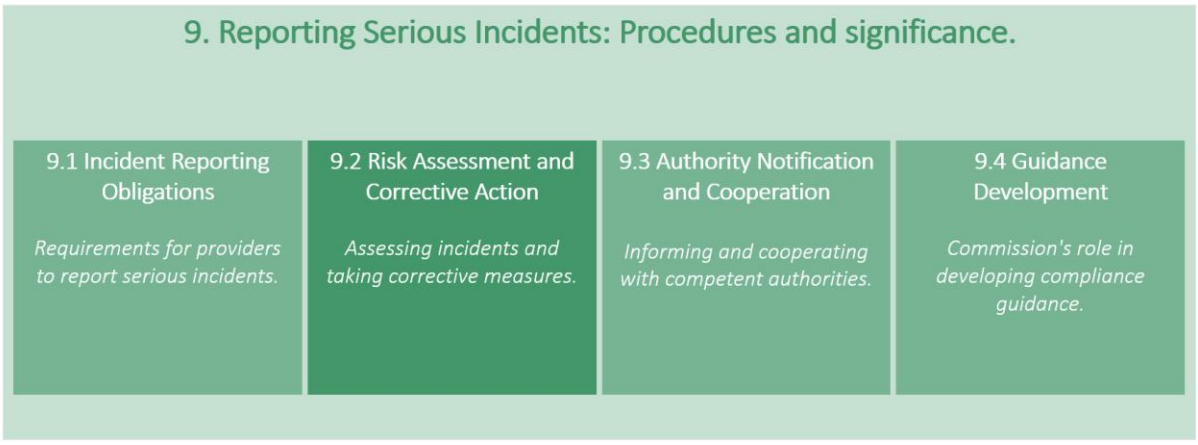
Proactive Measures: Assessing Incidents and Implementing Corrective Actions Under the EU AI Act

Co-authored with Matt Hervey, **Gowling WLG**, *Partner*

3 February 2025



Introduction

This is the second article in our series about reporting serious incidents under the EU AI Act. The first article in this series covered Incident Reporting Obligations with Dr. Benedikt Kohn.

To begin, we look at the basics: **What is the EU AI Act?** The EU AI Act is a landmark regulation designed to govern AI systems, ensuring safety, compliance, and innovation across the European Union.

The EU AI Act's Framework for Serious Incident Reporting

The EU AI Act establishes a robust framework for incident reporting by providers of high-risk AI systems. Under this framework, providers are mandated to report any serious incidents to the market surveillance authorities of the Member States where the incident occurred. This reporting obligation is triggered when a causal link between the AI system and the incident has been established.

Immediate reporting is paramount under the EU AI Act, emphasizing the urgency of notifying authorities upon confirming the connection between the AI system and the incident. This requirement ensures that relevant stakeholders are promptly informed of potential risks associated with AI systems, enabling swift action to mitigate harm and protect public safety.

By requiring providers to report serious incidents in a timely manner, the EU AI Act promotes transparency and accountability within the AI ecosystem. This transparency facilitates the exchange of critical information between providers, authorities, and other stakeholders, fostering collaboration in addressing emerging challenges and enhancing overall safety.

In essence, the EU AI Act's framework for incident reporting establishes clear guidelines for providers to fulfil their reporting obligations promptly and effectively. By adhering to these requirements, providers can contribute to a proactive approach to incident management, ultimately safeguarding the integrity and trustworthiness of AI systems.

Risk Assessment of Serious Incidents

Following the reporting of a serious incident as mandated by the EU AI Act, providers are required to conduct a comprehensive risk assessment. This assessment involves evaluating the incident's risk implications, with a particular focus on understanding the AI system's role in the event. Providers must identify the root cause of the incident and assess its potential impact on users, the environment, and critical infrastructure.

The risk assessment process encompasses a thorough analysis of the incident's contributing factors, including the AI system's design, functionality, and deployment context. Providers must also consider any relevant external factors that may have influenced the incident's occurrence.

Once the risk assessment is complete, providers are tasked with identifying and implementing corrective actions to mitigate similar risks in the future. This involves developing and implementing measures to address the root causes of the incident, enhance the AI system's safety and reliability, and prevent recurrence.

By conducting risk assessments and implementing corrective actions, providers can proactively address safety concerns and ensure the ongoing compliance of their AI systems with regulatory requirements. This proactive approach not only enhances user safety and confidence but also demonstrates the provider's commitment to responsible AI development and deployment.

In summary, the EU AI Act's requirement for risk assessment following a serious incident underscores the importance of proactive risk management in AI deployment. By systematically identifying and addressing risks, providers can strengthen the safety and reliability of AI systems, fostering trust and accountability in the AI ecosystem.

Implementing Corrective Actions

Providers are mandated by the EU AI Act to implement corrective actions following the completion of a risk assessment. These actions are crucial for preventing the recurrence of serious incidents and ensuring compliance with the Act's safety standards.

Upon identifying the root causes and potential risks associated with a serious incident, providers must promptly develop and implement corrective measures. These actions aim to address the underlying issues identified during the risk assessment process and mitigate similar risks in the future.

Corrective actions may include modifications to the AI system's design, functionality, or deployment protocols to enhance safety and reliability. Providers must also consider implementing additional safeguards and controls to minimize the likelihood of similar incidents occurring.

Furthermore, the implementation of corrective actions should be accompanied by ongoing monitoring and evaluation to ensure their effectiveness. Providers must remain vigilant in assessing the impact of these measures and adjusting them as necessary to maintain compliance with regulatory requirements and safeguard user safety.

By diligently implementing corrective actions, providers demonstrate their commitment to proactive risk management and continuous improvement in AI system safety. This approach not only mitigates potential risks but also enhances user confidence in the reliability and accountability of AI technologies.

Cooperation with Competent Authorities

Providers have a legal obligation under the EU AI Act to collaborate fully with competent authorities and, if applicable, the notified body involved during investigations into serious incidents. This cooperation is essential for facilitating thorough and effective inquiries into the incident's causes and identifying appropriate corrective actions.

It is imperative for providers to refrain from making any alterations to the AI system that could impact the assessment of the incident's root causes before notifying the competent authorities. This prohibition ensures the integrity of the investigation process and prevents potential interference that could hinder the accurate determination of factors contributing to the incident.

By adhering to these cooperative measures, providers demonstrate their commitment to transparency, accountability, and regulatory compliance. Collaboration with competent authorities enables a comprehensive evaluation of the incident, fostering trust among stakeholders and promoting the safety and reliability of AI systems.

In summary, the EU AI Act mandates providers to cooperate fully with competent authorities and refrain from altering AI systems before notifying them of serious incidents. This cooperative approach enhances the effectiveness of incident investigations and supports the overarching goal of ensuring the safety and compliance of AI technologies.

Confidentiality and Compliance Guidance

Providers must adhere to strict confidentiality obligations concerning information obtained during the reporting and investigation of serious incidents under the EU AI Act. This ensures the protection of sensitive data and maintains the integrity of the investigation process.

The Commission has recognized the importance of providing clear guidance to aid providers in fulfilling their reporting obligations effectively. As such, it has developed dedicated guidance to assist providers in understanding and complying with the requirements set forth in the EU AI Act.

By following these confidentiality obligations and leveraging the guidance provided by the Commission, providers can navigate the reporting and investigation process with confidence and clarity. This proactive approach not only facilitates compliance with regulatory requirements but also promotes transparency and accountability in addressing serious incidents involving AI systems.

In summary, confidentiality obligations play a crucial role in safeguarding information related to serious incidents, while the Commission's compliance guidance serves as a valuable resource for providers seeking to fulfil their reporting obligations under the EU AI Act. Compliance with these provisions ensures the protection of sensitive data and supports the overarching goal of promoting the safe and responsible use of AI technologies.

Conclusion

In conclusion, the EU AI Act underscores the pivotal role of risk assessment and corrective action in upholding the safety and reliability of AI systems. By mandating providers to conduct thorough risk assessments and implement appropriate corrective actions, the Act establishes a framework for proactive measures aimed at preventing the recurrence of serious incidents.

Adherence to these processes is paramount, serving as a cornerstone of AI regulation and market surveillance. It not only fosters accountability within the industry but also enhances public trust in AI technologies. Through rigorous risk assessment and timely corrective action, providers can ensure compliance with safety standards outlined in the EU AI Act, ultimately contributing to the advancement of responsible AI deployment and fostering a culture of safety and reliability in the AI ecosystem.

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.