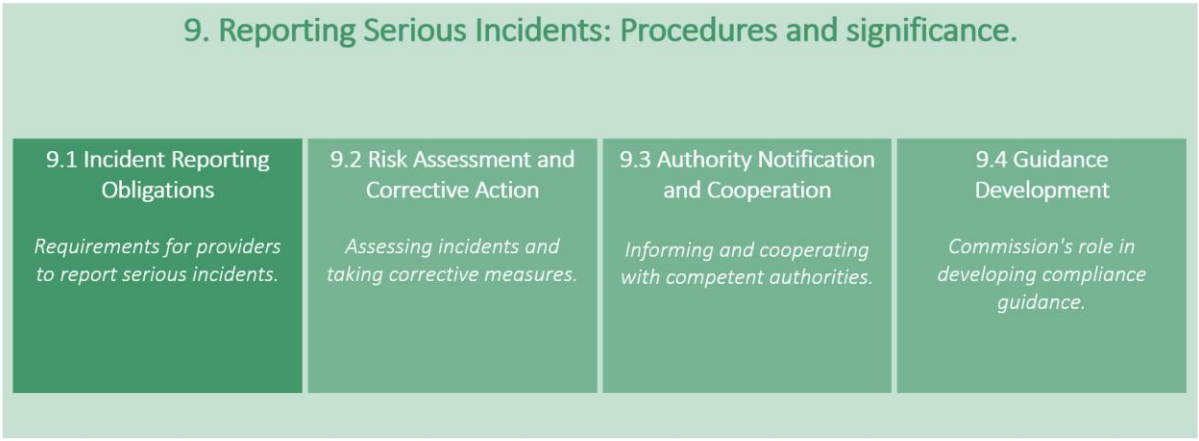
Navigating the Waters of Compliance: A Guide to Reporting Serious Incidents Under the EU AI Act

Co-authored with Dr. Benedikt Kohn, Taylor Wessing, *Tech Attorney | AI-Regulation, IT & Data*

27 January 2025



Introduction

In the realm of AI regulation, reporting serious incidents under the EU AI Act stands as a cornerstone of transparency and accountability. Providers play a pivotal role in upholding these obligations, ensuring the safety and reliability of AI systems.

By adhering to these reporting requirements, providers not only fulfill their legal obligations but also contribute to a culture of trust and integrity within the AI landscape. Transparent reporting allows for timely identification and mitigation of potential risks, safeguarding against adverse impacts on users and stakeholders.

Moreover, it fosters continuous improvement in AI systems, driving innovation while prioritizing safety and reliability. Through robust incident reporting mechanisms, providers demonstrate their commitment to ethical AI practices and stakeholder well-being.

As the regulatory framework evolves, the importance of reporting serious incidents remains paramount. It serves as a guiding principle for providers navigating the complex landscape of AI compliance, empowering them to navigate potential challenges with diligence and responsibility. Ultimately, adherence to reporting obligations under the EU AI Act not only mitigates risks but also strengthens the foundation of trust essential for the sustainable advancement of AI technologies.

Understanding Serious Incident Reporting

Under the EU AI Act, a "serious incident" is a term defined by Article 73, mandating providers of high-risk AI systems to report such incidents to the market surveillance authorities of the Member States where they occur. These incidents encompass a range of scenarios, including those resulting in death, serious harm to health, or significant disruptions to critical infrastructure.

Incidents requiring reporting may involve AI systems causing harm to individuals or infrastructure due to malfunction, error, or misuse. Examples include accidents resulting from autonomous vehicle malfunctions, medical diagnosis errors leading to patient harm, or AI-driven systems causing disruptions in essential services like transportation or energy distribution. The reporting obligation serves to ensure prompt and effective responses to incidents that pose risks to public safety, health, or critical infrastructure. By reporting serious incidents, providers contribute to the early detection and mitigation of potential harms associated with AI technologies.

Understanding the scope of incidents requiring reporting is essential for providers to fulfil their obligations under the EU AI Act responsibly. It underscores the importance of vigilance and transparency in managing the risks inherent in deploying AI systems, ultimately contributing to the safety and reliability of AI technologies in society.

Reporting Obligations and Timelines

Providers under the EU AI Act have clear obligations regarding the reporting of serious incidents, which are triggered once a causal link between the AI system and the incident is established. Timelines for reporting vary depending on the severity of the incident, ensuring appropriate and timely responses.

For general incidents, providers must report within a maximum of 15 days from the identification of the incident. However, for more severe cases, such as widespread infringements, the reporting window narrows to just two days. In instances where incidents result in death, providers are required to report within 10 days of the incident occurring. These timelines emphasize the importance of swift action in addressing serious incidents associated with AI systems. By promptly reporting incidents, providers enable authorities to assess risks, initiate investigations, and implement necessary measures to mitigate harm.

Adhering to reporting obligations not only ensures compliance with regulatory requirements but also demonstrates a commitment to transparency and accountability in AI deployment. It underscores the responsibility of providers to prioritize public safety and mitigate potential risks associated with AI technologies. Understanding reporting timelines is crucial for providers to navigate compliance requirements effectively. It enables them to establish robust incident response procedures, ensuring swift and appropriate actions in the event of serious incidents involving AI systems.

Initial and Follow-Up Reporting

Providers are required to promptly submit an initial report upon identifying a serious incident involving an AI system under the EU AI Act. This initial report may be incomplete and serves as a notification to competent authorities. Subsequently, providers must follow up with a complete report, which includes comprehensive details of the incident, the AI system involved, and any investigative findings.

The EU AI Act mandates providers to conduct thorough investigations into serious incidents, including risk assessments and corrective actions. Cooperation with competent authorities is essential throughout this process to ensure transparency and facilitate effective incident management. By performing diligent investigations and cooperating with authorities, providers demonstrate their commitment to addressing serious incidents and mitigating associated risks. This proactive approach not only fulfils regulatory obligations but also contributes to maintaining trust and confidence in AI technologies.

Understanding the process for initial and follow-up reporting is crucial for providers to navigate compliance requirements effectively. It enables them to establish robust incident response protocols, ensuring timely and accurate reporting of serious incidents involving AI systems.

Confidentiality and Compliance Guidance

Providers must adhere to strict confidentiality obligations outlined in the EU AI Act to safeguard information obtained during the reporting and investigation of serious incidents. This ensures that sensitive data related to incidents and AI systems remain protected, preserving the integrity of ongoing investigations and maintaining trust in the reporting process.

To facilitate compliance with these obligations, the Commission has developed dedicated guidance, offering clear directives and best practices for providers. This guidance assists providers in understanding their reporting obligations under the EU AI Act and provides practical insights into managing confidentiality concerns effectively.

By following the confidentiality requirements and utilizing the guidance provided by the Commission, providers can navigate the reporting process with confidence and ensure compliance with the EU AI Act. Upholding confidentiality not only demonstrates commitment to regulatory compliance but also reinforces trust in the reporting framework, ultimately enhancing the safety and reliability of AI systems within the EU.

Challenges and Best Practice

Meeting reporting obligations under the EU AI Act can present various challenges for providers, such as identifying and assessing incidents accurately and ensuring timely reporting. To overcome these challenges, providers should implement best practices for effective reporting. Firstly, establishing a robust post-market monitoring system is essential.

This system allows providers to continuously monitor the performance and safety of AI systems in real-world settings, enabling the early detection of potential incidents. Additionally, maintaining clear communication channels within the organization facilitates the prompt identification and reporting of incidents.

Furthermore, conducting regular risk assessments of AI systems can help providers anticipate and mitigate potential risks, enhancing their proactive approach to incident management. Implementing standardized procedures and protocols for incident reporting ensures consistency and efficiency in the reporting process. Collaborating closely with relevant stakeholders, including competent authorities and industry peers, can provide valuable insights and support in navigating reporting obligations effectively. By embracing these best practices, providers can ensure timely and accurate reporting of serious incidents, thereby fulfilling their obligations under the EU AI Act and contributing to the overall safety and reliability of AI systems.

Conclusion

In conclusion, incident reporting under the EU AI Act plays a pivotal role in ensuring the safe and responsible deployment of AI systems. By promptly reporting serious incidents, providers uphold transparency and accountability, fostering trust in AI technologies. Adherence to reporting obligations not only fulfils regulatory requirements but also supports effective market surveillance and risk management. It serves as a cornerstone of AI regulation, contributing to the overall safety and reliability of AI systems within the EU. Moving forward, continued diligence in incident reporting will be essential for maintaining the integrity of the regulatory framework and safeguarding against potential risks associated with AI deployment.

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'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

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