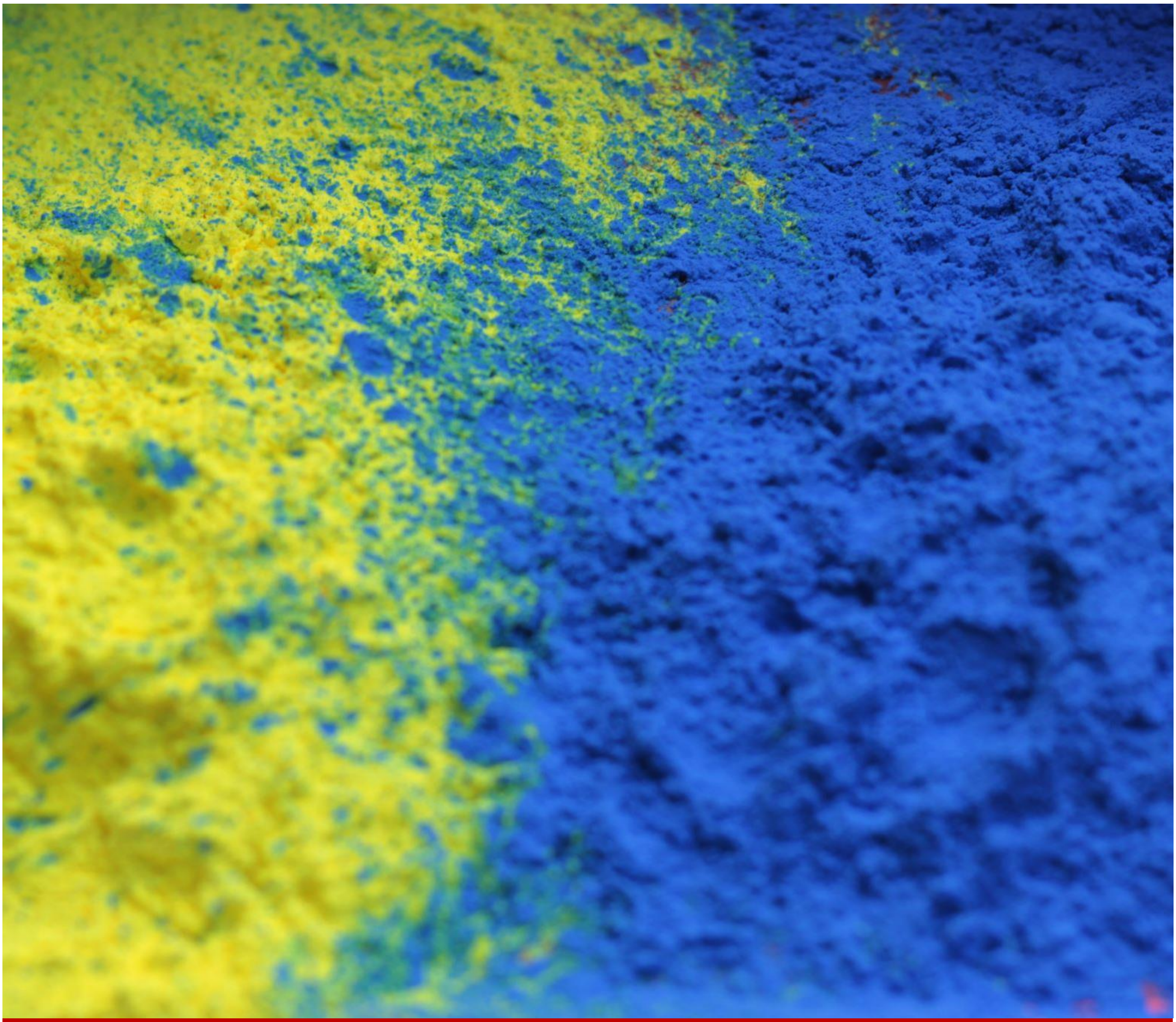
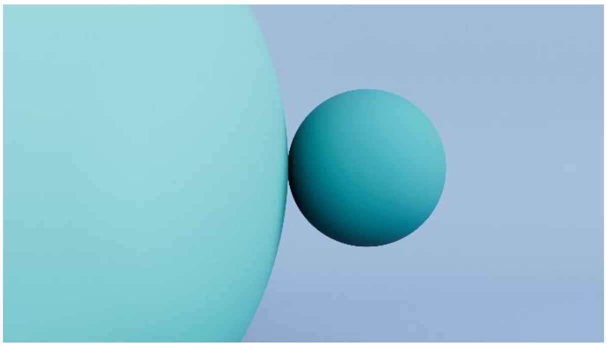


Compliance Pillars of the EU AI Act



The EU AI Rulebook, the AI Act, is due to be finalized by the **end of 2023** and be effective starting 2027. The legislation has extraterritorial effect and violations could be sanctioned with administrative fines of up to 6% of the violator global turnover or 30 million euros whichever is higher.

Although much ink has been spilled over the issue of control of AI tools and dire repercussions thereof, there is little literature analysing the extensive compliance obligations of **safety, transparency, traceability, non-discrimination, and environmental consciousness** imposed by the upcoming EU AI legislation.

In this short paper, we will therefore, focus our attention on the compliance pillars of the EU AI Act. By following the letter of the proposed legislation, we make sense that organisations will have to implement a set of at least twenty compliance mechanisms specifically to address the hazards of **high-risks AI systems**. We will analyse these mechanisms one by one.

1. Risk Management System

Smart companies match their approach to the nature of the threats they face.[1]

An AI risk management system must be established, implemented, documented, and maintained in relation to **high-risk AI systems**.

The risk management system must help with mitigating known and foreseeable risks: **i.e., bias, discrimination, privacy, ethical dilemmas, security, concentration of power, job displacement, etc.** Risks must be identified, analysed, estimated in magnitude, monitored, and appeased. Residual risks must be acceptable and communicated to the user.

Organisations can rely on the **National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF)** in their endeavour to better manage risks to individuals, organizations, and society associated with artificial intelligence. The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. We appreciate that **ISO 31000 Risk Management Guidelines** and **ENISA's Risk Management/Risk Assessment (RM/RA) Framework** can be equally utilised.

2. Data Governance

Besides ensuring data volume and availability, key challenges to successful uptake of AI include ensuring the high quality of input data sets. Poor-quality data, such as incomplete or biased data, can lead to inaccurate, discriminative, or incorrect outcomes, a result that engineers colloquially call "garbage in, garbage out."[2]

[1] Managing Risks: A New Framework, by Robert S. Kaplan and Anette Mikes https://hbr.org/2012/06/managing-risks-a-new-framework

[2] Quality of data sets that feed AI and big data applications for law enforcement, Martyna Kusak

Data governance and management practices must focus on a multitude of areas as listed below with benefits for the quality of the datasets and outputs:

- Relevant design choices.
- Data collection.
- Relevant data preparation processing operations, such annotation, labelling, cleaning, enrichment, and aggregation.
- The formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent.
- A prior assessment of the availability, quantity and suitability of the data sets that are needed.
- Examination in view of possible biases.
- The identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

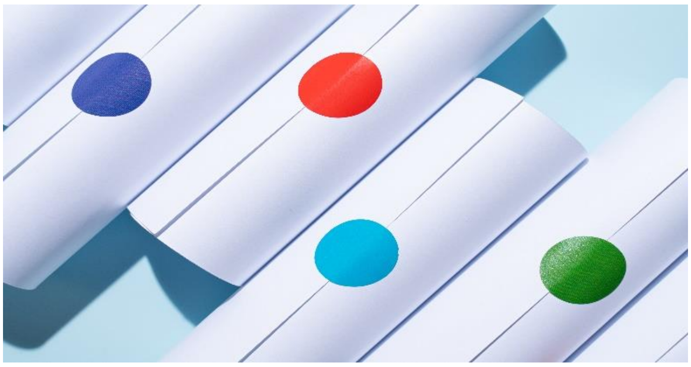
3. Technical Documentation

The technical documentation of a **high-risk AI system** must be drawn up before the system is placed on the market or put into service and must be kept up-to date.

It must contain at least the following information:

- A general description of the AI system; specific elements must be included as they are listed in AI Act.
- A detailed description of the elements of the AI system and of the process for its development; specific elements must be included as they are listed in the AI Act.
- Detailed information about the monitoring, functioning and control of the AI system.
- A detailed description of the risk management system.
- A description of any change made to the system through its lifecycle.
- A list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union
- A copy of the EU declaration of conformity
- A detailed description of the system in place to evaluate the System performance in the post-market phase, including the post-market monitoring plan.

4. Record Keeping



For traceability and auditability reasons **high-risk AI systems** must be designed and developed with capabilities enabling the automatic recording of events (**logs**) while the systems are operating. Logging capabilities must conform to recognised standards or common specifications.

The logging capabilities must ensure a level of traceability of the AI system functioning throughout its lifecycle that is appropriate to the intended purpose of the system.

For **high-risk AI systems**, the logging capabilities must provide, at a minimum:

- Recording of the period of each use of the system (start date and time and end date and time of each use).
- The reference database against which input data has been checked by the system.
- The input data for which the search has led to a match.
- The identification of the natural persons involved in the verification of the results.

5. Transparency and Provisions of Information to Users

Transparency is widely acknowledged as a core value in the governance of Artificial Intelligence technologies.

Transparency has been critical to artificial intelligence debates, not least because artificial intelligence algorithms come with significant transparency challenges. Due to their so-called black-box nature, Al Algorithms raise unprecedented opacity challenges by virtue of their technical complexity (powerful AI algorithms such as neural networks, or deep learning, are highly opaque in their function) in as well as due to the proprietary nature of many AI algorithmic systems deployed both in public and private domains.[3]

According to the AI Act, **high-risk AI systems** must be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct, and clear information that is relevant, accessible, and comprehensible to users. Such information must specify:

- The identity and the contact details of the provider and, where applicable, of its authorised representative.
- The characteristics, capabilities, and limitations of performance of the high-risk AI system, including:
  - intended purpose.
  - the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness, and cybersecurity.
  - risks to the health and safety or fundamental rights
  - its performance as regards the persons or groups of persons on which the system is intended to be used.
  - when appropriate, specifications for the input data,
  - or any other relevant information in terms of the training, validation and testing data sets used, considering the intended purpose of the AI system.
- The changes to the high-risk AI system and its performance which have been pre-determined by the provider during the initial conformity assessment.
- The human oversight measures including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users.
- The expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates.

6. Human Oversight

Humans may be placed "**in**" or "**on**" the loop of an AI system, depending on whether they are involved in every decision the system makes or monitor the system's overall operations. Various rationales for

[3] Reclaiming transparency: contesting the logics of secrecy within the AI Act, Cambridge University Press, Madalina Busuioc, Deirdre Curtin, and Marco Almada

implementing human oversight exist. First, humans supposedly improve the performance and safety of an AI system. Second, human oversight promotes values such as legitimacy, accountability, dignity, as well as human autonomy and agency. The AIA adds a third rationale: its overarching aim is to create European Union citizens' trust in AI.[4]

According to the AI Act human oversight must be ensured through either one or all the following measures:

- Identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service.
- Identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

7. Accuracy, Robustness & Cybersecurity

The levels of **accuracy and the relevant accuracy metrics** of **high-risk AI systems** must be declared in the accompanying instructions of use.

Robustness signifies the ability to withstand or overcome adverse conditions, including digital security risks. AI systems should not pose unreasonable safety risks including to physical security, in conditions of normal or foreseeable use or misuse throughout their lifecycle. Existing laws and regulations in areas such as consumer protection already identify what constitutes unreasonable safety risks. Governments, in consultation with stakeholders, must determine to what extent they apply to AI systems. Issues of robustness, security and safety of AI are interlinked. For example, digital security can affect the safety of connected products such as automobiles and home appliances if risks are not appropriately managed.[5]

Broadly, accuracy in AI (and, more generally, in statistical modelling) refers to how often an AI system guesses the correct answer, measured against correctly labelled test data.[6]

High-risk AI systems must be **resilient** as regards:

- Errors, faults, or inconsistencies that may occur within the system or the environment in which the system operates, due to their interaction with natural persons or other systems.
- Attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions to address AI specific vulnerabilities must include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset (data poisoning), inputs designed to cause the model to make a mistake (adversarial examples), or model flaws.

8. Obligations of Providers of High-Risk AI Systems

Most AI systems are complex socio-technical systems in which control over the system is extensively distributed. In many cases, a multitude of different actors is involved in the purpose setting, data management

[4] Institutionalised Distrust and Human Oversight of Artificial Intelligence Toward a Democratic Design of AI Governance under the European Union AI Act   Dr Johann Laux, Revised Working Paper Oxford Internet Institute August 2023
[5] https://oecd.ai/en/dashboards/ai-principles/P8
[6] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-do-we-need-to-know-about-accuracy-and-statistical-accuracy/

and data preparation, model development, as well as deployment, use, and refinement of such systems. Therefore, determining sensible addressees for the respective obligations is all but trivial. [7]

AI ACT focuses mostly on providers obligations and less on user's obligations. The AI Act defines providers as natural or legal person, public authority, agency, or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge.

According to the AI Act **distributors**, **importers**, **users**, and **third parties** are considered **providers** under the AI Act if:

- They place on the market or put into service a high-risk AI system under their name or trademark.
- They modify the intended purpose of a high-risk AI system already placed on the market or put into service.
- They make a substantial modification to the high-risk AI system.

According to the AI Act providers of AI systems must ensure that their **high-risk AI systems** are compliant with legal requirements, respectively:

- Have a **quality management system** in place.
- Draw-up the **technical documentation** of the high-risk AI system.
- When under their control, keep the **logs** automatically generated by their high-risk AI systems.
- Ensure that the high-risk AI system undergoes the relevant **conformity assessment procedure**, prior to its placing on the market putting into service.
- Comply with the **registration** obligations.
- Take the necessary **corrective actions** if the high-risk AI system is not in conformity with requirements.
- **Inform** the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken.
- **Affix the CE marking** to their high-risk AI systems to indicate the conformity with this Regulation.
- Upon request of a national competent authority, **demonstrate** the conformity of the high-risk AI system.

Let's turn our attention to the Quality Management System. That system must be documented in a systematic and orderly manner in the form of written **policies**, **procedures**, and **instructions**, and must include:

- A strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system.
- Techniques, procedures, and systematic actions to be used for the design, design control and design verification of the high-risk AI system.
- Techniques, procedures, and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system.
- Examination, test, and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they must be carried out.
- Technical specifications, including standards, to be applied.

[7] Assigning Obligations in AI Regulation: A Discussion of Two Frameworks Proposed By the European Commission, Mattis Jacobs & Judith Simon

- Systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems.
- The risk management system referred to in the law.
- The setting-up, implementation and maintenance of a post-market monitoring system.
- Procedures related to the reporting of serious incidents and of malfunctioning.
- The handling of communication with national competent authorities, competent authorities, including sectoral ones, providing, or supporting the access to data, notified bodies, other operators, customers, or other interested parties.
- Systems and procedures for record keeping of all relevant documentation and information.
- Resource management, including security of supply related measures.
- An accountability framework setting out the responsibilities of the management and other staff.

9. Obligations of Product Manufacturers

According to the AI Act where a **high-risk AI system** is placed on the market or put into service together with the product manufactured under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system have the same obligations imposed on the provider.

10. Authorised Representative

Prior to making their systems available on the Union market, where an importer cannot be identified, providers established outside the Union must, by written mandate, appoint an **authorised representative** which is established in the Union.

The authorised representative must perform the tasks specified in the mandate received from the provider. The mandate shall empower the authorised representative to carry out the following tasks:

- Keep a copy of the EU declaration of conformity and the technical documentation at the disposal of the national competent authorities and national authorities.
- Provide a national competent authority, upon a reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system including access to the logs automatically generated by the high-risk AI system.
- To the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law.
- Cooperate with competent national authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.

11. Obligations of Importers

Obligations also fall on importers and distributors in a way similar to the product safety regime, with the intent of stopping dangerous products built outside the EU from entering it. The primary actor on whom obligations are placed is nonetheless the provider.[8]

Before placing a **high-risk AI system** on the market, importers of such system must ensure that:

- The appropriate conformity assessment procedure has been carried out by the provider of that AI system.
- The provider has drawn up the technical documentation.
- The system bears the required conformity marking and is accompanied by the required documentation and instructions of use.

Where an importer considers or has reason to consider that a high-risk AI system is not in conformity it must not place that system on the market until that AI system has been brought into conformity. Where the high-risk AI system presents a risk, the importer must inform the provider of the AI system and the market surveillance authorities to that effect.

Importers must indicate their name, registered trade name or registered trademark, and the address at which they can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation.

Importers must ensure that, while a high-risk AI system is under their responsibility, storage or transport conditions do not jeopardise its compliance with the legal requirements.

Importers must provide national competent authorities, upon a reasoned request, with all necessary information and documentation to demonstrate the conformity of a high-risk AI system   in a language which can be easily understood by that national competent authority, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law. They must also cooperate with those authorities on any action national competent authority takes in relation to that system.

12. Obligations of Distributors

Similar in nature with the obligations of the importers. The distributor must verify that the **high-risk AI system** bears the required CE conformity marking, that it is accompanied by the required documentation and instruction of use, and that the provider and the importer of the system, as applicable, have complied with the obligations set out in the Regulation.

13. Obligations of Users

Users must monitor the operation of the **high-risk AI system** based on the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk, they must inform the provider or distributor and suspend the use of the system. They also must keep the logs of the AI systems, in an automatic and documented manner and inform the provider or distributor when they have identified any serious incident or any malfunctioning and interrupt the use of the AI system.

Users of high-risk AI systems shall carry out a data protection impact assessment under Article 35 of the GDPR.

[8] The EU AI Act: a summary of its significance and scope, Lilian Edwards Professor of Law, Innovation and Society, Newcastle University

14. Registration

Before placing on the market or putting into service a **high-risk AI system** the provider or, where applicable, the authorised representative must register that system in the EU database.

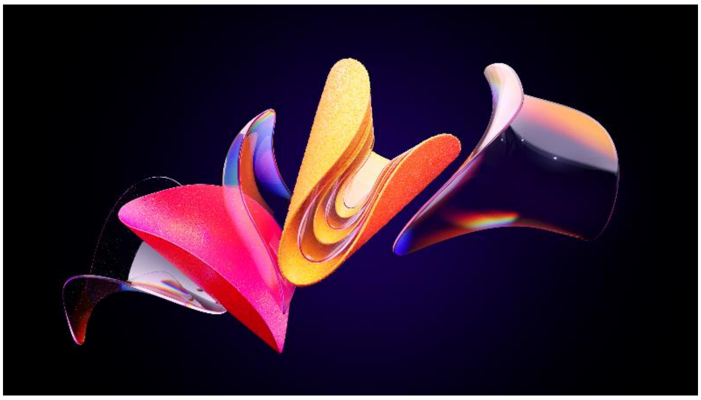
15. AI Regulatory Sandboxes

AI regulatory sandboxes established by one or more Member States competent authorities, or the European Data Protection Supervisor shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan. In the AI regulatory sandbox personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the specific conditions.

16. Governance

The European Artificial Intelligence Board is created. At the same time, national competent authorities must be established or designated by each Member State for the purpose of ensuring the application and implementation of AI Act

17. EU database for stand-alone high-risk AI systems



The draft AI Act sets out to establish and maintain a EU database for stand-alone high-risk AI systems. This database offers a chance for increased public transparency on AI systems vis-à-vis impacted individuals and civil society and could greatly facilitate public interest research. Given that the AI Act largely depends on self-assessment procedures by providers and users of AI systems, the EU database offers a way of enhancing accountability through public scrutiny. Thus, it could ensure effective public transparency on AI systems and therefore provide a necessary first step on the path towards a responsible use of AI systems that is in line with fundamental rights. [9]

The Commission must, in collaboration with the Member States, setup and maintain a EU database containing information concerning registered high-risk AI systems. The data must be entered into the EU database by the providers. The Commission must provide them with technical and administrative support. Information contained in the EU database must be accessible to the public.

18. Post Market Monitoring

[9] Algorithm Watch, EU Artificial Intelligence Act, Recommendations on Public Transparency, Ensure Consistent and Meaningful Public Transparency, April 2022 https://algorithmwatch.org/en/wp-content/uploads/2022/04/Database-issue-paperApril2022.pdf

The post-market monitoring system shall actively and systematically collect, document, and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the legal requirements.

The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation. The Commission must adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

19. Reporting of serious incidents and of malfunctioning

Providers of **high-risk AI systems** placed on the Union market must report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred. Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.

20. Enforcement

Depending on the type of infringement companies may be sanctioned with administrative fines ranging between 2%-6% of the total worldwide annual turnover for the preceding financial year.

EU Digital Partners, Regulatory Compliance Services
Contact Us
+40 747489033
https://eudigitalpartners.com/
pp@eudigitalpartners.com

Contact Point:
Petruta Pirvan, Founder and Legal Counsel Data Privacy and Digital Law
pp@eudigitalpartners.com
+40747 489 033