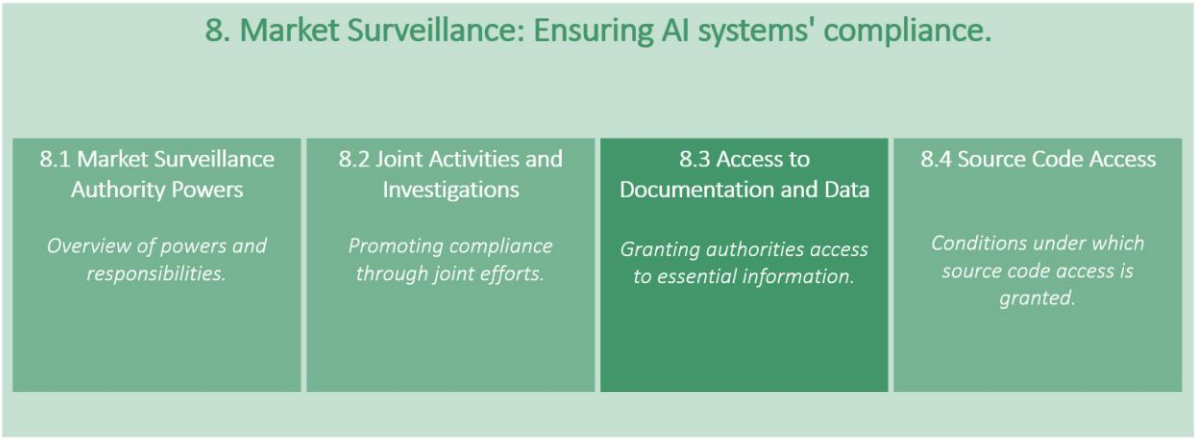
Ensuring AI Compliance: The Critical Role of Documentation and Data Access

Co-authored with Charles Kerrigan, **CMS Law**, *Partner*

13 January 2025



Introduction

This is the third article in our series about market surveillance under the EU AI Act. Previous articles in this series include Market Surveillance Powers with Dr. Derek Warden, and closely followed by Joint Activities and Investigations with Prof. Dr. Ingrid Vasiliu-Feltes.

As always, we start at step one: **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 and Market Surveillance

To enforce the EU AI Act, market surveillance authorities are responsible for monitoring AI systems to ensure they meet safety, performance, and ethical standards. A critical part of their role is gaining access to the necessary documentation and data to evaluate whether an AI system complies with the law.

This access is essential for ensuring AI technologies are transparent and accountable. However, it must be managed carefully to protect sensitive information, including trade secrets, proprietary data, and other confidential details that give developers their competitive edge.

The challenge is balancing these needs—granting regulators the information they require for thorough assessments while safeguarding intellectual property rights. This balance is vital for fostering trust and accountability, supporting responsible AI innovation, and preserving the integrity of the European AI ecosystem.

Market surveillance authorities come in different forms and operate with varying capacities, as summarized in Table 1 below.

Table 1: Overview of Market Surveillance Authorities (Articles 26, 74, 75, and 76)

Question	Answer
What are they?	Market surveillance authorities are designated national bodies within the European Union responsible for overseeing the compliance of AI systems with the EU AI Act. Their primary role is to ensure that AI systems, particularly high-risk ones, adhere to safety, ethical, and legal standards.
What do they do?	They do a range of things under Articles 74 & 85: **Enforcement and Monitoring**: They enforce compliance with the EU AI Act, especially for high-risk AI systems, ensuring these systems meet safety and fundamental rights standards. **Information Sharing**: Authorities report annually to the European Commission and national competition authorities about findings that could impact Union law on competition, as well as any prohibited practices and measures taken. **Coordination and Joint Activities**: They coordinate with other national bodies and propose joint activities to promote compliance and identify non-compliance. **Access to Information**: They have the right to access documentation, training, validation, and testing data sets used for developing high-risk AI systems. They may also access the source code under specific conditions. **Handling Complaints**: Individuals or entities can lodge complaints with these authorities if they believe there has been an infringement of the regulation. **Testing in Real World Conditions**: They ensure that testing of AI systems in real-world conditions complies with regulations and can suspend or modify testing if necessary. **Mutual Assistance and Supervision**: They collaborate with the AI Office and other authorities to monitor and supervise compliance, especially for general-purpose AI systems.

Who are they?	Article 74 and Recital 156 requires market surveillance authorities to be designated under the EU AI Act, which applies from 2 August 2026. At this time, the European Data Protection Supervisor will be one market surveillance authority.
What powers do they have?	They have several powers: **Access to Information:** They can access documentation, training, validation, and testing data sets used for developing high-risk AI systems. They can also request access to the source code if necessary for compliance assessment. **Testing and Evaluation:** Authorities can organize testing of high-risk AI systems to verify compliance, especially if documentation is insufficient. **Enforcement Actions:** They can require operators to take corrective actions, withdraw, or recall non-compliant AI systems from the market. **Confidentiality:** They must handle all obtained information in accordance with confidentiality obligations to protect intellectual property and sensitive data.
Who do they apply to?	They oversee both providers and deployers: Deployers • **High-Risk AI Systems:** Deployers must ensure these systems are used correctly, assign qualified human oversight, and continuously monitor their operation. • **Financial Institutions:** Deployers in financial institutions are supervised by the national authority responsible for financial oversight. • **Public Authorities and Union Institutions:** Public deployers or Union institutions must register high-risk AI systems and inform authorities if a system is not registered. Providers • **High-Risk AI Systems:** Providers are closely monitored to ensure their systems meet safety and fundamental rights standards. • **Financial Institutions:** Providers in financial institutions are also supervised by the relevant national financial authority. • **General-Purpose AI Models:** Providers of these models are monitored when their systems are used in high-risk applications. • **Union Institutions and Bodies:** The European Data Protection Supervisor oversees Union institutions, except for the Court of Justice of the European Union in its judicial role.

Their responsibilities encompass a wide range of tasks, including assessing documentation and data provided by AI developers and providers. By accessing this information, market surveillance authorities can conduct thorough evaluations to ascertain the conformity of AI systems with regulatory standards. However, this oversight is balanced with the need to protect proprietary information and trade secrets held by AI stakeholders.

Striking this balance is essential to foster transparency, accountability, and responsible innovation in the deployment of AI technologies across the EU. Market surveillance authorities' responsibilities cover many things, as outlined in Table 2 below.

Table 2: Market Surveillance Authorities' Responsibilities (Articles 74, 75, 78, 79, and 85)

Question	Answer
Monitoring	**Post-Market Monitoring:** Authorities oversee AI systems after they have been placed on the market to ensure ongoing compliance with the EU AI Act. **Information Sharing:** They report annually to the European Commission and relevant national competition authorities about any findings that could impact Union law on competition, as well as any prohibited practices and measures taken. **Coordination:** Authorities coordinate with other national bodies and propose joint activities to promote compliance and identify non-compliance.
Enforcement	**Access to Information:** Authorities have the right to access documentation, training, validation, and testing data sets used for developing high-risk AI systems. They may also access the source code under specific conditions. **Testing and Evaluation:** They can organize testing of high-risk AI systems to verify compliance, especially if documentation is insufficient. **Corrective Actions:** Authorities can require operators to take corrective actions, withdraw, or recall non-compliant AI systems from the market. **Handling Complaints:** They handle complaints from individuals or entities regarding potential infringements of the regulation. **Confidentiality:** Authorities must handle all obtained information in accordance with confidentiality obligations to protect intellectual property and sensitive data.

Overall, market surveillance authorities serve as guardians of compliance, working diligently to uphold the integrity of the regulatory framework and promote the safe and ethical use of AI systems within the European Union.

Access to Documentation and Data

Under the EU AI Act, market surveillance authorities are empowered with access to crucial documentation and data to ensure compliance with regulatory standards. The Act stipulates that the AI Office, as a key regulatory body, has the authority to monitor and supervise compliance efforts.

This includes the access to technical documentation and data sets pertaining to high-risk AI systems, enabling thorough assessments of their conformity with regulatory requirements. Market surveillance authorities can only access documentation and data for specific reasons, as outlined in Table 3 below.

Table 3: Market Surveillance Authorities powers regarding access to documentation and data (Articles 74, 77, and 78)

Question	Answer
What Documentation and Data Can They Access?	**General Access:** Authorities can access documentation, training, validation, and testing data sets used for developing high-risk AI systems. **Source Code Access:** They may access the source code of high-risk AI systems upon a reasoned request, but only when necessary to assess conformity and when other verification methods have been exhausted or proved insufficient.
Under What Conditions Can They Access Documentation and Data?	**Necessity for Compliance Assessment:** Access is granted when it is necessary to assess the conformity of a high-risk AI system with the requirements set out in the regulation. **Security Safeguards:** Access to sensitive information, such as source code, is subject to security safeguards to protect intellectual property and confidentiality. **Necessity and Proportionality:** Access is granted when it is necessary and proportionate to fulfill their tasks under the regulation, ensuring that authorities do not overreach in their data requests.
How is Confidentiality Maintained?	**Confidentiality Obligations:** Any information or documentation obtained by market surveillance authorities must be treated in accordance with confidentiality obligations to protect intellectual property rights and sensitive data. **Consultation Before Disclosure:** Information exchanged on a confidential basis cannot be disclosed without prior consultation with the originating authority and the deployer, especially when it involves law enforcement or national security interests.
What Happens if Documentation is Insufficient?	**Testing Requests:** If documentation is insufficient to ascertain compliance, authorities can request testing of the high-risk AI system through technical means.

Moreover, the Act outlines conditions under which access to source code is granted (see **Table 4** below). Source code access is vital for market surveillance authorities to conduct in-depth evaluations of AI systems, particularly those deemed high-risk. However, access to source code is subject to certain safeguards to protect proprietary information and trade secrets held by AI developers and providers.

Table 4: Market Surveillance Authorities powers regarding access to documentation and data (Article 78)

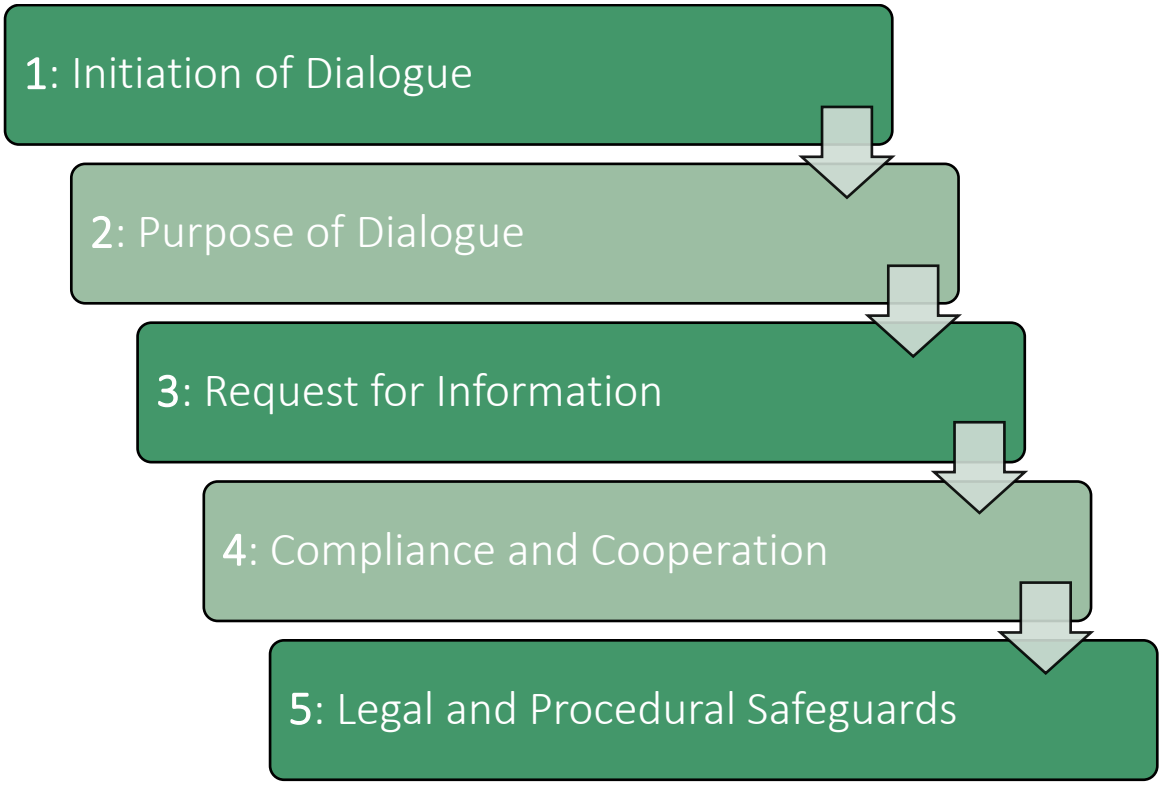
Section	Answer
Confidentiality Obligations	**Protection of Intellectual Property and Trade Secrets:** Authorities must respect the confidentiality of information and data obtained during their tasks, particularly protecting intellectual property rights, confidential business information, and trade secrets, including source code. **Security and Confidentiality Measures:** Authorities are required to implement adequate cybersecurity measures to protect the security and confidentiality of the information and data obtained. They must also delete data once it is no longer needed for its original purpose. **Consultation Before Disclosure:** Information exchanged on a confidential basis between national competent authorities or with the Commission cannot be disclosed without prior consultation with the originating authority and the deployer, especially when it involves high-risk AI systems used by law enforcement or other sensitive sectors.
Specific Conditions	**Access to Documentation:** When law enforcement, immigration, or asylum authorities are providers of high-risk AI systems, the technical documentation must remain within their premises. Market surveillance authorities can access this documentation only if they have the appropriate security clearance. **Exchange with Third Countries:** The Commission and Member States may exchange confidential information with regulatory authorities of third countries, provided there are bilateral or multilateral confidentiality arrangements ensuring an adequate level of confidentiality.

By granting market surveillance authorities access to essential documentation, data, and source code under specific conditions, the EU AI Act ensures robust oversight and enforcement of compliance measures. This access enables authorities to effectively evaluate AI systems' adherence to safety, performance, and ethical standards, thereby upholding the integrity of the regulatory framework and promoting trust in AI technologies within the European Union.

The Commission's Powers and Responsibilities

The Commission plays a pivotal role in ensuring AI compliance by requesting documentation and information from providers of general-purpose AI models. This process is governed by a structured dialogue initiated by the AI Office to facilitate communication and gather necessary details before sending a formal request. These requests are made based on a solid legal basis established under the EU AI Act. It follows five easy steps, as shown in **Figure 1** below.

Figure 1: Process for Requesting Documentation and Information (Article 91)



1. Initiation of Dialogue

The AI Office may initiate a structured dialogue with the provider of a general-purpose AI model to gather more information and facilitate understanding.

2. Purpose of Dialogue

The dialogue aims to clarify requirements and expectations regarding the documentation and information needed to assess compliance with the EU AI Act.

3. Request for Information

If necessary, following the structured dialogue, the Commission may issue a formal request for documentation and information. This request will specify the legal basis, purpose, and the specific information required, along with a deadline for compliance.

4. Compliance and Cooperation

The provider is obligated to supply the requested information, ensuring it is complete, accurate, and not misleading.

5. Legal and Procedural Safeguards

The request will indicate potential fines for non-compliance and ensure that the legal basis and purpose of the request are clearly stated.

The structured dialogue serves as a precursor to the formal request for documentation and data, enabling the Commission to engage with AI providers in a collaborative manner. Through this dialogue, the AI Office can clarify requirements, address any concerns, and ensure that the subsequent request is well-founded and aligned with regulatory objectives.

Once the structured dialogue is completed, the Commission can proceed with a formal request for documentation and information. This request is supported by the legal framework provided by the EU AI Act, which grants the Commission the authority to obtain necessary documentation to assess compliance with regulatory standards.

By exercising its powers and responsibilities in requesting documentation and information, the Commission plays a crucial role in ensuring transparency, accountability, and adherence to regulatory requirements within the AI industry. This approach promotes trust and confidence in AI technologies while upholding the integrity of the regulatory framework established by the EU AI Act.

Confidentiality and Data Protection

The EU AI Act upholds strict confidentiality obligations to safeguard information and data obtained during market surveillance activities. These obligations ensure that sensitive information provided by AI providers remains protected, balancing the imperative of regulatory oversight with the preservation of intellectual property rights and confidential business information.

Under the Act, market surveillance authorities are bound by confidentiality requirements, preventing the unauthorized disclosure of proprietary data or trade secrets. This framework establishes trust between authorities and AI providers, fostering a collaborative environment conducive to compliance.

Moreover, the Act outlines mechanisms for handling confidential information securely, such as restricted access and encryption protocols. These measures bolster data protection while enabling authorities to fulfil their regulatory responsibilities effectively.

By striking a delicate balance between transparency and confidentiality, the EU AI Act promotes accountability and fairness in regulatory enforcement. It enables market surveillance authorities to access essential documentation and data while safeguarding the sensitive information vital for innovation and competitiveness in the AI industry. This approach ensures that compliance efforts uphold the integrity of the regulatory framework without compromising the confidentiality of proprietary information.

Challenges and Best Practices

Market surveillance authorities encounter several challenges when accessing and handling documentation and data in the context of AI compliance. These challenges may include navigating complex legal frameworks, ensuring data security, and balancing the need for transparency with confidentiality requirements.

To address these challenges, market surveillance authorities and AI providers can adopt several best practices. Authorities can streamline their procedures for requesting documentation and data, providing clear guidelines to AI providers and minimizing bureaucratic hurdles. Additionally, they can implement robust data protection measures, such as encryption and restricted access protocols, to safeguard sensitive information.

For AI providers, transparency and cooperation are key. They should proactively engage with authorities, promptly responding to requests for documentation and data while ensuring compliance with confidentiality obligations. Moreover, AI providers can establish internal protocols for data management and security, ensuring that sensitive information is handled responsibly. AI system players can expect support on this with upcoming guidance from the European Commission due in Q2/Q3 2025, as shown in Table 5 below.

Table 5: Commission guidance about reporting of serious incidents under Article 73(7)

Article 73	Answer
This article explains that companies offering high-risk AI systems are required to notify the authorities in the country where a serious incident occurs. The notification must happen as soon as the company becomes aware of a potential link between their AI system and the incident, or if there is a reasonable likelihood of such a connection. Reports must be filed within 15 days of discovering the incident. In cases of particularly severe or widespread incidents, reporting is required within two days, while incidents involving fatalities must be reported within 10 days. Companies are allowed to submit an initial, incomplete report but are obligated to provide a comprehensive follow-up. Additionally, they must investigate the incident and cooperate with authorities, who are expected to take appropriate measures within seven days.	This guidance is directly relevant to market surveillance authorities as it facilitates compliance with obligations related to the reporting of serious incidents involving AI systems. Market surveillance authorities are involved in receiving notifications of serious incidents and taking appropriate measures.

This article explains that companies offering high-risk AI systems are required to notify the authorities in the country where a serious incident occurs. The notification must happen as soon as the company becomes aware of a potential link between their AI system and the incident, or if there is a reasonable likelihood of such a connection. Reports must be filed within 15 days of discovering the incident. In cases of particularly severe or widespread incidents, reporting is required within two days, while incidents involving fatalities must be reported within 10 days. Companies are allowed to submit an initial, incomplete report but are obligated to provide a comprehensive follow-up. Additionally, they must investigate the incident and cooperate with authorities, who are expected to take appropriate measures within seven days.

By adhering to these best practices, market surveillance authorities and AI providers can effectively navigate the challenges associated with accessing and handling documentation and data. This collaborative approach promotes compliance with regulatory requirements while upholding the confidentiality and security of sensitive information.

Conclusion

Access to documentation and data plays a pivotal role in ensuring AI systems' compliance under the EU AI Act. It enables market surveillance authorities to effectively monitor and supervise AI activities, ensuring adherence to regulatory standards and promoting safety and reliability.

Confidentiality obligations outlined in the EU AI Act strike a balance between regulatory oversight and the protection of sensitive information, fostering trust and collaboration between authorities and AI providers. By upholding these obligations, stakeholders can navigate challenges associated with data access while safeguarding intellectual property rights and confidential business information.

In conclusion, the EU's approach to documentation and data access is essential for fostering innovation while prioritizing safety and compliance in the AI landscape. By adhering to confidentiality obligations and adopting best practices, stakeholders can collectively contribute to a transparent and trustworthy AI ecosystem within the EU, ensuring that AI technologies benefit society while mitigating potential risks.

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.