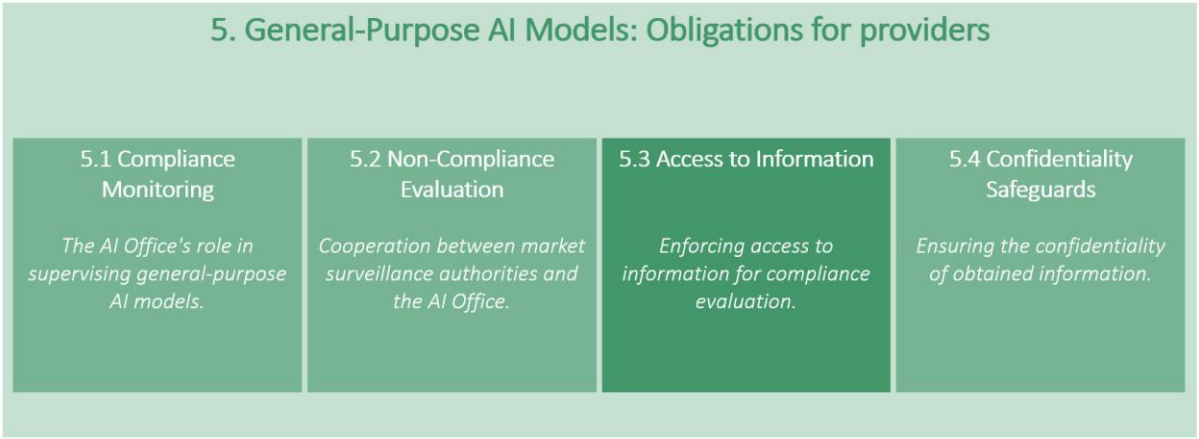
AI & Partners
Amsterdam – London - Singapore

Unlocking Compliance: Enforcing Access to Information for General-Purpose AI Models

Co-authored with Uthman Ali, *Global AI Ethics & Safety Leader*

21 October 2024



Introduction

In the digital age, transparency and access to information are paramount for regulatory compliance, especially within the realm of artificial intelligence ("AI"). The European Union ("EU") AI Act (the "EU AI Act") sets a precedent for this, particularly for providers of general-purpose AI models. These providers are mandated to share detailed information about their AI models with regulatory bodies, a step crucial for compliance evaluation.

This obligation includes the preparation and updating of technical documentation that outlines the model's training, testing processes, and evaluation results. Such documentation must at least contain the information set out in Annex XI, ensuring that it can be provided upon request to the AI Office and national competent authorities. Furthermore, providers must make available information that enables other AI system providers to understand the capabilities and limitations of the general-purpose AI model, thereby facilitating compliance across the AI value chain.

The EU AI Act's emphasis on information sharing underscores the importance of transparency in the AI ecosystem. By mandating access to comprehensive model documentation, the Act aims to foster an environment where regulatory bodies can effectively evaluate AI models for compliance, ensuring that they adhere to the highest standards of safety and accountability. This framework not only protects public interests but also supports the sustainable development of AI technologies within the EU.

The EU AI Act and General-Purpose AI Models

The EU AI Act represents a landmark regulatory framework aimed at governing the development and deployment of AI within the European Union. A key focus of the Act is on general-purpose AI models, which are versatile AI systems that can be used across a range of applications. The Act mandates that providers of these models adhere to specific obligations to ensure transparency, safety, and accountability in AI technologies.

Under the EU AI Act, providers of general-purpose AI models are required to compile and regularly update technical documentation. This documentation must detail the AI model's training, testing processes, and evaluation outcomes. It should contain, at a minimum, the information set out in Annex XI, making it accessible to the AI Office and national competent authorities upon request. Additionally, providers must prepare and make available information that enables other AI system providers to understand the capabilities and limitations of the general-purpose AI model. This includes ensuring compliance with their obligations under the regulation, while also safeguarding intellectual property rights and confidential business information.

These requirements underscore the EU AI Act's commitment to fostering an AI ecosystem that is both innovative and trustworthy. By enforcing access to information, the Act aims to facilitate compliance evaluation and promote an understanding of AI models' functionalities and potential risks, thereby ensuring that AI technologies are developed and used in a manner that aligns with EU values and standards.

Obligations for Providers

Under the EU AI Act, providers of general-purpose AI models are subject to a series of stringent obligations designed to ensure transparency, accountability, and compliance within the AI ecosystem. These obligations are critical for maintaining the integrity and safety of AI technologies across the European Union.

Providers are mandated to create and regularly update technical documentation for their AI models. This documentation must detail the model's training, testing processes, and the results of its evaluations, adhering to the minimum information requirements set out in Annex XI. Additionally, providers must compile and update information and documentation for other AI system providers who intend to integrate the general-purpose AI model into their systems.

This is essential for enabling these providers to understand the model's capabilities and limitations, ensuring their compliance with the regulation. The information provided must include, at a minimum, the elements outlined in Annex XII, while also protecting intellectual property rights and confidential business information.

Furthermore, providers are required to establish a policy to comply with Union copyright law, particularly in identifying and adhering to rights reservations. They must also prepare and publicly share a detailed summary about the content used for training the general-purpose AI model, following a template provided by the AI Office.

These comprehensive obligations underscore the EU's commitment to fostering a transparent, safe, and accountable AI landscape. By enforcing access to detailed information and documentation, the EU AI Act ensures that general-purpose AI models are developed and utilized in a manner that aligns with the Union's standards and values.

Enforcing Access to Information

The EU AI Act empowers the AI Office with significant mechanisms to enforce access to information from providers of general-purpose AI models, ensuring compliance with the regulation. This authority is crucial for maintaining transparency and accountability within the AI ecosystem. Under Article 91 of the EU AI Act, the Commission may request providers to supply documentation and additional information necessary for assessing compliance with the regulation. This includes technical documentation prepared in accordance with Articles 53 and 55, which outlines the AI model's training, testing processes, and evaluation results. The AI Office may initiate a structured dialogue with the provider before sending this request, aiming to facilitate voluntary compliance and information sharing.

Furthermore, upon a substantiated request from the scientific panel, the Commission can issue a request for information to a provider, where access to information is deemed necessary and proportionate for the fulfilment of the scientific panel's tasks under Article 68(2). The request must specify the legal basis, purpose, required information, and the timeframe for response, highlighting the fines for supplying incorrect, incomplete, or misleading information. This framework underscores the EU's commitment to a transparent and accountable AI landscape. By granting the AI Office the authority to enforce access to information, the EU AI Act ensures that AI technologies are developed and deployed in a manner that aligns with the Union's standards for safety, transparency, and accountability.

Challenges in Accessing Information

In navigating the terrain of the EU AI Act, both the AI Office and providers of general-purpose AI models encounter significant challenges in the exchange and access of information. A primary concern is the safeguarding of confidentiality and trade secrets. The Act mandates the sharing of detailed technical documentation and training data summaries, which could potentially expose sensitive proprietary information. Balancing the need for transparency with the protection of intellectual property rights and confidential business information is hard, underscored by the Act's provisions to respect these concerns.

Another hurdle is the technical feasibility of providing access to complex AI models. The intricate nature of these models, coupled with the vast amounts of data they utilize, poses a challenge in sharing comprehensive information without compromising the models' integrity or breaching copyright laws.

The Act addresses this by allowing for the provision of detailed summaries rather than exhaustive technical data, aiming to strike a balance between transparency and the protection of sensitive information. These challenges highlight the intricate balance the EU AI Act seeks to achieve between fostering innovation and ensuring accountability in the AI sector.

The Role of Authorised Representatives

Authorized representatives play a pivotal role in bridging the gap between providers of general-purpose AI models based outside the European Union and the AI Office, ensuring adherence to the EU AI Act's stringent requirements. These representatives, established within the Union, act on behalf of the non-EU providers through a written mandate, facilitating compliance and access to information. Their responsibilities include verifying that the technical documentation, as specified in Annex XI, has been accurately prepared and that all obligations under Articles 53 and, where applicable, Article 55, have been met by the provider.

The tasks of these authorized representatives are clearly defined; they are responsible for verifying that the technical documentation, as specified in Annex XI, has been accurately drawn up and that all obligations under Articles 53 and, where applicable, Article 55, have been fulfilled by the provider. Moreover, they must retain a copy of this documentation and the provider's contact details for a decade after the AI model has been introduced to the market, ensuring that this information is readily available to the AI Office and national competent authorities upon request.

Authorized representatives also play a crucial role in providing all necessary information and documentation to demonstrate compliance with the Act's obligations, cooperating with the AI Office and competent authorities in any actions related to the general-purpose AI model. This cooperative framework ensures that even AI models developed outside the EU's borders meet the Union's regulatory standards, promoting a safe and transparent AI ecosystem across the Union.

Conclusion

Enforcing access to information stands as a pivotal element in the EU AI Act's strategy to regulate general-purpose AI models, ensuring they align with the Union's standards for safety, transparency, and innovation. The Act mandates providers to maintain and share comprehensive technical documentation and other relevant information, detailing the AI model's development, capabilities, and limitations. This requirement not only aids regulatory bodies, such as the AI Office, in assessing compliance but also enhances the understanding and trust between AI providers and the broader community.

Moreover, the Act's provisions for transparency extend to making summaries of training data publicly available, balancing the need to protect intellectual property with the public's right to information. This fosters an environment where innovation can thrive, supported by a framework of accountability and public trust.

The collaboration between AI providers and regulatory bodies, facilitated by the EU AI Act, underscores the Union's commitment to a digital future that is safe, transparent, and innovative. By prioritizing access to information, the Act ensures that AI technologies developed or deployed within the EU contribute positively to society, adhering to the highest standards of compliance and ethical considerations.

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.