DRAFT GUIDANCE ARTICLE 73 AI ACT- INCIDENT REPORTING (HIGH-RISK AI SYSTEMS)

1. BACKGROUND AND OBJECTIVES

(1) The obligation to report serious incidents is laid down in Article 73 of Regulation (EU) 2024/1689 ("AI Act")[1]. It establishes reporting obligations for providers of high-risk AI systems[2].

(2) The objectives of the obligation to report serious incidents are multifaceted. First, the reporting obligation aims to create an early warning system that allows market surveillance authorities to identify potentially harmful patterns or important risks of high-risk AI systems at an early stage. Second, it establishes clear accountability for providers, and to a certain extent as well users, of these systems, ensuring they take responsibility for the proper functioning and safety of their products. Third, it enables market surveillance authorities to take timely corrective measures when incidents occur. Finally, it fosters transparency in how high-risk AI systems operate, ultimately building public trust in AI technologies through proper oversight.

(3) Besides the reporting obligation of the AI Act other international reporting regimes have emerged, most notably the AI Incidents Monitor and Common Reporting Framework of the Organisation for Economic Co-operation and Development (OECD)[3]. The AI Act incident monitoring seeks to align with the OECD framework wherever possible.

(4) The reporting obligation of Article 73 AI Act applies to serious incidents and widespread infringements of high-risk AI systems. Article 55 (1)(c) AI Act also lays down an obligation for providers of general-purpose AI models with systemic risk to report serious incidents to the AI Office. This guidance is not dealing with the obligation to report such serious incidents of general-purpose AI models with systemic risk.

2. DEFINITIONS

2.1. Definitions AI Act

(5) The AI Act defines a serious incident in Article 3(49) AI Act as "an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

---

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

[2] Article 6 (1) and (2) AI Act and Annex I and III.

[3] AI incidents Overview - OECD.AI

(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;"

(6) Widespread infringement is defined in Article 3(61) AI Act as "any act or omission contrary to Union law protecting the interest of individuals, which:

(a) has harmed or is likely to harm the collective interests of individuals residing in at least two Member States other than the Member State in which:

i. the act or omission originated or took place;

ii. the provider concerned, or, where applicable, its authorised representative is located or established; or

iii. the deployer is established, when the infringement is committed by the deployer;

(b) has caused, causes or is likely to cause harm to the collective interests of individuals and has common features, including the same unlawful practice or the same interest being infringed, and is occurring concurrently, committed by the same operator, in at least three Member States;"

2.2. Incident and malfunction

(7) The AI Act defines "serious incident" in Article 3(49) AI Act, the term "incident" however is not defined. The AI Act does not include reporting obligations for "incidents".

(8) The term incident appears across multiple European regulatory frameworks, each tailored at specific sectorial needs. While these sectorial definitions do not apply to the AI Act, several common elements emerge. Incidents are generally defined by their actual or potential negative consequences, particularly (potential) harm to humans or critical systems, additionally considering sectorial specificities.[4] An incident is a not planned/programmed deviation in the characteristics of performance. OECD defines an AI

[4] As an example, Article 2 (64) of Regulation (EU) 2017/745 (Medical Device regulation "MDR") defines an incident as "any malfunction or deterioration in the characteristics or performance of a device made available on the market, including use-error due to ergonomic features, as well as any inadequacy in the information supplied by the manufacturer and any undesirable side-effect". Article 6 (6) of Directive (EU) 2022/2555 ("NIS 2") defines an Incident as "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems". Besides the term incident European regulatory frameworks use the term event. NIS 2 for example defines the incident as an "Event compromising […]". The usage of the two terms seems to differ with the event describing the pure occurrence while the term incident describes the concrete result or manifestation of an event or an occurrence.

incident as an event where the development or use of an AI system results in *actual* harm[5], while an event where the development or use of an AI system is *potentially* harmful is termed an "AI hazard".

(9) The wording of Article 3(49) AI Act "refers to an incident or malfunctioning" and implies that a malfunction is not considered to be an incident. Unlike the AI Act, the Medical Device Regulation "MDR"[6] also includes the term malfunction in the definition of the term incident.

(10) A malfunction can be understood as any function of the AI system not performing as intended or a situation where an AI system fails to uphold the performance stated by the provider in the technical documentation (Article 11 AI Act), for its intended purpose and reasonably foreseeable misuse.

(11) In practice, the distinction between "incident" and "malfunction" in the AI Act should not be understood as a strict distinction, but rather as an emphasis on the importance of malfunctions in the context of incident monitoring.

(12) Examples of incidents or malfunctions include:

- Misclassifications
- Significant drops in accuracy
- Temporary system downtime
- Unexpected system behaviour

2.3. 'Directly or indirectly' caused

(13) The incident or malfunction needs to be causal, or likely to be causal, for the serious harms specified in Article 3(49) AI Act (Article 73(2) AI Act). The incident or malfunction is causal if, without it, the harm in its concrete form would not have occurred (or reasonably likely respectively more probable not to have occurred). The causation can also be indirect, i.e. secondary effects. Indirect examples include:

---

[5] OECD paper Defining AI incidents and related terms, An AI incident is an event, circumstance or series of events where the development, use or malfunction of one or more AI systems directly or indirectly leads to any of the following harms: (a) injury or harm to the health of a person or groups of people; (b) disruption of the management and operation of critical infrastructure; (c) violations of human rights or a breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights; (d) harm to property, communities or the environment.
A serious AI incident is an event, circumstance or series of events where the development, use or malfunction of one or more AI systems directly or indirectly leads to any of the following harms: (a) the death of a person or serious harm to the health of a person or groups of people; (b) a serious and irreversible disruption of the management and operation of critical infrastructure; (c) a serious violation of human rights or a serious breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights; (d) serious harm to property, communities or the environment.

[6] Regulation (EU) 2017/745 (Medical Device regulation "MDR")

- An AI system provides an incorrect analysis of medical imaging, leading a physician to make an incorrect diagnosis or treatment decision, which subsequently causes harm to the patient.
- An AI based credit scoring system incorrectly flags the unreliability of a person and a loan is denied based on this decision.
- An AI system classifies a patient incorrectly as low risk, leading to a doctor not detecting a health condition which otherwise would have been easily identified.
- An AI based recruitment system checks CVs received and discards highly qualified candidates because of their gender or ethnicity and the hiring organisation only pursues applications that have passed the AI based first check.

(14) The direct or indirect causations should be limited to cases in which the AI system is used in accordance with its intended purpose and reasonably foreseeable misuse, and the incident is not due to the wrong, unexpected use and unexpected errors by the system-users.

2.4. Death of a person or serious harm to a person's health

(15) Serious[7] harm to person's health can include[8]:

- a life-threatening illness or injury
- temporary or permanent impairment of a body structure or a body function
- a condition necessitating hospitalisation or prolongation of existing hospitalization
- medical or surgical intervention to prevent the first two examples. Examples of this can be:
    - professional medical care or additional unplanned medical treatment
    - a clinically relevant increase in the duration of a surgical procedure
- a chronic disease or serious psychological disease (a disease is serious when it impairs a person from significant life activities, including day-today functioning).
- foetal distress, foetal death or any congenital abnormality (including congenital physical or mental impairment) or birth defects.

2.5. Serious and irreversible disruption of the management or operation of critical infrastructure

(16) For the definition of critical infrastructure, Article 3 (62) AI Act refers to Article 2, point (4) of Directive (EU) 2022/2557 Critical Entities Resilience Directive ("CER"): "an asset,

[7]In addition, the assessment of 'seriousness' should generally take into account the scale and scope of the harm, as well as its monetary value.
[8]Inspired by MDCG 2023-3 Rev. 2, Questions and Answers on vigilance terms and concepts as outlined in the Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Page 10.

a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service".

(17) Directive (EU) 2022/2555 (NIS2 Directive) applies to essential and important entities in "sectors of high criticality" and other critical sectors", as defined in Annexes I and II of the Directive. Among other obligations, the NIS2 Directive requires essential and important entities to notify significant incidents. Pursuant to Article 23(3)(a) of the NIS2 Directive, an incident that has caused or is capable of causing severe operational disruption of the services shall be considered a significant incident. Therefore, where a provider of high-risk AI systems has reported an incident under the NIS2 Directive due to the incident having caused severe operational disruption of the services, such an incident should also be considered a serious incident under the AI Act, provided that the disruption is irreversible and that the disruption is caused by an incident or malfunctioning of an AI system.

(18) Moreover, where a provider of high-risk AI systems becomes aware that an essential or important entity has reported an incident under the NIS2 Directive due to the incident having caused severe operational disruption of the services, and that the incident was caused by an incident or malfunctioning of an AI system provided by the provider of high-risk AI systems, the incident should also be considered a serious incident under AI Act, provided that the disruption is irreversible.

(19) The AI Act does not provide a threshold for when a disruption is considered to be serious. The CER and Recital 55 of the AI Act provide orientation. Under the AI Act a disruption is to be considered serious if for example:

- The disruption might result in an imminent threat to life or the physical safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core function of the State
- Destruction of key infrastructure.
- Disruption in social and economic activities.

(20) The disruption would also need to be irreversible.

(21) When evaluating a disruption whether it qualifies as irreversible the following aspects should be taken into account:

- The disruption requires rebuilding of physical infrastructure or destroys specialized equipment which is not readily available
- Contamination of water, soil or air
- Loss or corruption of essential records—such as patient data, civil registries, or financial transactions—that cannot be reliably restored or reconstructed.
- Permanent disablement of a critical node, such as a rail junction, power substation, or landing station, that cannot be repaired or replaced without years-long lead times.

- Loss of a space-based asset (e.g. Global Navigation Satellite System or communications satellite) whose destruction vacates its orbital slot or frequency and cannot be replaced without an extended replacement procedure that typically lasts years.

(22) Article 73(3) AI Act requires to report the incident no later than two days after the provider/deployer became aware of the incident. If at that point it is not clear whether the incident is irreversible, an initial report should be submitted.

2.6. Infringements of obligations under Union law intended to protect fundamental rights

(23) The term “fundamental rights” relates to the Charter of Fundamental Rights[9].

(24) The definition of a serious incident in Article 3 (49) (c) AI Act includes "the infringement of obligations under Union law intended to protect fundamental rights". In contrast to Article 3 (49) (a), (b) and (d) AI Act, the term "serious" is not used. However, the wording "intended to protect fundamental rights" is to be understood narrowly, since the reporting obligation of Article 73 AI Act only applies to serious incidents.

(25) The focus on serious incidents fulfils an important filtering function, as without it the reporting obligation could lead to a flow of information on incidents that do not require any action or awareness at the level of the relevant authorities.

(26) Only those infringements that significantly interfere with Charter-protected rights on a large scale, should be reportable. The following cases are examples for such infringements:

- An AI based recruitment system excludes candidates based on ethnicity or gender.
- A credit scoring system excludes certain categories of persons, such as those having a name from a certain region or living in certain neighbourhoods.
- A biometric identification system frequently wrongly identifies people of different ethical background.

2.7. “Serious” harm to property

(27) When assessing whether harm to property is serious the following parameters should be taken into account:

- The economic impact, including the cost of repair or replacement. The damage to property is deemed to be serious if the damage or destruction impairs the intended usability or substance of the property to such an extent that it can no longer be used for its intended purpose. The amount of damage, the cost of repair or the reduction

[9] Recital 1 AI Act “fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the ‘Charter’)”

in value are not decisive in this respect, but should in any case exceed 5% of the purchase price.
- The cultural, or historical significance of the property.
- The extent to which the property loss or damage affects the livelihood or quality of life of individuals or communities.
- The permanence of the damage, including whether the property can be restored to its former state.
- The ripple effects of the damage, such as its impact on surrounding areas or related operations.

2.8. "Serious" harm to the environment

(28) The AI Act does not define serious harm to the environment, but guidance can be found in other EU legislation. The Environmental Liability Directive 2004/35/EC identifies environmental damage as harm to protected species and habitats, water, and land. The Environmental Crime Directive (EU) 2024/1203 "qualifies criminal offences" as actions causing irreversible or long-lasting widespread damage to significant ecosystems, habitats in protected areas, air quality, soil, or water.

(29) Art. 3 (5) of the environmental crime directive further defines elements that must be taken into account when assessing whether a damage or likely damage is serious. These elements include:

- the baseline condition of the affected environment
- whether the damage is long-lasting, medium-term or short-term
- the extent of the damage
- the reversibility of the damage.

(30) Moreover, "Serious" harm to the environment could include:

- Contamination of environmental resources
- Disruption of natural ecosystems
- […]

2.9. Widespread infringement

(31) Article 73 (3) AI Act requires instant incident reporting in case of a widespread infringement. The term widespread infringement is defined in Art. 3 (61) AI Act as "any act or omission contrary to Union law protecting the interest of individuals, which: (a) has harmed or is likely to harm the collective interests of individuals residing in at least two Member States other than the Member State in which: (i) the act or omission originated or took place; (ii) the provider concerned, or, where applicable, its authorised

representative is located or established; or (iii) the deployer is established, when the infringement is committed by the deployer; (b) has caused, causes or is likely to cause harm to the collective interests of individuals and has common features, including the same unlawful practice or the same interest being infringed, and is occurring concurrently, committed by the same operator, in at least three Member States;"

(32) When Article 73(3) AI Act addresses the reporting for a widespread infringement, it implicitly refers to a serious incident that also constitutes a widespread infringement. The widespread infringement accordingly must qualify as a serious incident. An event that only constitutes a widespread infringement but not a serious incident is not addressed by Article 73(3) AI Act.

2.9.1. "Act or omission"

(33) The term "act or omission" should be understood wide and include any act or omission that is causal related to the high-risk AI system.

2.9.2. Harm to "collective interests of individuals"

(34) The definition of the term widespread infringement refers to any "act or omission contrary to Union law protecting the interest of individuals that has harmed or is likely to harm the collective interests of individuals". refers to interest (that is protected under Union law) that is shared by a group of people, rather than just one individual. These collective interests may conflict with individual preferences.

(35) Examples of widespread harm to the "collective interest of individuals" under Article 73 AI Act include:

- Environmental protection,
- Public health,
- The functioning of democratic institutions.

2.9.3. "Occurring concurrently"

(36) Occurring concurrently requires that the harmful practices or infringements are happening simultaneously.

3. OBLIGATIONS FOR DIFFERENT ACTORS

3.1. Providers of high-risk AI Systems

3.1.1. Obligation to report

(37) Article 73 (1) AI Act specifies that providers of high-risk AI Systems need to report any serious incident to the market surveillance authorities of the Member States where that incident occurred. If the exact location is not known to the provider, it is the business location of the deployer that counts.

(38) Article 73 (2) AI Act further specifies that the reporting needs to be made immediately but not later than 15 days after the provider becomes aware of the serious incident. If the serious incident is a widespread infringement or the Serious Incident is a serious and irreversible disruption of the management or operation of critical infrastructure, the reporting should be immediately, but not later than 2 days after the provider becomes aware of the serious incident (Article 73(3) AI Act). In the event of the death of a person the reporting should be immediately, but not later than 10 days after the provider becomes aware of the serious incident (Article 73(4) AI Act).

(39) If necessary to ensure timely reporting, an initial report that is incomplete should be submitted (Article 73(5) AI Act).

(40) For high-risk AI systems which are safety components of medical devices, or are themselves medical devices[10], the notification of serious incidents shall be limited to infringements of obligations under Union law intended to protect fundamental rights, and shall be made to the national competent authority chosen for that purpose by the Member States where the incident occurred (Article 73 (10) AI Act).

(41) For example: […]

3.1.2. Obligation to investigate

(42) The provider has to perform, without delay, the necessary investigations in relation to the serious incident and the AI system concerned. This has to include a risk assessment of the incident, and corrective action (Article 73 (6) AI Act). The provider "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". Any change that could negatively affect the assessment or other measures under Article 19 of regulation (EU) 2019/1029 should be considered an alteration that is subject to the notification requirements of Article 73(6) AI Act.

(43) When assessing whether such an alteration has occurred, the following factors should be considered:

- Alterations to components directly involved in the serious incident, including software updates, hardware replacements, or configuration changes
- Changes affecting the availability of data required for technical investigations (e.g., overwriting training datasets or disabling monitoring tools)
- Whether the change affects the ability to reconstruct the sequence of events leading to the incident (e.g., modification of log files, sensor data, or decision-making algorithms)

[10] Regulations (EU) 2017/745 and (EU) 2017/746

- […]

3.1.3. Obligation to cooperate

(44) The provider has to cooperate with the competent authorities, and where relevant with the notified body concerned during the investigations (Article 73(6) AI Act).

(45) Cooperation includes:

- Complying with measures by market authorities according to Article 19 of the market surveillance regulation[11]
- Communicating and reacting within reasonable time, but not later than 24 hours
- […]

(46) Communication with notified bodies is considered relevant if:

3.2. Deployers of high-risk AI Systems

(47) Where deployers have identified a serious incident, they shall immediately inform the provider, and then the importer or distributor as well as the relevant market authorities (Article 26 (5) AI Act). Immediately should be understood as within 24 hours.

(48) If the deployer is not able to reach the provider, the provider obligations apply mutatis mutandis to the deployer. The deployer should be considered unable to reach the provider if:

- The Provider does not answer within 24 hours
- […]

3.3. Providers of GPAI Models with systemic risk

(49) According to Article 55 (1) (c) AI Act providers of general-purpose AI models with systemic risks shall keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them.

(50) The term ‘serious incident’ is defined in Article 3(49) AI Act only in relation to AI systems. For serious incidents concerning general-purpose AI models with systemic risk pursuant to Article 55(1)(c) AI Act, the General-Purpose AI Code of Practice facilitates demonstrating compliance by way of its Commitment 9 in the Safety and Security Chapter. This is complemented by the Commission Guidelines on the scope of the obligations for providers of general-purpose AI models lay out the Commission’s application of the term ‘serious incident’ for providers of general-purpose AI models with

[11] Regulation 2019/1020

systemic risk. Further, the Commission will publish a template for the serious incident reporting by providers of general-purpose AI models with systemic risk."

3.4. Market surveillance authority

(51) The market surveillance authority will have to take appropriate measures, as provided for in Article 19 of the market surveillance regulation[12], within seven days from the date it received the notification of the serious incident (Article 73(8) AI Act).

(52) When receiving a notification related to a serious incident with regard to the protection of fundamental rights, the relevant market surveillance authority has to inform the national public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights (referred to in Article 77 AI Act).

3.5. National competent authority

(53) National competent authorities have to immediately notify the Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of the market surveillance regulation[13]. (Article 73 (11) AI Act).

3.6. Commission

(54) Inform/Establish other market authorities – Alert System

3.7. AI Board

(55) The AI Board may evaluate and review the incident reporting. (Article 66(e) AI Act.

4. INTERPLAY WITH OTHER UNION INCIDENT REPORTING OBLIGATIONS

(56) Following Article 73(9) AI Act, when it comes to high-risk AI systems listed in Annex III that are subject to Union legislative instruments laying down reporting obligations equivalent to those set out in the AI Act, the notification of serious incidents shall be limited to incidents referred to in Art. 3 (49) (c) AI Act, i.e. fundamental rights.

(57) Under Directive (EU) 2022/2557 Critical Entities Resilience Directive ("CER") critical entities have to notify the competent authority within 24 hours of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. The "sectors" mentioned in Annex III point 2 AI Act, digital infrastructure, road, traffic, water, gas, heating or electricity are also subject to the CER Directive. Therefore under the AI Act the obligation to report incidents for AI systems mentioned in Annex III point 2 AI Act only applies to the violation of fundamental rights. The CER Directive also applies to credit institutions as defined in Article 4(1) of Regulation 575/2013 and

[12] Regulation (EU) 2019/1020
[13] Regulation (EU) 2019/1020

Public administration entities of central governments as defined by Member States in accordance with national law. Insofar as these bodies are obliged to report incidents under the CER, only the additional requirements of reporting violations of fundamental rights apply. The following cases could be examples for such serious incidents:

(58) A load-shedding AI system prioritises supply using a proxy for household income, systematically cutting power to low-income areas and violating the right to non-discrimination.

(59) A predictive-maintenance AI system ranks pipe-replacement projects with a variable that correlates to neighbourhood ethnicity and in this way delaying safe-water access for unprivileged demographic groups and breaching equal-treatment rights.

(60) Under the NIS2 Directive, essential and important entities have to notify the CSIRT or, where applicable, the competent authority of any significant incident as defined in Article 23(3) of the Directive. The incident reporting timelines are defined in Article 23(4) of the Directive, encompassing an early warning within 24 hours of becoming aware of the significant incident, an incident notification within 72 hours of becoming aware of the significant incident, and a final report not later than one month after the submission of the incident notification. The "sectors" mentioned in Annex III point 2 AI Act, digital infrastructure, road, traffic, water, gas, heating or electricity are also subject to the NIS2 Directive. Therefore, under the AI Act the obligation to report incidents for AI systems mentioned in Annex III point 2 AI Act only applies to the violation of fundamental rights. The NIS2 Directive also applies to credit institutions as defined in Article 4(1) of Regulation 575/2013 and public administration entities of central governments as defined by Member States in accordance with national law. Insofar as these bodies are obliged to report incidents under NIS2, only the additional requirements of reporting violations of fundamental rights apply.

(61) The Digital Operational Resilience Act (DORA) obligates in Article 19 financial entities to report major ICT-related incidents and significant cyber threats to relevant competent authorities and Regulation 2025/302 provides financial entities with standardized templates for reporting major ICT-related incidents and notifying significant cyber threats. Regulation 2025/302 also includes a detailed data glossary and comprehensive instructions to guide the financial entities in reporting such incidents, ensuring consistency and clarity in incident notification and management within the financial sector. Therefore insofar AI systems falling under Annex III Point 5 (b) and (c) are considered financial entities in the meaning of Regulation 2025/302, only the additional requirements of reporting violations of fundamental rights apply. The following cases could be examples for such serious incidents:

(62) A machine-learning model embeds postcode as a feature, resulting in systemic loan rejections for applicants from predominantly minority neighbourhoods leading to discrimination.

(63) An AI based risk scoring tool infers genetic predispositions from pharmacy-purchase data, raising premiums for individuals with certain hereditary conditions without consent and breaching privacy and equality rights.

(64) In addition, there might be situations where incident reporting obligations overlap with Article 33 GDPR, when there is a "personal data breach", Article 23 NIS 2 Directive[14] on reporting obligations for significant incidents affecting essential and important entities, the Cyber Resilience Act[15]. The Commission will at a later point specify the interplay between incident reporting under sectorial legislation, horizontal legislations and the AI Act.

(65) According to Article 73 (10) AI Act, for high-risk AI systems which are safety components of medical devices, or are themselves medical devices, covered by the MDR and IVDR, the reporting of serious incidents is limited to fundamental rights, (Article 3 (49) (c) AI Act).

(66) Other (than medical devices) AI systems (or components of AI systems) that are listed in Annex I, Section A (e.g., machinery, lifts, toys) are subject to the incident reporting obligations of Article 73 AI Act. Providers may be obliged to report the same incident under both the AI Act and the sectoral regulation. The Commission will at a later point specify the interplay between incident reporting under sectorial legislation and the AI Act.

(67) Additionally, Article 2(2) AI Act establishes special rules for AI systems that are components of products governed by Annex I, Section B — a list of Union harmonisation legislation covering sectors such as motor vehicles, aviation, marine equipment, and others. These products are deemed sufficiently regulated under their own frameworks, and AI systems embedded within them do not fall under the AI Act's reporting regime, including Article 73.

[14] Directive (EU) 2022/2555
[15] Regulation (EU) 2024/2847