    - Measures identified and built, when technically feasible, into the system by the provider before it is placed on the EU's market or put into service in the European Union;
    - Measures identified by the provider before placing the system on the market or putting it into service in the European Union and that are appropriate to be implemented by the deployer.
  - Individuals to whom oversight is assigned must be able, as appropriate and proportionate to the circumstances, to:
    - Properly understand the relevant capacities and limitations of the system and monitor its operations, including in view of detecting and addressing anomalies, dysfunctions, and unexpected performance;
    - Remain aware of the possible tendency of automatically relying or over-relying on the output produced by the system;
    - Correctly interpret the system's output;

    - Decide not to use the system or otherwise disregard, override, or reverse the system's output; and
    - Intervene in the operation of the system or interrupt it through a "stop" button or a similar procedure that allows the system to come to a halt in a safe state.
- *Accuracy, Robustness, and Cybersecurity*. High-risk AI systems must be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and perform consistently in those respects throughout their life cycle. The EC will encourage the development of benchmarks and measurement methodologies to that effect.
    - The levels of accuracy and the relevant accuracy metrics must be declared in the instructions of use.
    - High-risk systems must be as resilient as possible regarding errors, faults, or inconsistencies that may occur within the system or the environment in which it operates.
    - High-risk AI systems that continue to learn after being placed on the market or put into service must be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.
    - High-risk AI systems must be resilient against attempts by unauthorized third parties to alter their use, outputs, or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems must be appropriate to the risks and circumstances.

Notes

* The authors, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, may be contacted at martin.braun@wilmerhale.com, anne.vallery@wilmerhale.com, and itsiq.benizri@wilmerhale.com, respectively.

1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.