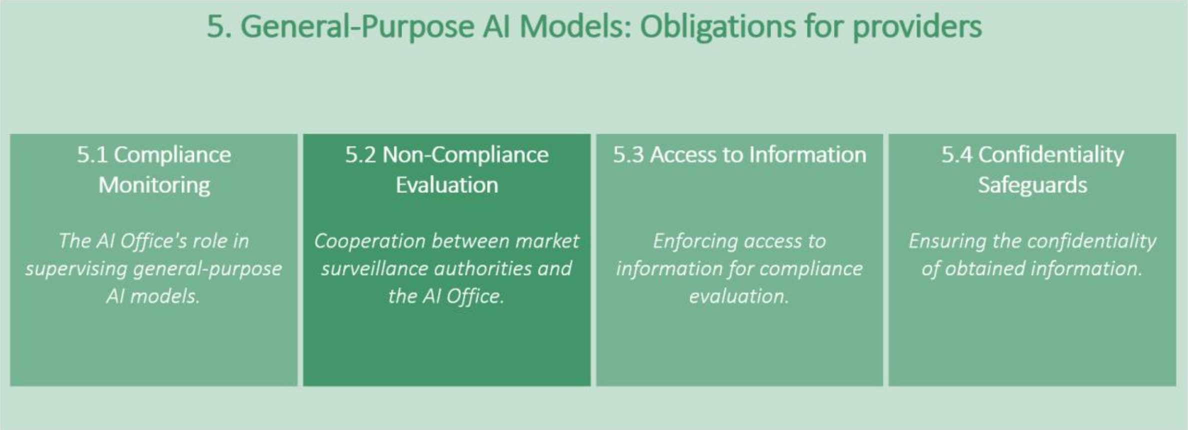
Ensuring Compliance: The Collaborative Framework Between Market Surveillance Authorities and the AI Office

Co-authored with Matt Hervey, **General Editor of The Law of Artificial Intelligence (law, regulation and ethics)**, *AI and IP expert*

14 October 2024



5. General-Purpose AI Models: Obligations for providers

5.1 Compliance Monitoring

The AI Office's role in supervising general-purpose AI models.

5.2 Non-Compliance Evaluation

Cooperation between market surveillance authorities and the AI Office.

5.3 Access to Information

Enforcing access to information for compliance evaluation.

5.4 Confidentiality Safeguards

Ensuring the confidentiality of obtained information.

Introduction

The European Union's ("EU") Artificial Intelligence ("Ai") Act (the "EU AI Act") sets a global benchmark for the regulation of artificial intelligence, with a keen focus on general-purpose AI models. These models, due to their broad applicability across various sectors, pose unique challenges and opportunities for regulatory oversight. The Act delineates clear obligations for providers of these models, emphasizing the necessity of compliance to ensure safety, transparency, and accountability in AI deployment.

A critical aspect of the EU AI Act is the collaborative framework it establishes between market surveillance authorities and the AI Office. This partnership is pivotal in evaluating and addressing non-compliance issues. Market surveillance authorities, armed with the mandate to monitor the market and enforce compliance, work in tandem with the AI Office to ensure that AI systems, especially those classified as high-risk, adhere to the stringent requirements set forth by the Act. This cooperative approach not only facilitates the sharing of information and resources but also enhances the effectiveness of the regulatory mechanisms in place.

Through this synergy, the EU AI Act aims to foster an environment where innovation in AI can progress within a structured and secure regulatory framework, ensuring that AI technologies benefit society while mitigating potential risks 6. This introduction sets the stage for a deeper exploration of the roles and responsibilities that underpin this collaborative framework, highlighting the importance of compliance and the collective effort required to achieve it.

Overview of the EU AI Act

The EU AI Act is a comprehensive regulatory framework designed to govern the deployment and use of AI systems within the EU, with a particular emphasis on general-purpose AI models. This legislation aims to ensure that AI technologies are developed and utilized in a manner that is safe, transparent, and accountable, thereby fostering trust and innovation in the digital economy.

For providers of general-purpose AI models, the EU AI Act outlines specific obligations to ensure compliance with its provisions. These obligations include the requirement to draw up and keep up-to-date technical documentation detailing the model's training, testing processes, and evaluation results. This documentation must be made available to the AI Office and national competent authorities upon request. Additionally, providers must establish policies to comply with Union copyright laws and make publicly available a detailed summary of the training content used for their models 2. Providers established outside the EU are also required to appoint an authorized representative within the Union to facilitate compliance and interaction with the AI Office.

These measures are integral to the Act's broader objective of creating a harmonized regulatory environment for AI systems. By setting clear standards and obligations for providers, the EU AI Act aims to balance the promotion of technological innovation with the need to address the ethical and societal challenges posed by AI. This legislative background is crucial for understanding the collaborative framework between market surveillance authorities and the AI Office in ensuring compliance and fostering a safe and innovative digital future.

Obligations for Providers of General-Purpose AI Models

Under the EU AI Act, providers of general-purpose AI models are subject to a comprehensive set of obligations designed to ensure the safety, transparency, and accountability of AI technologies. These obligations are crucial for maintaining public trust and safeguarding the rights of individuals in the digital age.

Firstly, providers must maintain up-to-date technical documentation of their AI models, detailing the training, testing processes, and evaluation results. This documentation, which must include information as specified in Annex XI, is essential for demonstrating compliance with the AI Act to the AI Office and national competent authorities upon request.

In addition to technical documentation, providers are required to make available information that enables other AI system providers to understand the capabilities and limitations of the general-purpose AI model. This includes ensuring that such information helps these providers comply with their regulatory obligations, while also protecting intellectual property rights and confidential business information.

For AI models identified as presenting systemic risks, providers must go further by performing model evaluations using standardized protocols, assessing and mitigating systemic risks at the Union level, and promptly reporting serious incidents to the AI Office and national competent authorities. This includes ensuring an adequate level of cybersecurity protection for both the AI model and its infrastructure.

The Role of Market Surveillance Authorities

Under the EU AI Act, market surveillance authorities play a pivotal role in ensuring the compliance of AI systems with regulatory standards. These authorities are endowed with the responsibility to monitor, investigate, and evaluate AI systems, particularly those classified as high-risk, to ascertain their adherence to the Act's requirements.

Market surveillance authorities have the authority to request information from providers of general-purpose AI models when investigating high-risk AI systems. If they encounter obstacles in accessing necessary information, they can seek assistance from the AI Office, which will facilitate access to the required data within 30 days. This collaborative mechanism ensures a thorough evaluation of AI systems, safeguarding public interests and compliance with the EU AI Act.

In cases where non-compliance is suspected, these authorities are tasked with conducting evaluations and informing both the AI Office and other relevant authorities. They must take decisive action if an AI system is found non-compliant, including requiring corrective measures from the provider or, in severe cases, prohibiting or restricting the AI system's market availability.

This framework underscores a collaborative approach between market surveillance authorities and the AI Office, emphasizing the importance of shared responsibilities in monitoring AI systems. Through their combined efforts, they ensure that AI technologies deployed across the EU are safe, transparent, and accountable, aligning with the overarching goals of the EU AI Act.

Cooperation Between the AI Office and Market Surveillance Authorities

In the evolving landscape of AI regulation within the European Union, the cooperation between the AI Office and market surveillance authorities is pivotal for the effective evaluation and enforcement of compliance concerning general-purpose AI models. This collaborative framework is designed to ensure that AI systems adhere to the stringent requirements set forth by the EU AI Act, thereby safeguarding public interests and maintaining the integrity of the digital market.

The procedural aspects of this cooperation are meticulously outlined, emphasizing the process of compliance evaluation, information sharing, and enforcement actions. When market surveillance authorities suspect non-compliance of general-purpose AI systems, especially those posing high risks, they engage with the AI Office to conduct thorough compliance evaluations. This partnership is crucial when authorities face challenges in accessing necessary information for their investigations. In such instances, they can request the AI Office's intervention to enforce access to the required data, ensuring a comprehensive evaluation is possible within 30 days.

Furthermore, the AI Office plays a significant role in supervising and enforcing compliance, particularly when systemic risks at the Union level are identified. It may conduct evaluations independently or appoint experts for this purpose, highlighting the importance of collaboration in addressing and mitigating systemic risks associated with general-purpose AI models.

This cooperative approach between the AI Office and market surveillance authorities underscores the EU's commitment to a transparent, accountable, and safe AI ecosystem. Through shared responsibilities and mutual assistance, they work towards the common goal of ensuring that AI systems deployed across the Union meet the highest standards of compliance and public safety.

Challenges and Solutions in Compliance Evaluation

In the realm of AI regulation within the European Union, the collaboration between the AI Office and market surveillance authorities is central to ensuring compliance with the EU AI Act. However, this partnership faces challenges, notably in information access and resource allocation, which are critical for effective compliance evaluation of AI systems.

One significant challenge is the difficulty market surveillance authorities may encounter in accessing necessary information related to general-purpose AI models. This is particularly problematic when investigating high-risk AI systems and assessing their compliance. The AI Act addresses this by enabling market surveillance authorities to request the AI Office's assistance in obtaining such information, ensuring that evaluations can be completed within a stipulated 30-day period. Another challenge lies in the allocation of resources. The comprehensive evaluation of AI systems, especially those presenting systemic risks, requires substantial expertise and manpower. The AI Office has the authority to conduct evaluations and may appoint independent experts for this purpose, which can help mitigate resource constraints.

To overcome these challenges, the AI Act establishes a structured framework for cooperation and information sharing. This includes the provision for mutual assistance and the enforcement of access to information, thereby facilitating a more efficient and effective compliance evaluation process. Best practices within this framework involve leveraging the AI Office's powers to support market surveillance authorities, ensuring that both entities work synergistically to uphold the regulation's standards. This collaborative approach not only addresses the challenges of information access and resource allocation but also strengthens the overall capacity to monitor and enforce AI compliance across the EU, ensuring that AI systems are safe, transparent, and accountable.

Conclusion

The collaborative framework between market surveillance authorities and the AI Office is a cornerstone of the EU AI Act, playing a vital role in upholding compliance and fostering a secure and innovative AI ecosystem within the European Union. This partnership is designed to ensure that AI systems, especially those classified as high-risk, meet the stringent requirements set forth by the Act, thereby protecting public interests and fundamental rights.

Market surveillance authorities, with the support of the AI Office, are empowered to conduct thorough evaluations of AI systems, demand corrective actions for non-compliance, and facilitate access to necessary information and documentation. This cooperative approach not only enhances the efficiency of compliance evaluations but also ensures that AI technologies deployed across the EU are safe, transparent, and accountable. Furthermore, the framework allows for the sharing of best practices and information, strengthening the overall capacity to monitor and enforce AI compliance.

Glossary

Act or EU AI Act: European Union Artificial Intelligence Act

AI: Artificial Intelligence

Board: European Union Artificial Intelligence Board

EU: European Union

SME: Small and Medium-Sized Enterprise

How can we help?

AI & Partners
Amsterdam – London - Singapore

AI & Partners – 'AI That You Can Trust'

Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialize in providing comprehensive and tailored solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organizations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.