14

Guide 14. Serious incident reporting

European
Artificial Intelligence Act

Companies developing compliance with requirements

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

This guide has been developed within the framework of the development of the Spanish pilot for the regulatory AI Sandbox, through collaboration among participants, technical assistance providers, potential competent national authorities, and the sandbox's expert advisory group.

The aim of the guide **is to serve as an introductory support to the European Regulation on Artificial Intelligence and its applicable obligations.** Although it is not legally binding and does not replace or develop the applicable legislation, it provides practical recommendations aligned with regulatory requirements, pending the approval of the harmonised implementing standards for all Member States.

This document **is subject to an ongoing process of evaluation and review, with periodic updates** in line with the development of standards and the various guidelines published by the European Commission, and it will be updated once the Digital Omnibus amending the Artificial Intelligence Act is approved.

Revision date: 10 December 2025

General content

Detailed Index

1. Preamble

1.1 Purpose of the document

The **version** of the AI Act taken as a reference in this document has been the one published by the Council of the European Commission on 13 June 2024.

Article 73 *of the European Artificial Intelligence Act (*AI Act) is dedicated to the notification of serious incidents involving high-risk AI systems. This article is part of **Chapter IX** (Post-market control, exchange of information and market surveillance) **section two** *(Sharing of information on serious incidents*) of the mentioned Act.

This document describes the procedure for reporting such serious incidents, as well as the measures to address that procedure.

1.2 How to read this guide?

As mentioned, **this document provides implementation measures** for providers and deployers of AI systems **that facilitate compliance with** the obligations expressed in Article 73 of the AI Act, dedicated to the Notification of Serious Incidents.

To this end, the document **goes through** all the sections of said article in order, answering the fundamental questions necessary to **facilitate the fulfilment** of the obligations expressed in these sections.

1.3 Who is it for?

This document is **addressed to the provider entity**, as the AI Act in Article 73 referred to in this document (Notification of serious incidents) states that it shall be the providers of high-risk AI systems placed on the Union market who shall notify any serious incident occurred in said AI system.

But **it is also aimed at the deployer**, since, in the event that the deployer is unable to contact the provider, they will be responsible for said notification. This is specified in Article 26-Section 5 of the AI Act (Obligations of the deployers of high-risk AI systems), indicating that "*In the event that the deployer is unable to contact the provider, Article 73 will apply mutatis mutandis*", i.e. changing what needs to be changed.

1.4 Use Cases used in the guide

To contextualize, where they apply, the measures exposed that allow the requirements of the AI Act to be met, examples will be used on two use cases:

- **Granting financial aid to families without resources**
- **Chronic disease management - Smart insulin pump**

These use cases are developed in detail in the **Guide 2. Practical guide and examples to understand the AI Act.**

The examples of these use cases are presented at a high level, without going into detail or being exhaustive, to try to cover as many cases as possible. In addition, they do not respond to real experiences (but with the intention of being realistic from a didactic point of view), with only the aim of clarifying the measures a little more, therefore they cannot be taken as specifications in a real implementation.

2. Introduction

2.1 What are serious incidents?

To begin with, it is important **to establish the concept of "serious incident"** referred to in article 73. This concept is detailed in Article 3 (paragraph 49) of the AI Act:

'serious incident' means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

(a) the death of a person, or serious harm to a person's health

(b) a serious and irreversible disruption of the management or operation of critical infrastructure

(c) the infringement of obligations under Union law intended to protect fundamental rights

(d) serious harm to property or the environment

It must also be understood that it is a continuous process over time which can be visualized as:

And that will be studied with a greater breakdown in detail throughout the guide.

3. European Regulation on Artificial Intelligence

The putting into service or use of high-risk AI systems should be subject to compliance with certain mandatory requirements, including the reporting of serious incidents. Those requirements aim to ensure that high-risk AI systems available in the Union or whose output outputs are used in the Union do not pose unacceptable risks to important public interests recognised and protected by Union law.

This section includes the articles referring to the management of serious incidents of Regulation 2024/1689 of the European Parliament and of the Council, June 13th, 2024 (European Regulation on Artificial Intelligence) and details in which sections of this guide the different elements of these articles are addressed.

3.1 Previous analysis and relationship of the articles

The obligations on the reporting of serious incidents are mainly found in Article 73 of the European AI Act, "Reporting of serious incidents".

Reporting of serious incidents article establishes the need for the notification of serious incidents to the market surveillance authorities and throughout its sections, defines different scenarios depending on the type of AI system, in addition to the actors involved and actions.

Below is the most up-to-date version of the article "*Reporting of serious incidents*" corresponding to the general position of the Council of the European Union, published on June 13th 2024, of the European AI Act. This section also details in which sections of this guide the different elements of this article are addressed.

3.2 Content of the articles in the AI Act

AI Act

Art.73 - Notification of serious incidents

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred.

2. The report referred to in paragraph 1 shall be made immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the provider or, where applicable, the deployer, becomes aware of the serious incident.

The period for the reporting referred to in the first subparagraph shall take account of the severity of the serious incident.

3. Notwithstanding paragraph 2 of this Article, in the event of a widespread infringement or a serious incident as defined in Article 3, point (49)(b), the report referred to in paragraph 1 of this Article shall be provided immediately, and not later than two days after the provider or, where applicable, the deployer becomes aware of that incident.

4. Notwithstanding paragraph 2, in the event of the death of a person, the report shall be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident, but not later than 10 days after the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

5. Where necessary to ensure timely reporting, the provider or, where applicable, the deployer, may submit an initial report that is incomplete, followed by a complete report.

6. Following the reporting of a serious incident pursuant to paragraph 1, the provider shall, without delay, perform the necessary investigations in relation to the serious incident and the AI system concerned. This shall include a risk assessment of the incident, and corrective action.

The provider shall cooperate with the competent authorities, and where relevant with the notified body concerned, during the investigations referred to in the first subparagraph, and shall not perform any investigation which involves altering the AI system concerned in a way which may affect any subsequent evaluation of the causes of the incident, prior to informing the competent authorities of such action.

7. Upon receiving a notification related to a serious incident referred to in Article 3, point (49)(c), the relevant market surveillance authority shall inform the national public authorities or bodies referred to in Article 77(1). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1 of this Article. That guidance shall be issued by 2 August 2025, and shall be assessed regularly.

8. The market surveillance authority shall take appropriate measures, as provided for in Article 19 of Regulation (EU) 2019/1020, within seven days from the date it received the notification referred to in paragraph 1 of this Article, and shall follow the notification procedures as provided in that Regulation.

9. For high-risk AI systems referred to in Annex III that are placed on the market or put into service by providers that are subject to Union legislative instruments laying down reporting obligations equivalent to those set out in this Regulation, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c).

10. For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulations (EU) 2017/745 and (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c) of this Regulation, and shall be made to the national competent authority chosen for that purpose by the Member States where the incident occurred.

11. National competent authorities shall immediately notify the Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of Regulation (EU) 2019/1020.

3.3 Correspondence of the articles with the sections of the guide

The following table lists the sections of the document in which the explanations and measures applicable to each section of the article dedicated to human surveillance are found.

Article	AI Act Requirement	Guide Section
73.1 73.2 73.3 73.4 73.5 73.6 73.9 73.10	Requirements regarding serious incidents by providers.	Section 4.1.1
73.7 73.8 73.11	Requirements for serious incidents by market surveillance authorities and national competent authorities.	Section 4.1.2

4. How to approach the requirements?

The article on Reporting serious incidents has **eleven sections** that describe the **procedure** to follow when a serious incident has occurred and a causal link has been established between the AI system and the serious incident, or simply the reasonable possibility that such a link exists.

This procedure defines **different scenarios** depending on the type of AI system, in addition to the **actors** involved and **actions** to be carried out, indicating that the European Commission **will develop specific guidelines for those actions** within a maximum period of twelve months after the entry into force of this Act.

The article is then set out in an orderly, easily understandable manner, integrating in said exposition the references made to other articles, and the necessary measures to address the requirements set out by the AI Act are set out.

4.1 Requirements on Reporting of serious incidents in the Regulations

4.1.1 What the provider should do. Paragraphs 1 to 6 (inclusive), 9 and 10.

AI Act

Art.73. Notification of serious incidents

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred.

2. The report referred to in paragraph 1 shall be made immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the provider or, where applicable, the deployer, becomes aware of the serious incident.

The period for the reporting referred to in the first subparagraph shall take account of the severity of the serious incident.

3. Notwithstanding paragraph 2 of this Article, in the event of a widespread infringement or a serious incident as defined in Article 3, point (49)(b), the report referred to in paragraph 1 of this Article shall be provided immediately, and not later than two days after the provider or, where applicable, the deployer becomes aware of that incident.

4. Notwithstanding paragraph 2, in the event of the death of a person, the report shall be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident, but not later than 10 days after the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

5. Where necessary to ensure timely reporting, the provider or, where applicable, the deployer, may submit an initial report that is incomplete, followed by a complete report.

6. Following the reporting of a serious incident pursuant to paragraph 1, the provider shall, without delay, perform the necessary investigations in relation to the serious incident and the AI system concerned. This shall include a risk assessment of the incident, and corrective action.

The provider shall cooperate with the competent authorities, and where relevant with the notified body concerned, during the investigations referred to in the first subparagraph, and shall not perform any investigation which involves altering the AI system concerned in a way which may affect any subsequent evaluation of the causes of the incident, prior to informing the competent authorities of such action.

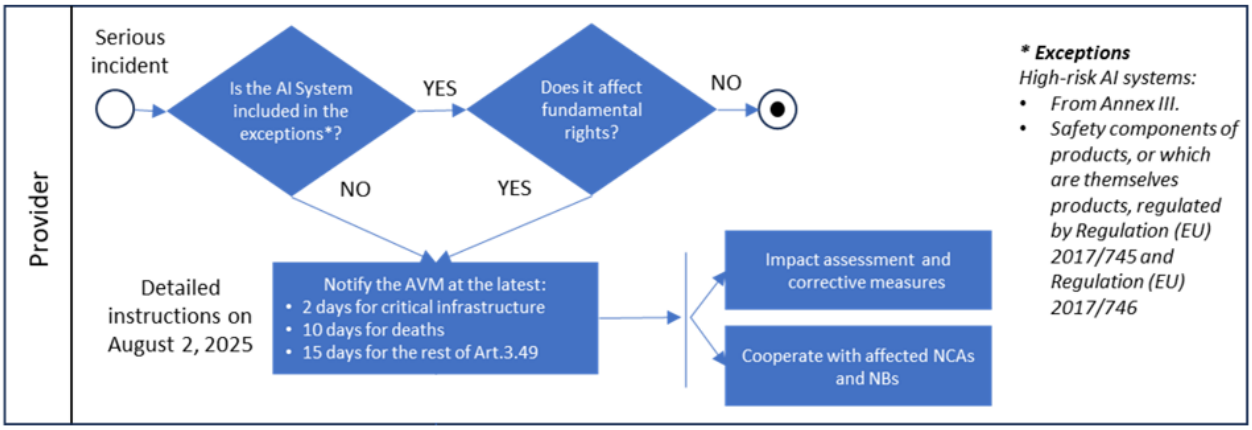
….

9. For high-risk AI systems referred to in Annex III that are placed on the market or put into service by providers that are subject to Union legislative instruments laying down reporting obligations equivalent to those set out in this Regulation, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c).

10. For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulations (EU) 2017/745 and (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c) of this Regulation, and shall be made to the national competent authority chosen for that purpose by the Member States where the incident occurred.

What we understand

The procedure is detailed below in a visual way to facilitate its understanding



The first thing to consider is whether the system falls under any of the following exceptions that apply to categories of high-risk systems:

- Annex III systems placed on the market or put into service by providers subjects to Union legislative instruments.

- Medical devices (*Regulation (EU) 2017/745*)
- In vitro diagnostic medical devices (*Regulation (EU) 2017/746)*

In such cases, the notification of serious incidents **shall be limited to** the incidents referred to in Article 3(49)(c), which are those which lead to a breach of obligations under Union law to protect **fundamental rights**.

As for notification, it is the provider who must notify the incident. If the incident is detected by the deployer, and if they are unable to contact the provider, this Article shall apply *mutatis mutandis,* i.e. changing what should have been changed, as indicated in Article 26 of the AI Act in paragraph 5.

In accordance with paragraph 7 of Article 73, in order to make such a notification, the Commission **shall draw up specific guidance** which shall be published by 2 August 2025 at the latest.

The provider (or the deployer as indicated above) **must make the notification in a maximum of:**

- 2 days for critical infrastructures
- 10 days for deaths
- 15 days for the rest of the serious incidents indicated in Art.3.49

On the other hand, it should be noted that this measure applies to any provider regardless of its origin, as long as the AI system operates in the European Union market.

In addition, it should be noted that the AI system may be operational in several Member States, and the notification must be made **to all** market surveillance authorities in the Member States where the incident occurred.

Measures to carry it out

- Knowledge of AI system categorization
- Knowledge of fundamental rights
- Frame the reporting of serious incidents in the QMS
- Contact the Market Surveillance Authority
- Contact the provider

4.1.2 What MSAs should do. Paragraphs 7, 8 and 11

AI Act

Art.73 - Notification of serious incidents

7. Upon receiving a notification related to a serious incident referred to in Article 3, point (49)(c), the relevant market surveillance authority shall inform the national public authorities or bodies referred to in Article 77(1). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1 of this Article. That guidance shall be issued by 2 August 2025, and shall be assessed regularly.

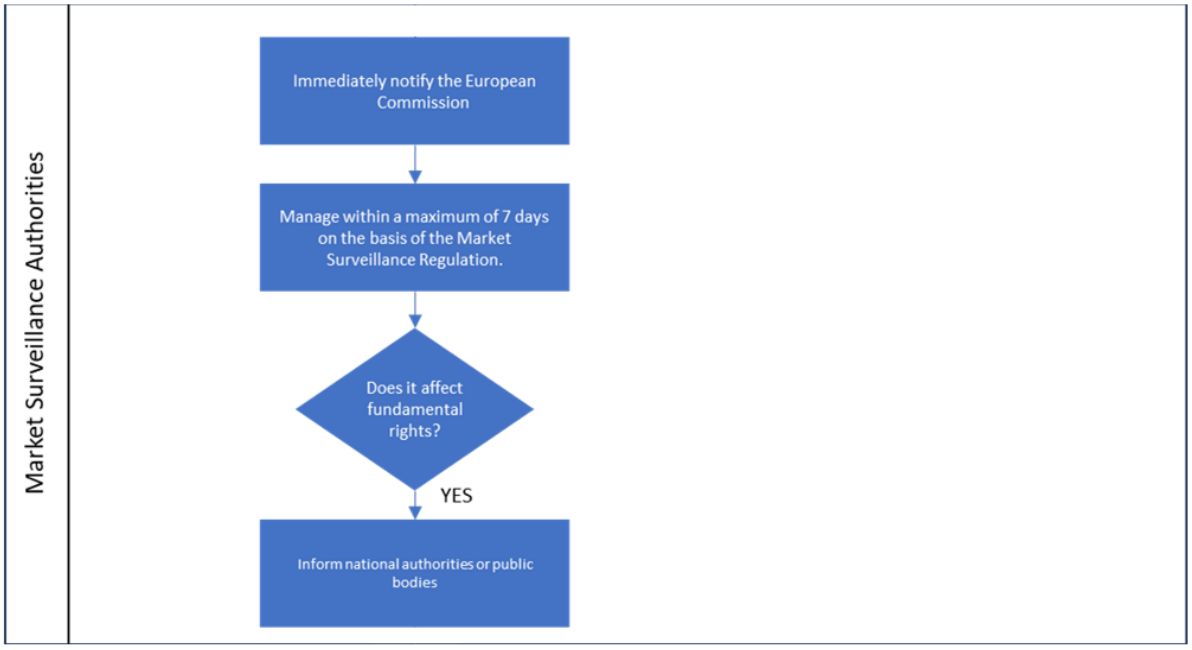
8. The market surveillance authority shall take appropriate measures, as provided for in Article 19 of Regulation (EU) 2019/1020, within seven days from the date it received the notification referred to in paragraph 1 of this Article, and shall follow the notification procedures as provided in that Regulation.

…

11. National competent authorities shall immediately notify the Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of Regulation (EU) 2019/1020.

What we understand

The procedure is detailed below in a visual way to facilitate its understanding



Upon receipt of the notification from the provider, the MSA shall immediately notify **the Commission**, whether or not it has taken action, in accordance with Article 20 of Regulation (EU) 2019/1020 (Market Surveillance Regulation, MSR).

The MSA will then have **7 days to take appropriate action** in accordance with Article 19 of the Market Surveillance Regulation.

If the serious incident involves a breach of the obligations under Union law to protect **fundamental rights** (which are those referred to in Article 3(49)(c)), the market surveillance authority shall inform the **national public authorities or bodies.**

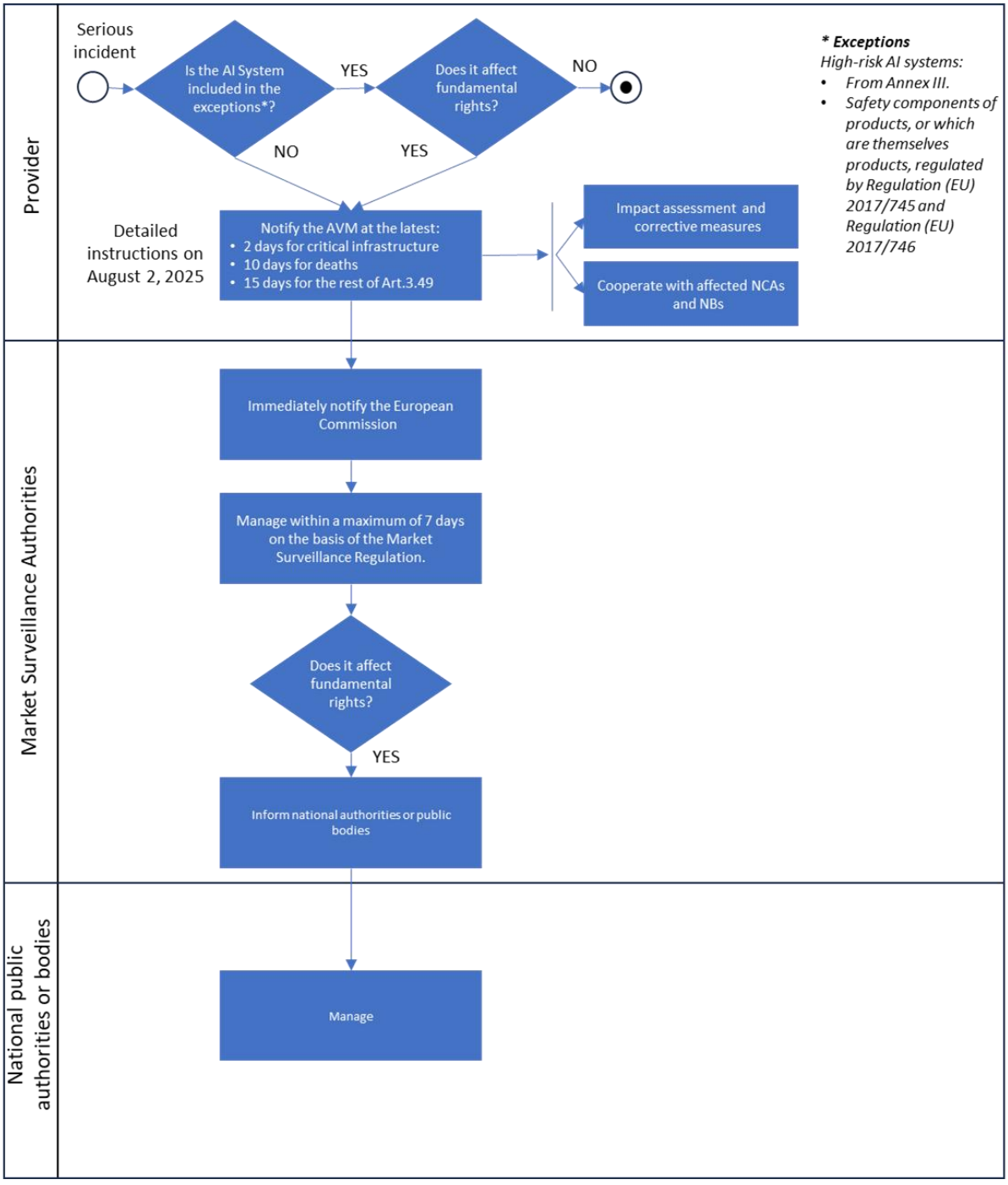
Those national public authorities or bodies are responsible for monitoring or enforcing the obligations under Union law on the protection of fundamental rights, in particular the right to non-discrimination, with regard to the use of high-risk AI systems.

Measures to carry it out

This document defines measures to facilitate compliance by deployers and providers with the requirements established by the AI Act. The activity of the incident notification procedure defined in this section corresponds to the Market Surveillance Authority, and therefore the definition of any measure for that Authority does not apply in this document.

4.1.3 Visual Summary of the Procedure

Given that the procedure is detailed in an extensive way, and that the order in its explanation is different from the one that occurs chronologically, the procedures of each of the actors are detailed in a visual way below to facilitate their understanding.



4.2 Applicable measures for the management of serious incidents

This chapter of the document includes the details of the measures necessary to cover the requirements for the Notification of Serious incidents set out in Article 73 of the AI Act, previously explained.

4.2.1 Framing serious incidents management in the QMS

AI Act

Art.17.1i – Quality management system

Procedures related to the reporting of a serious incident in accordance with Article 73.

Who it applies to

To the provider, since said QMS is the responsibility of the latter.

Without forgetting that, if the incident is detected by the deployer, and if he or she is unable to contact the provider, incident reporting must be applied *mutatis mutandis,* i.e. changing what should be changed. Therefore, the deployer must also include this procedure in their own QMS or in their governance model on the AI system.

Example

This is a global measure, not exemplified by a use case.

To which sections does this measure apply?

- What the provider should do.

4.2.2 Contact the Market Surveillance Authority

It is essential to have contact with the Market Surveillance Authority, as the incident must be notified to that authority.

Who does it apply to?

- To the provider, as it is responsible for the notification.
- To the deployer, given that the notification must be made *mutatis mutandis*, as indicated in Article 26 of the AI Act (Obligations of deployers deploying high-risk AI systems) and, in the case of not being able to contact the provider, it must be the deployer who does it.

Example

This is a global measure, not exemplified by a use case.

To which sections does this measure apply?

- What the provider should do.

4.2.3 Contact with the provider

If the incident is detected by the deployer, they must contact the provider. To do so, they must contact them through the channel provided to do so, as described in Article 13 of the AI Act dedicated to Transparency.

AI Act

Art.13.3.a – Transparency and communication of information to those responsible for deployment

The identity and the contact details of the provider and, where applicable, of its authorised representative;

Who does it apply to?

- The provider shall provide such contact and the channel through which it will occur.
- The deployer must also identify the persons responsible within their organization in charge of activating such contact with the provider in the event of serious incidents.

Example – Aid Grant

The deployers detect through an alarm provided by the system that the amount proposed for the aid of a family is not homogeneous with respect to others provided in the past to families with similar characteristics, or that requests from a segment of families are not being considered because the AI system is discriminating on the basis of some criterion (e.g. single-parent families of any kind). These deployers activate contact with the provider by opening a request in the demand management system.

Example – Insulin Pump

A medical manager of the entity responsible for deploying detects through an alarm provided by the system that the next dose prescribed to a patient is not the usual one despite having similar parameters in blood. The medical manager activates contact with the provider by opening a request in the demand management system.

To which sections does this measure apply?

- What the provider should do.

4.2.4 Knowledge of AI system categorization

The first step is to identify whether the AI system belongs to any of the categories indicated as exceptions, since if it belongs to any of them and the system does not affect fundamental rights, notification to the Market Surveillance Authority will not be necessary. Therefore, it is essential to know the categorizations and include the AI system in one of them.

Who does it apply to?

- To the provider, as it is responsible for the notification.
- To the deployer, given that the notification must be made *mutatis mutandis*, as indicated in Article 26 of the AI Act (Obligations of deployers of high-risk AI systems) and, in case of not being able to contact the provider, it must be the deployer that does it.

Example – Grant

This is an AI system framed in Annex III-Point 5. (Access to and enjoyment of essential public and private services and their benefits). Therefore, it belongs to the group of systems in which notification to the Market Surveillance Authority will be necessary only when it affects EU fundamental rights.

Example – Insulin Pump

This is an AI system framed in Annex II-Section A.-Subsection 11 (Medical devices). Therefore, it is not among the exceptions and any incident must be reported to the Market Surveillance Authority, as it can also affect the patient's life (a fundamental right).

To which sections does this measure apply?

- What the provider should do.

4.2.5 Knowledge of fundamental rights

The first step of the procedure is to identify whether the system belongs to any of the categories indicated as exceptions. If you belong to any of them, if the system affects fundamental rights, it will be necessary to notify the Market Surveillance Authority.

Therefore, it is essential to know these **fundamental rights** in order to know how to proceed.

Who does it apply to?

- To the provider, as it is responsible for the notification.
- To the deployer, given that the notification must be made *mutatis mutandis*, as indicated in Article 26 of the AI Act (Obligations of deployers of high-risk AI systems) and, in case of not being able to contact the provider, it must be the deployer who does it.

Example – Aid Grant

This is an AI system framed in Annex III-Point 5. (Access to and enjoyment of essential public and private services and their benefits). It therefore belongs to the group of systems in which notification to the Market Surveillance Authority will be necessary only when it affects EU fundamental rights.

In the event that it is detected that the AI system is making any discrimination in the granting of aid (for example, by sex, race, colour, ethnic or social origins, genetic characteristics, language, religion or beliefs, political or any other opinion, membership of a national minority, heritage, birth, disability, age or sexual orientation, etc.), it would be affecting the fundamental right to EQUALITY (Section III of fundamental rights), and it would be necessary to notify the incident.

Example – Insulin Pump

As indicated in the previous measure, this is an AI system framed in Annex II-Section A.-Subsection 11 (Medical devices). Therefore, it is not among the exceptions and any incident must be reported to the Market Surveillance Authority, since any incident will potentially affect fundamental rights (in this case life).

To which sections does this measure apply?

- What the provider should do.

5. Technical documentation

Article 11 (Technical Documentation) states that the system must be documented in such a way as to demonstrate that it meets the requirements set out in Section 2 (to which this article on transparency corresponds), providing the competent national authorities and notified bodies with the information necessary to assess the conformity of the AI system with those requirements in a clear and comprehensive manner.

The aforementioned article states that such documentation shall contain, as a minimum, the elements set out in Annex IV. [1]

Furthermore, this transparency guide sets out measures to meet the requirements set out in the **European AI Act** in the article dedicated to transparency in AI systems. **As a result of these measures, aspects of the system set out below can be documented**, which may help to generate the minimum documentation required.

Framing serious incidents management in the QMS

1. Provider. Within your QMS, procedures associated with the notification of a serious incident.
2. Deployer. Within your QMS, procedures associated with the notification of a serious incident.

Contact the Market Surveillance Authority

3. Provider. Document with the responsible contact of the Market Surveillance Authority.
4. Deployer. Document with the responsible contact of the Market Surveillance Authority.

Contact with the provider

5. Provider. Preparation of the channel's user manual, which allows the management of requests and incidents between the deployer and the provider.
6. Deployer. Access to the channel's user manual that allows the management of requests and incidents between the deployer and the provider.

Knowledge of AI system categorization

7. Provider. Preparation of the document explaining the category of the AI system according to those defined in the AI Act.
8. Deployer. Access to the document explaining the category of the AI system according to those defined in the AI Act.

Knowledge of fundamental rights

9. Provider. Document certifying knowledge of the fundamental rights of the European Union.
10. Deployer. Document certifying knowledge of the fundamental rights of the European Union.

[1] SMEs, including start-ups, may provide the technical documentation specified in Annex IV in a simplified manner. To this end, the Commission shall establish a simplified technical documentation form tailored to the needs of small and micro-enterprises. Where an SME, including start-ups, chooses to provide the information required in Annex IV in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept that form for the purposes of conformity assessment.

6. Self-assessment questionnaire

To carry out a self-assessment of compliance with the requirements of the Artificial Intelligence Act referred to in this guide, a global self-assessment questionnaire has been generated with a series of questions with the key points to be taken into account with respect to the obligations dictated by the articles of the AI Act mentioned in this guide.

It will be necessary to refer to this document in order to carry out the section of the self-assessment questionnaire corresponding to this guide.

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de
Recuperación,
Transformación
y Resiliencia

España | digital 2026