that you responded to this consultation as, your answer regarding residence, and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself.

If you represent one or more organisations: *All contributions to this consultation may be made publicly available. You can choose whether you would like respondent details to be made public or to remain anonymous. Only organisation details may be published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its size, its presence in or outside the EU and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.*

- (●) Yes
- ( ) No

* Do you agree that we may contact you in the event of follow-up questions or if we want to learn more about your responses?

- (●) Yes
- ( ) No

☑ I acknowledge the attached privacy statement.

Privacy_Statement_2025-08-25.pdf

---

* **On which part(s) of the public consultation are you interested to contribute to?** *Multiple answers are possible. Please note that selecting a particular answer will direct you to a set of questions specifically related to subject specified.*

- ☑ Questions in relation to **relevant definitions** as provided by the AI Act. (Section 1)
- ☑ Question in relation to **practical examples** (use cases). (Section 2)
- ☑ Questions in relation to the **interplay** between incident reporting for high-risk systems pursuant to **Annex III** with other incident reporting obligations. (Section 3)
- ☑ Questions in relation to the **interplay** between incident reporting for high-risk systems pursuant to **Annex I** with other incident reporting obligations. (Section 4)
- ☑ Question in relation to the **incident reporting template**. (Section 5)

Section 1. Questions in relation to relevant definitions as provided by the AI Act

Article 73(1) AI Act mandates 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.
*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: (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;"
For further clarification the guidance already provides examples for incidents or malfunctions in paragraph 12.

Question 1. Do you agree with the examples provided by the guidance?

- ○ Yes
- ◉ No

* Explain why you disagree with the provided examples.

500 character(s) maximum

P.12 does a bad job at tying the examples back to the criteria for 'serious incident'. It lists malfunction types but doesn't clarify if these are automatically reportable. Leaving open questions: If an autonomous system malfunction misfires a weapon but injures no one, being an unexpected system behaviour with high potential of causing death, is this reportable? If a deployer detects highly manipulative or unsafe emergent behaviour, can they wait until harm materialises before reporting?

Question 2. Provide further examples for an incident or malfunctioning.

1500 character(s) maximum

The notion of "malfunctioning" remains unclear. The term is included in the definition of "serious incident," yet the guidelines state that the distinction between incident and malfunction "should not be understood as a strict one." This is confusing, is there or is there not a distinction? OECD definition considers an incident an actual harm and a hazard a potential harm. Why does the AI Act & guidelines overlook the "AI hazard" notion? Examples that illustrate this gap: 1. Model hallucination with no identifiable victim: the system repeatedly outputs false medical advice, but no concrete harm has yet been traced to an individual; or there are signs of possible harms but a casual pathway is not easy to establish. 2. Significant unexplained drop in accuracy: performance deterioration is detected, but no downstream harm has been confirmed. 3.Emergent manipulative or psychopathic model behaviour: signals are visible at the technical level, yet no incident meeting Art. 3(49) has occurred. 4. AI system exploiting electricity-market rules: behaviour distorts competition, but no precise economic harm can yet be attributed to a specific actor or consumer. This differs from regulated markets regulation where a "non-competitive" behaviour has to be always reported. These cases are safety-relevant early warnings, but under the current wording they may not qualify as reportable incidents because the causal link to one of the four Art. 3(49) outcomes cannot yet be proven.

*Article 3(49)(a) AI Act lists the **death of a person, or serious harm to a person's health** as one of the (alternative) conditions for a serious incident. The guidance provides a list of examples for serious harm to a person's health in paragraph 15.*

Question 3. Do you agree with the examples provided by the guidance?

- ○ Yes
- ○ No

Question 4. Do you consider it necessary to include further examples in the list?

- [x] Yes
- [ ] No

* Describe further examples and explain why it would be useful to add them to the existing list.

1500 character(s) maximum

The guidelines should explicitly clarify that “serious harm to a person’s health” under Article 3(49)(a) also includes psychological and emotional harm, not only physical injury by adding examples illustrating when psychological harm triggers reporting obligations. This would be consistent with how JTC21 understands the scope of ‘health’. This is particularly important, given the growing use of AI systems in areas like mental-health support, behavioural profiling, recommender systems, and content moderation. We would also like more examples to clarify if the following cases trigger reporting obligations under art. 3(49) (a) (or alternatively (b) to (d). If delayed medical harms should be reported or if a system malfunction threatens the health of a human but the situation is mitigated by a human. For example: 1. An AI-based diagnostic tool recommends the wrong medication but the doctor overrules it. 2. A patient's harm manifests later, outside the healthcare setting. 3. Vulnerabilities that create latent risks to human health. For example: An adversarial sticker applied to a stop sign causes an autonomous vehicle to ignore it. No accident has happened but the threat to human life is clear.

*Article 3(49)(b) AI Act lists **a serious and irreversible disruption of the management or operation of critical infrastructure** as one of the (alternative) conditions for a serious incident. The guidance provides examples to determine whether a disruption is to be considered serious in paragraph 19.*

Question 5. Do you agree with the examples provided by the guidance?

- [ ] Yes
- [ ] No

Question 6. Do you consider it necessary to include further examples in the list?

- [x] Yes
- [ ] No

* Describe further examples and explain why it would be useful to add them to the existing list.

1500 character(s) maximum

Additional examples need to clarify what qualifies as an “imminent threat to life or the physical safety of a person” in the context of a serious and irreversible critical infrastructure disruption (Art. 3(49)(b)). It is important for examples to make clear that "imminent" refers to a dangerous situation including one that has not materialised in a harm to persons yet. It would be useful to add examples showing whether wrong or exploitative behaviour with no realised harm is reportable because they constitute a disruption of social and economic activities: - Electricity markets: an AI trading agent systematically exploits market design loopholes, artificially influencing prices. No harm can yet be quantified, but the behaviour undermines grid stability and market integrity. In regulated energy markets, such behaviour must be reported before damage occurs. Further examples for other critical sectors: 1. Emergency call routing: an AI triage model misclassifies emergency calls, delaying ambulance dispatch. No death has occurred yet. 2. Logistics/supply chains: AI-related errors could cause delay/halting of food, medical shipments or other critical materials. E.g. temperature-controlled shipments of insulin or blood plasma are late due to an AI scheduling failure. Including such examples would clarify whether near-misses and latent safety failures in critical infrastructure fall under Article 73, or whether only already-realised damage triggers notification.

The guidance also provides examples of factors to consider when evaluating whether a disruption qualifies as irreversible in paragraph 21.

Question 7. Do you agree with the examples provided by the guidance?

- Yes
- No

Question 8. Do you consider it necessary to include further examples in the list?

- Yes
- No

Article 3(49)(c) AI Act lists ***the infringement of obligations under Union law intended to protect fundamental rights*** *as one of the (alternative) conditions for a serious incident. The guidance provides examples for serious infringements on fundamental rights in paragraph 26.*

Question 9. Do you agree with the examples provided by the guidance?

- Yes
- No

* Explain why you disagree with the provided examples.

500 character(s) maximum

Paragraphs 23–26 do not clarify what counts as an infringement of fundamental-rights obligations. Using the example, if “a recruitment AI filters candidates by gender or ethnicity” but HR overturns the decision, no right is actually violated. Is this still a “serious incident” because the system attempted to infringe a protected right? The guidance should clarify whether prevented or corrected infringements are reportable and by who (the provider, deployer)?

Question 10. Provide one or several examples for an infringement that significantly interferes with Charter-protected rights on a large scale.

1500 character(s) maximum

The examples provided all focus on the same article of the Charter. (1) A data breach of the system or the possibility of inferring data from other users by prompting the system would also be a fundamental rights infringements. (2) A customer-service system that leaks conversation logs. (Article 8) An automated decision system for social benefits issues mass denials with opaque reasoning and no effective human review channel, blocking access to redress for thousands. (Arts. 41, 47). Article 31 (Fair and Just working conditions) - There can be many examples for infringements of workers rights: - Autosuspensions without due process: A platform’s risk model mass-flags “fraudulent activity,” deactivating worker accounts, cutting income or causing them to get fired. - Working-time violations at scale: A shift-scheduling AI routinely assigns rosters exceeding legal weekly limits and shortens rest periods for employees, causing fatigue and health risks. An AI tool falsely flags exam anomalies, invalidating thousands of exams with difficult or limited appeal procedures. (article 14 Education) In addition, the guidance may need to make a distinction between human rights violations avoided by required

routine human oversight from the deployer according to the system documentation, and violations that were avoided via managerial or escalation processes not included among required oversight processes. Could this impact who needs to report the incident?

Question 11. Provide one or several examples for an infringement that does not significantly interfere with Charter-protected rights on a large scale.

1500 character(s) maximum

Minor payroll rounding error for a small team (Art. 31 CFR). An automated timekeeping system miscalculates overtime for a small number of workers in one company/office during a single pay period; the error is noticed in the next cycle, the wages are compensated (with interest?) and the system checked. This would be a localized, short-lived impact on workers conditions and not “significant at scale.”

*Article 3(49)(d) AI Act lists **serious harm to property or the environment** as one of the (alternative) conditions for a serious incident. The guidance provides parameters to determine whether harm to **property** is serious in paragraph 27.*

Question 12. Do you agree with the parameters provided by the guidance?

- ○ Yes
- ○ No

Question 13. Do you consider it necessary to include further parameters in the list?

- ◉ Yes
- ○ No

* Describe one or several parameters and explain why it would be useful to add them to the existing list.

500 character(s) maximum

Unclear whether intangible or digital assets are included. In AI environments, seriousness of property damage is also operational. Cascade or spill-over effects where failure of 1 asset triggers disruption across supply chain or dependent systems. Proportion of affected users: A <5% monetary loss may become serious when scaled. Maybe include a base monetary threshold as a parameter. For low value damages 5% shouldn’t trigger the obligation and for high quantities 5% threshold might be too high

*The guidance also provides examples for serious harm to the **environment** in paragraph 30.*

Question 14. Do you agree with the examples provided by the guidance?

- ◉ Yes
- ○ No

Question 15. Provide further examples for serious harm to the environment.

500 character(s) maximum

Article 73(2) AI Act mandates that the reporting needs to 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, but not later than 15 days after the provider becomes aware of the serious incident. 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. The guidance provides examples of indirect causation in paragraph 13.

Question 16. Do you agree with the examples provided by the guidance?

- ○ Yes
- ◉ No

* Explain why you disagree with the provided examples.

500 character(s) maximum

The examples do not clarify the threshold for triggering reporting. “Establishing a causal link” may require full investigation, while “reasonable likelihood” should enable earlier notification, yet the guidance never defines it. A clearer explanation of the later term could be that there are credible technical or operational signs that an AI system may have contributed to the incident, even before causality is proven or pending causal verification.

Question 17. Do you consider it necessary to include other examples in the list?

- ◉ Yes
- ○ No

* Describe other examples and explain why it would be useful to add them to the existing list.

1500 character(s) maximum

Additional examples would be useful because the current list does not address two key gaps: How “indirect harm” is to be distinguished from harms too remote or too diffuse to be reportable. How providers or deployers can reasonably become aware of an indirect incident, especially when the harm occurs far downstream and outside their technical visibility. Two example scenarios: 1. Infrastructure chain reaction: An AI-based demand-forecasting tool used by a shipping company underestimates port congestion. This triggers a cascade of delays that ultimately lead hospitals to receive spoiled temperature-sensitive medicines. The harm is real, but the AI provider never sees the link, because the impact occurs several actors later in the supply chain. 2. Financial knock-on effect: A credit-risk model downgrades small energy suppliers, increasing their cost of capital. Months later, one supplier collapses, causing price spikes for households. The provider has no direct access to market data and may never realise its model contributed to the failure. These type of examples would help clarify: When an indirect causal chain is still “reasonably attributable” to the AI system, and when it becomes too remote. Whether the duty to monitor includes proactively seeking downstream signals, or only reacting once information passively reaches the provider.

Article 73 (3) AI Act requires instant incident reporting in case of a serious incident that also constitutes 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) […]; (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;"*
The definition 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.
The guidance provides examples for widespread harm to the "collective interest of individuals" in paragraph 35.

Question 18. Do you agree with the examples provided by the guidance?

- Yes
- No

Question 19. Provide further examples for widespread harm to the "collective interest of individuals".

1500 character(s) maximum

Article 73(6) AI Act mandates that 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.
The guidance provides factors/indications to be considered in the assessment whether such an alteration has occurred in paragraph 43.

Question 20. Do you agree with the indications provided by the guidance?

- Yes
- No

Question 21. Provide further indications for assessing whether an alteration has occurred.

1500 character(s) maximum

Article 73(6) AI Act also mandates that the provider has to cooperate with the competent authorities, and where relevant with the notified body concerned during the investigations. The guidance provides a list of examples of cooperation in paragraph 45.

Question 22. Do you agree with the examples provided by the guidance?

- Yes
- No

Question 23. Provide further examples for cooperation.

600 character(s) maximum

Question 24. Provide factors to determine when cooperation with the notified body is relevant.

600 character(s) maximum

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. If the deployer is not able to reach the provider, the provider obligations apply mutatis mutandis to the deployer. The guidance provides an example in which the deployer is considered to not be able to reach the deployer in paragraph 48.

Question 25. Do you agree with the example provided by the guidance?

- ○ Yes
- ◉ No

* Explain why you disagree with the provided example.

500 character(s) maximum

The example seems to suggest that silence for 24h shifts all reporting and investigation duties to the deployer. Providers may simply delay responding and let the deployer assume the burden. This creates an incentive for strategic inaction, weakens accountability, and risks poorer-quality incident reports, since deployers might lack the technical insight needed to assess root causes. Can there be legal consequences for the provider for omitting its duties?

Question 26. Provide further examples for situations in which the deployer should be considered not able to reach the deployer.

500 character(s) maximum

Conflict of interest in the value chain: The provider is contractually or commercially entangled with actors involved in the incident creating a clear risk that the investigation would not be impartial. Ongoing legal or reputational obstruction: The provider is under regulatory investigation, litigation, would face reputational or financial damage if the incident is confirmed, giving reasonable grounds to doubt their willingness to cooperate or conduct a credible investigation.

Section 2. Question in relation to practical examples (use cases)

This section provides the possibility to provide further use cases for clarification in the guidance. The cases should fulfil one of the following criteria: (1) provide an illustrative example of an incident that does or does not fall under the incident reporting obligations, (2) presents a difficult borderline case that from your

assessment is not sufficiently clarified from the current guidance, (3) indicates the need for further clarification beyond the current scope of the guidance. You can provide up to five answers.

Question 27.

	Provide the paragraph(s) in the guidance the use case relates to (if applicable).	Describe your use case.	Describe why you consider this use case helpful.
1	*50 character(s) maximum*	*1000 character(s) maximum*	*1000 character(s) maximum*
2	*50 character(s) maximum*	*1000 character(s) maximum*	*1000 character(s) maximum*
3	*50 character(s) maximum*	*1000 character(s) maximum*	*1000 character(s) maximum*
4	*50 character(s) maximum*	*1000 character(s) maximum*	*1000 character(s) maximum*
5	*50 character(s) maximum*	*1000 character(s) maximum*	*1000 character(s) maximum*

Section 3. Questions on horizontal aspects of the high-risk classification

The same incident can produce the need for incident reporting obligations not only under the AI Act, but also for example under Data Protection law, Cybersecurity law or Sectoral legislation.
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.

Question 28.

	Legislation that requires to report incidents that could involve a high-risk system pursuant to Annex III of the AI Act	Do you consider this obligation equivalent to the incident reporting obligation under Art. 73 AI Act, thus reducing the obligation to report to infringements on fundamental rights?	Motivate your answer.
1	Art. 15 CER – Directive (EU) 2022/2557	◉ always ○ sometimes ○ never	*2000 character(s) maximum* Definition of Incident under CER (art.2(3)): “Incident means an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service, including when it affects the national systems that safeguard the rule of law” An AI system that due to any circumstance imaginable creates an event that disrupts or POTENTIALLY disrupts an essential service would trigger the reporting obligation. This is a lower threshold than the reporting obligations under the AI Act which only trigger under actual harms or disruptions (art.3(49)). Differences in timelines: the CER gives 24h to the entity to report all incidents that trigger under their regulation. On the other hand, the AI Act reporting time-limits depend on severity. Typically 15 days as the baseline, accelerated to 10 days if death and 2 days if widespread infringement or a serious or irreversible disruption. The CER has a more robust framework, replicating most EU prior reporting standards where potential damages usually have to be reported (in this case potential disruptions). Therefore it is a good thing that the CER directive obligations are not equivalent. On the one hand this is very positive for art.3(49)(a),(b) and (d) but undermines the protection of fundamental rights for Annex III systems as the threshold is higher to have to report a violation of fundamental rights.
2	Art. 19 DORA – Regulation (EU) 2022/2554	○ always ○ sometimes ○ never	*2000 character(s) maximum*
3	Art. 33 GDPR – Regulation (EU) 2016	○ always ○ sometimes ○	*2000 character(s) maximum*

	/679	never	
4	Art. 23 NIS 2 – Directive (EU) 2022/2555	always sometimes never	*2000 character(s) maximum*
5	Art. 14 CRA – Regulation (EU) 2024 /2847	always sometimes never	*2000 character(s) maximum*
6	Other (please fill in) *100 character(s) maximum*	always sometimes never	*2000 character(s) maximum*
7	Other (please fill in) *100 character(s) maximum*	always sometimes never	*2000 character(s) maximum*

The guidance provides examples for serious incidents that required a report pursuant to CER in paragraph 58 and 59 and therefore do not require a report under Art. 73 except for incidents referred to in Art. 3(49)(c) AI Act, i.e. fundamental rights.

Question 29. Do you agree with the examples provided by the guidance?

- ○ Yes
- ○ No

Question 30. Do you consider it necessary to include other examples in the list?

- ◉ Yes
- ○ No

* Describe other examples and explain why it would be useful to add them to the existing list.

2000 character(s) maximum

Yes, more examples are needed in different critical infrastructures covered by CER to better understand how AI systems are used or will be used. These examples need to help limit when a system is considered to be part of the critical infrastructure or when it is something internal or complimentary used by the company and therefore, falls out of the scope of CER and falls within art.73 AI Act. For example: 1.Air transport: Scheduling algorithm failure causes cascading flight delays. Is this part of the critical infrastructure? Or would it only cover systems that directly impact the safety of the flight? 2. A predictive analytics that optimises staffing levels for grid-maintenance crews. It does not operate the grid directly, but understaffing caused by a faulty model could delay repairs and indirectly lead to grid failure. Is this part of “the provision of the essential service” (CER) or just an HR tool (AI Act only)?

The guidance provides examples for serious incidents that require a report pursuant to DORA in paragraph 62 and 63 and therefore do not require a report under Art. 73 except for incidents referred to in Art. 3(49)(c) AI Act, i.e. fundamental rights.

Question 31. Do you agree with the examples provided by the guidance?

- ◉ Yes
- ○ No

Question 32. Do you consider it necessary to include other examples in the list?

- ○ Yes
- ○ No

The Commission plans to further specify the interplay in situations where incident reporting obligations overlap with the GDPR, the NIS2 Directive or the CRA. Please provide examples which (1) are covered under Art. 73 of the AI Act and (2) also covered under at least one of the following: GDPR, NIS2 Directive, or the CRA. You can provide up to five use cases.

Question 33.

	Provide a use case.	Under which legislation (s) do you need to report the incident other than the AI Act?	Explain your assessment.
1	*2000 character(s) maximum* Paragraph 61 states that an AI system is only exempted from AI-Act reporting (except for fundamental-rights cases) when it falls under Annex III point 5(b) or 5(c) of the AI Act: (b) creditworthiness and credit scoring of natural persons and (c) risk assessment and pricing in life and health insurance. Therefore, this seems to mean that This means that many other financial-sector AI uses, algorithmic trading, asset-allocation models, AML/CTF monitoring, robo-advisors, market-surveillance tools, liquidity-risk engines, high-frequency execution algorithms etc. do not clearly fall under DORA even though they are core to financial stability.	☐ GDPR ☐ NIS2 ☐ CRA ☐ CER ☑ DORA	*2000 character(s) maximum* There is a significant interplay ambiguity for AI systems used in the financial sector. Under the CER Regulation, financial services are not required to report incidents because they are already covered by sector-specific legislation (e.g., DORA, MiFID II, PSD2, CRD/CRR). However, the draft AI-Act guidance narrows the scope of this "sector-specific overlap" much further than those frameworks do. Paragraph 61 states that an AI system is only exempted from AI-Act reporting (except for fundamental-rights cases) when it falls under Annex III point 5(b) or 5(c) of the AI Act: (b) creditworthiness and credit scoring of natural persons and (c) risk assessment and pricing in life and health insurance. This means that many other financial-sector AI uses, algorithmic trading, asset-allocation models, AML/CTF monitoring, robo-advisors, market-surveillance tools, liquidity-risk engines, high-frequency execution algorithms etc. do not clearly fall under DORA even though they are core to financial stability. As a result, it is unclear whether these AI systems (1) always fall within alternative financial sectorial regulations, (2) fall under CER because incident-driven disruption of payment services or market infrastructure could be considered critical, or (3) default back into full Article 73 AI-Act reporting because no specific regime is recognised by the guidance. Some use cases appear to be both covered by CER's logic that delegates financial sector reporting obligations to DORA and other sectorial financial regulation and not covered under reporting guidelines (paragraph 61 logic) that narrows the application of DORA for AI systems.
2	*2000 character(s) maximum*	☐ GDPR ☐ NIS2 ☐ CRA ☐ CER	*2000 character(s) maximum*

		☐ DORA	
3	*2000 character(s) maximum*	☐ GDPR ☐ NIS2 ☐ CRA ☐ CER ☐ DORA	*2000 character(s) maximum*
4	*2000 character(s) maximum*	☐ GDPR ☐ NIS2 ☐ CRA ☐ CER ☐ DORA	*2000 character(s) maximum*
5	*2000 character(s) maximum*	☐ GDPR ☐ NIS2 ☐ CRA ☐ CER ☐ DORA	*2000 character(s) maximum*

The incident reporting obligations in the AI Act can also overlap with other (sectoral) incident reporting obligations. The commission plans to further specify the interplay.

Question 34.

	Name the sectoral legislation and the exact article that mandates reporting	Provide an example of an incident that would lead to reporting obligations under both the AIA and the sectoral legislation.	Under which point(s) of Annex III of the AI Act would that system be covered?	Do you consider this obligation equivalent to the incident reporting obligation under Art. 73 AI Act, thus reducing the obligation to report to infringements on fundamental rights?	Motivate your answer.
1	*100 character(s) maximum*	*2000 character(s) maximum*	☐ Point (1)(a) ☐ Point (1)(b) ☐ Point (1)(c) ☐ Point (2) ☐ Point (3)(a) ☐ Point (3)(b) ☐ Point (3)(c) ☐ Point (3)(d) ☐ Point (4)(a) ☐ Point (4)(b) ☐ Point (5)(a) ☐ Point (5)(b) ☐ Point (5)(c) ☐ Point (5)(d) ☐ Point (6)(a) ☐ Point (6)(b) ☐ Point (6)(c) ☐ Point (6)(d) ☐ Point (6)(e) ☐ Point (7)(a) ☐ Point (7)(b) ☐ Point (7)(c) ☐ Point (7)(d) ☐ Point (8)(a) ☐ Point (8)(b)	○ always ○ sometimes ○ never	*2000 character(s) maximum*
			☐ Point (1)(a) ☐ Point (1)(b)		

2	*100 character(s) maximum*	*2000 character(s) maximum*	☐ Point (1)(c) ☐ Point (2) ☐ Point (3)(a) ☐ Point (3)(b) ☐ Point (3)(c) ☐ Point (3)(d) ☐ Point (4)(a) ☐ Point (4)(b) ☐ Point (5)(a) ☐ Point (5)(b) ☐ Point (5)(c) ☐ Point (5)(d) ☐ Point (6)(a) ☐ Point (6)(b) ☐ Point (6)(c) ☐ Point (6)(d) ☐ Point (6)(e) ☐ Point (7)(a) ☐ Point (7)(b) ☐ Point (7)(c) ☐ Point (7)(d) ☐ Point (8)(a) ☐ Point (8)(b)	○ always ○ sometimes ○ never	*2000 character(s) maximum*
			☐ Point (1)(a) ☐ Point (1)(b) ☐ Point (1)(c) ☐ Point (2) ☐ Point (3)(a) ☐ Point (3)(b) ☐ Point (3)(c) ☐ Point (3)(d)		

3	*100 character(s) maximum*	*2000 character(s) maximum*	☐ Point (4)(a) ☐ Point (4)(b) ☐ Point (5)(a) ☐ Point (5)(b) ☐ Point (5)(c) ☐ Point (5)(d) ☐ Point (6)(a) ☐ Point (6)(b) ☐ Point (6)(c) ☐ Point (6)(d) ☐ Point (6)(e) ☐ Point (7)(a) ☐ Point (7)(b) ☐ Point (7)(c) ☐ Point (7)(d) ☐ Point (8)(a) ☐ Point (8)(b)	○ always ○ sometimes ○ never	*2000 character(s) maximum*
4	*100 character(s) maximum*	*2000 character(s) maximum*	☐ Point (1)(a) ☐ Point (1)(b) ☐ Point (1)(c) ☐ Point (2) ☐ Point (3)(a) ☐ Point (3)(b) ☐ Point (3)(c) ☐ Point (3)(d) ☐ Point (4)(a) ☐ Point (4)(b) ☐ Point (5)(a) ☐ Point (5)(b) ☐ Point (5)(c) ☐ Point (5)(d)	○ always ○ sometimes ○ never	*2000 character(s) maximum*

			☐ Point (6)(a) ☐ Point (6)(b) ☐ Point (6)(c) ☐ Point (6)(d) ☐ Point (6)(e) ☐ Point (7)(a) ☐ Point (7)(b) ☐ Point (7)(c) ☐ Point (7)(d) ☐ Point (8)(a) ☐ Point (8)(b)		
5	*100 character(s) maximum*	*2000 character(s) maximum*	☐ Point (1)(a) ☐ Point (1)(b) ☐ Point (1)(c) ☐ Point (2) ☐ Point (3)(a) ☐ Point (3)(b) ☐ Point (3)(c) ☐ Point (3)(d) ☐ Point (4)(a) ☐ Point (4)(b) ☐ Point (5)(a) ☐ Point (5)(b) ☐ Point (5)(c) ☐ Point (5)(d) ☐ Point (6)(a) ☐ Point (6)(b) ☐ Point (6)(c) ☐ Point (6)(d) ☐ Point (6)(e) ☐ Point (7)(a)	○ always ○ sometimes ○ never	*2000 character(s) maximum*

			☐ Point (7)(b) ☐ Point (7)(c) ☐ Point (7)(d) ☐ Point (8)(a) ☐ Point (8)(b)		

Question 35. Provide examples of technical measures or additional guidance initiatives that you believe might be helpful for you or the organisation that you represent in addressing concurrent incident reporting obligations under Union legislative instruments.

500 character(s) maximum

Section 4. Questions in relation to the interplay between incident reporting for high-risk systems pursuant to Annex I with other incident reporting obligations

For high-risk AI systems which are safety components of medical devices, or are themselves medical devices, 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).

Question 36. Provide examples for incidents that include safety components of medical devices, or medical devices, covered by the MDR and IVDR so the reporting of serious incidents is limited to fundamental rights (Article 3 (49) (c) AI Act).

1000 character(s) maximum

Non-discrimination (Art. 21): A triage CDS systematically deprioritises patients with darker skin tones for ICU beds due to biased training data. Privacy/Data protection (Arts. 7–8): A connected glucose monitor uploads granular location and health data to third parties without valid consent or lawful basis. Freedom of expression /info (Art. 11) & Autonomy/Dignity (Arts. 1, 3): An AI mental-health assistant embedded in a medical app suppresses crisis keywords, blocking access to information and undermining informed decision-making. Right to education/professional life (Arts. 14, 15) via FR lens: An AI credentialing tool in a diagnostic device wrongly flags foreign-trained clinicians as “unqualified,” barring them from using the device. Equality before the law /Effective remedy (Arts. 20, 47): A radiology AI denies second-opinion requests at scale through opaque automated rules, impeding appeals.

The incident reporting obligations in the AI Act can also overlap with other (sectoral) incident reporting obligations. The commission plans to further specify the interplay.

Question 37.

	Name the sectoral legislation and the exact article that mandates reporting.	Provide an example of an incident that would lead to reporting obligations under both the AIA and the sectoral legislation.	Under which point of Annex I of the AI Act would that system be covered?	Do you consider this obligation equivalent to the incident reporting obligation under Art. 73 AI Act, thus reducing the obligation to report to infringements on fundamental rights?	Motivate your answer.
1	*100 character(s) maximum*	*2000 character(s) maximum*	○ Point 1 ○ Point 2 ○ Point 3 ○ Point 4 ○ Point 5 ○ Point 6 ○ Point 7 ○ Point 8 ○ Point 9 ○ Point 10 ○ Point 11 ○ Point 12	○ always ○ sometimes ○ never	*2000 character(s) maximum*
2	*100 character(s) maximum*	*2000 character(s) maximum*	○ Point 1 ○ Point 2 ○ Point 3 ○ Point 4 ○ Point 5 ○ Point 6 ○ Point 7 ○ Point 8 ○ Point 9 ○ Point 10 ○ Point 11 ○ Point 12	○ always ○ sometimes ○ never	*2000 character(s) maximum*
			○ Point 1 ○ Point 2 ○ Point 3		

3	*100 character(s) maximum*	*2000 character(s) maximum*	Point 4 Point 5 Point 6 Point 7 Point 8 Point 9 Point 10 Point 11 Point 12	always sometimes never	*2000 character(s) maximum*
4	*100 character(s) maximum*	*2000 character(s) maximum*	Point 1 Point 2 Point 3 Point 4 Point 5 Point 6 Point 7 Point 8 Point 9 Point 10 Point 11 Point 12	always sometimes never	*2000 character(s) maximum*
5	*100 character(s) maximum*	*2000 character(s) maximum*	Point 1 Point 2 Point 3 Point 4 Point 5 Point 6 Point 7 Point 8 Point 9 Point 10	always sometimes never	*2000 character(s) maximum*

			Point 11 Point 12		

Section 5. Question in relation to the incident reporting template

The European Commission has provided a template for the report to the market surveillance authority.

Reporting Template - Incident Report for Serious Incidents under the AI Act (High-risk AI systems)
Incident_Report_for_Serious_Incidents_under_the_AI_Act__High-risk_AI_systems_.pdf

The template consists of five sections. The first section relates to administrative information, the second section relates to information about the AI system, the third section relates to information about the incident, the fourth section relates to the providers analysis and the fifth section allows for additional comments.

Question 38.

Section:	Need for amendments or deletions.	Provide the exact section (s) of the template you are referring to (e.g. 1.3.1. a).	Explain your proposal for amendment
1	(•) Yes ( ) No	*50 character(s) maximum* 1.2 and 1.3	*1000 character(s) maximum* A new subsection could be added for cross-linking to prior or related incident reports. E.g. a 'linked incident id' field to support traceability if multiple reports relate to the same case. Section 1.2 - Add (optional) data fields for 'frequency' and 'remediability'. Section 1.2(e): split the 'initial' option into two options: 'initial and incomplete, to be followed by a complete report' and 'initial and complete'. This is to allow the submitter to indicate what logic they are following according to Article 73(5). Section 1.3.5 - More information could be provided, such as authority, date, and relevant reference ID.
2	( ) Yes (•) No	*50 character(s) maximum*	*1000 character(s) maximum*
3	(•) Yes ( ) No	*50 character(s) maximum*	*1000 character(s) maximum* Section 3 - Yes - (1) 3.1 Nature of incident - Subsection 3.1 provides a single free-text form, covering three different incident-related aspects (what went wrong, the effects, and the likely causality). We think that the 'likely causality' part could have its own subsection. 'Description of the effects' could also be described in more detail or even quantified in a separate subsection. (1) 3.1 Nature of incident - some expressions are a bit vague. For example, it's unclear whether 'what went wrong with the system' should also cover the causality, which is listed as a separate item in the same free-text form.
4	(•) Yes ( ) No	*50 character(s) maximum* 4.1, 4.2(b)	*1000 character(s) maximum* 4.1 In addition to the 'initial actions' field, have a field for 'post-incident actions planned'. Right now, subsection 4.1c ('further investigations') does not fully cover this point. 4.1 - 'Preliminary results' could be further divided into technical causes, human or organizational causes, and other relevant contextual information. 4.2(b) – the intended logic of this field seems to be that if a provider submitted an initial report in the belief that the incident was of a nature that needed reporting, but later concludes that this was actually not the case (e.g. because it was a false alarm, or its seriousness was mis-estimated), this field can be used to communicate this conclusion. However, no detailed explanation

			for how to use this field is available. It would be good to add a few lines in the guidance document (or the form itself) stating explicitly that re-assessment of the reportable nature of the incident is allowed and how the form can be used to report this re-assessment.
5	(•) Yes ( ) No	*50 character(s) maximum*	*1000 character(s) maximum* Perhaps this section could be renamed to 'Comments' and have fields for 'General Comments', 'Recommendations for actions by the receiving authority', and also include the fields 'lessons learned', and 'preventive measures proposed'. It should also be clarified in the template that filling in any text in the comment boxes of this section is optional.