AI Standards Lab Recommendations on the Digital Omnibus Amendments to the EU AI Act

Contact person for this document: Marcel Mir, marcel@aistandardslab.org
20 Jan 2026

Introduction

The digital omnibus process offers an opportunity to amend specific provisions of the AI Act. In this context, we provide (i) comments and recommendations on selected amendments as proposed by the Commission in the digital omnibus package, and put forward (ii) a curated set of additional, targeted amendments, not included in the Commission proposal, that would address a few key shortcomings of the AI Act.

We submit these recommendations for consideration by the European Parliament and the Member States acting in their capacity as co-legislators.

There have been recent discussions about amending the AI Act or other laws based on the Grok nudification scandal. In this document we provide no recommendations or analysis specifically related to this scandal.

1 Recommendations related to Commission proposals

In this section, we provide recommendations concerning the Commission's proposals to amend the Artificial Intelligence Act (Regulation (EU) 2024/1689). These proposals are set out in the **AI Act omnibus proposal (COM(2025) 836)** available at https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal pages 20 to 31; the proposals are numbered (1) to (33). We use these numbers in the section titles below, where each section title then also contains the number of the corresponding Article in the AI Act.

We do not make recommendations for all numbered parts: if a number in the range (1) to (33) is missing, it means that our analysis does not see any problems should the co-legislators decide to accept the Commission proposal as is.

(5) Addition of Article 4a

Analysis

This addition aims to give deployers some extra rights related to the use of personal data for bias detection and mitigation. Given that the current GDPR does not explicitly grant these

rights, and given that having these rights will indeed be technically useful for bias detection and mitigation in AI systems, we think this addition is somewhat welcome, as a way to reduce legal uncertainties about what is required or allowed.

That being said, we believe the extra rights granted are useful and proportionate only if the safeguards defined in Article 4a points to the *current* version of the GDPR. But the digital omnibus package from the Commission also proposes a significant weakening of the protections through an omnibus procedure for the GDPR. If this article 4a were to define its safeguards by pointing to the weakened version of the GDPR proposed by the Commission, then we no longer consider this Article 4a to strike the right balance of proportionality and appropriateness: it would weaken fundamental rights protections too much.

We believe that the Commission's proposed changes to the GDPR are so controversial and significant, in their impact on human rights protections, that it would be inappropriate to handle them via the fast omnibus process: they need to be handled by the regular legislative process instead.

One option that the co-legislators have is therefore to reject handling this proposed addition to Article 4a via the omnibus process, in order to send an unambiguous signal to the Commission and the market on where they stand.

While this signal would potentially delay the creation of some useful extra rights and some useful clarifications, we consider such a delay to be acceptable. We note that the GDPR already contains several mechanisms that can be used by providers if they want to be able to legitimately process certain personal data for bias detection and mitigation.

Recommendation

We recommend that the co-legislators consider two options:

1. Accept the proposed addition of Article 4a as part of an AI Act omnibus track based on the consideration that currently the safeguards point to the current, not weakened, version of the GDPR.
2. Reject the proposed addition and suggest the topic is taken up in a regular legislative process that will look at amending the GDPR.

(6) Article 6(4)

Excerpt from Commission proposal for context

Art. 6(4) proposal:

> '4. A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Upon request of national competent authorities, the provider shall provide the documentation of the assessment.';

This proposal removes the text "*Such provider shall be subject to the registration obligation set out in Article 49(2)*" from the AI Act.

Analysis

We do not like this proposal. The removal of the AI system registration requirement will most likely help in keeping the regulator in the dark, facilitating that providers violate the Act hoping that they will remain unnoticed by authorities. It weakens oversight measures and transparency of AI systems in the EU. Removal sends entirely the wrong signal to the market: it will encourage bad actors to enter the market, and have a detrimental effect on trust in the market and on fundamental rights outcomes.

Recommendation

We recommend that the co-legislators aim to keep art. 6(4) unaltered, in its current AI Act wording.

(13) Article 43(3)

Analysis

Concerns:

The requirement for notified bodies already designated under Annex I legislation to apply for AI Act designation **within an 18 months deadline** is problematic:

- The fixed deadline lacks clear justification and may prevent organisations that develop expertise later from entering the system, reducing the long-term pool of notified bodies. This could limit competition, slow conformity assessments as demand grows and reduce the long term scalability of the European AI oversight ecosystem.
- Ideally, the network of notified bodies should grow organically over time to meet demand, as the AI adoption increases across industries. Therefore, a more flexible, ongoing application process would better support the development of a robust auditing infrastructure capable of meeting regulatory and market demand.

Positives:

- High risk AI systems that fall under other Union laws (Annex I) must follow the conformity assessment including Article 17 and Annex VII (QMS assessment by notified body).
- Clarifies that manufacturers may avoid third party assessment only if harmonised standards or common specifications cover all relevant AIA requirements.
- Explicitly states systems covered by Annex I and simultaneously listed in Annex III must follow the Annex I conformity assessment procedure, ensuring consistency.

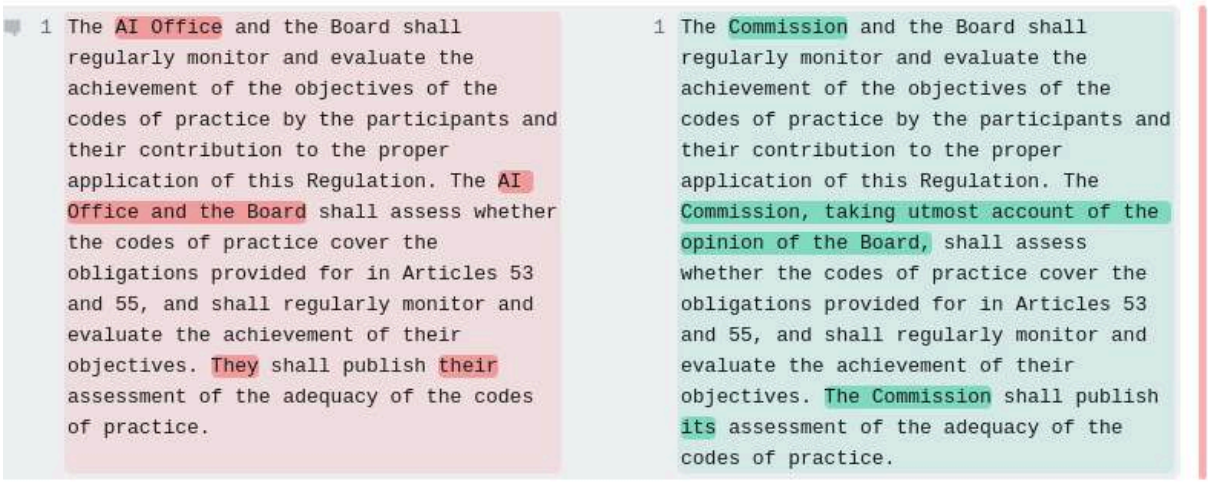
Recommendation

We recommend that the co-legislators aim to accept the proposed changes <u>EXCEPT</u> for the addition of the "18 month deadline" to apply to become a notified body.

(16) Article 56(6)

<u>Excerpt from Commission proposal for context</u>

Red text on the left is the original AI Act, green text on the right are the proposed changes by the Commission.



1 The AI Office and the Board shall regularly monitor and evaluate the achievement of the objectives of the codes of practice by the participants and their contribution to the proper application of this Regulation. The AI Office and the Board shall assess whether the codes of practice cover the obligations provided for in Articles 53 and 55, and shall regularly monitor and evaluate the achievement of their objectives. They shall publish their assessment of the adequacy of the codes of practice.	1 The Commission and the Board shall regularly monitor and evaluate the achievement of the objectives of the codes of practice by the participants and their contribution to the proper application of this Regulation. The Commission, taking utmost account of the opinion of the Board, shall assess whether the codes of practice cover the obligations provided for in Articles 53 and 55, and shall regularly monitor and evaluate the achievement of their objectives. The Commission shall publish its assessment of the adequacy of the codes of practice.

<u>Analysis</u>

The edits reduce the Board's influence, which implies reducing member state influence, and shift responsibilities from the AI Office to the Commission. They increase the Commission's ability to overrule member state judgments and unilaterally assess the Codes of Practice.

<u>Recommendation</u>

We recommend that the co-legislators aim to <u>reject</u> the proposed changes shown in the middle and the bottom of the text above, those that change the wording of "The AI Office and the Board" and "They" to "The Commission". These changes would practically eliminate the role and influence of the Board in the assessment and oversight of the Codes of Practices**.** We do not take a position on whether the relevant responsibilities are exercised by the Commission or the AI Office, provided that the Board's role and influence remain unchanged.

(20) Article 60a

<u>Excerpt from Commission proposal for context</u>

We reproduce parts of the proposed new Article 60a below.

3. Member States, the Commission, market surveillance authorities and public authorities responsible for the management and operation of infrastructure and products covered by Union harmonisation legislation listed in Section B of Annex I shall cooperate closely with each other and in good faith, and shall remove any practical obstacles, including on procedural rules providing access to physical public infrastructure, where this is necessary, to successfully implement the voluntary real-world testing agreement and test AI-enabled products covered by Union harmonisation legislation listed in Section B of Annex.

4. The signatories of the voluntary real-world testing agreement, shall specify conditions of the testing in real world conditions and establish detailed elements of the real-world testing plan for AI systems covered by Union harmonisation legislation listed in Section B of Annex I.

5. Article 60(2), (5) and (9) shall apply.';

Analysis

Article 60a introduces a framework for Member States and the Commission to enter agreements for the testing of high-risk AI systems of Section B Annex I. This creates the possibility of testing in the real world AI-powered vehicles, transport, aviation, etc. We believe that key safeguards and interpretive boundaries are unclear:

- Article 60a does not address how the interests and exposure of **non-consenting third parties** (e.g., road users, passengers, residents relying on critical infrastructure) are handled when testing occurs on physical public infrastructure.
- The Article 60a writing and integration with the rest of the AI Act text, particularly its referencing of 60(5), leaves significant doubt on whether it intends to enable only a) testing of e.g. AI based autonomous vehicles on a closed track where all persons at risk have positively consented to the risk, so testing must be according to 60(4)(i), or whether it means to enable also b) testing of such vehicles on the open road while freely mixing with regular road users, so in cases where positive consent from all persons at risk will be impossible to obtain, meaning that 60(4)(i) is no longer required.
- Paragraph 3 empowers authorities to "remove any practical obstacles, including procedural rules providing access to physical public infrastructure." The provision does not delimit which obstacles may be removed, under what criteria, or what procedural guarantees must remain intact (e.g., safety approvals, operational authorisations, consultation rules).
- Paragraph 4 requires a testing plan and paragraph 5 references Article 60(2), (5), and (9). However, the text does not explicitly ensure continuous oversight once the test is live (monitoring, audit access, incident escalation, or clear stop/suspension triggers). This is especially relevant for Annex I, Section B products as they operate in real-world conditions with public exposure.

- It remains uncertain in paragraph 4 if the conditions that need to be specified for the real world test need to be made openly available to the public or not.

Recommendation

We recommend that the co-legislators aim to condition the operation of Article 60a(3) ("removal of obstacles") on minimum procedural safeguards to be included in the agreement and testing plan, and clarify the treatment of third parties, the role of consent, and the degree of public disclosure of the testing plan. On the first part, example add an annex or Article 60a(6) detailing that the testing plan agreed should include, at least:

1. An **impact assessment** covering, health, Safety, fundamental rights, and impacts on the operation of the relevant infrastructure;
2. Measures taken to reduce the exposure, risks and impact on third parties.
3. **Strict scoping** (time, geography, conditions) and **clear stop/suspension criteria**;
4. **Monitoring** obligations, and an incident reporting protocol;

(21) Article 63(1)

Excerpt from Commission proposal for context

Art.63(1) proposal

> '1. SMEs, including start-ups, may comply with certain elements of the quality management system required by Article 17 in a simplified manner. For that purpose, the Commission shall develop guidelines on the elements of the quality management system which may be complied with in a simplified manner considering the needs of SMEs, without affecting the level of protection or the need for compliance with the requirements in respect of high-risk AI systems.';

Analysis

This proposal deletes the sentence "*provided that they do not have partner enterprises or linked enterprises within the meaning of that Recommendation*" included in the current AI Act: this could enable larger companies creating SMEs to benefit from the simplified quality management system (art.17) obligation.

Recommendation

We recommend that the co-legislators aim to keep the sentence "*provided that they do not have partner enterprises or linked enterprises within the meaning of that Recommendation*", **while accepting the change to include SMEs:**

This would mean that the text above would read:

"*1. SMEs, including startups, may comply with certain elements of the quality management system required by Article 17 in a simplified manner,* ***provided that they do not have partner enterprises or linked enterprises within the meaning of that Recommendation.***

For that purpose, the Commission shall develop guidelines on the elements of the quality management system which may be complied with in a simplified manner considering the needs of SMEs, without affecting the level of protection or the need for compliance with the requirements in respect of high-risk AI systems."

(25) Article 75

Excerpt from Commission proposal for context

In the AI Act, article 75(1) reads as follows:

> 1. Where an AI system is based on a general-purpose AI model, and the model and the system are developed by the same provider, the AI Office shall have powers to monitor and supervise compliance of that AI system with obligations under this Regulation. To carry out its monitoring and supervision tasks, the AI Office shall have all the powers of a market surveillance authority provided for in this Section and Regulation (EU) 2019/1020.

The commission proposes major changes and additions to Art.75(1):

> paragraph 1 is replaced by the following:
>
> '1. Where an AI system is based on a general-purpose AI model, with the exclusion of AI systems related to products covered by the Union harmonisation legislation listed in Annex I, and that model and that system are developed by the same provider, the AI Office shall be exclusively competent for the supervision and enforcement of that system with the obligations of this Regulation in accordance with the tasks and
>
> responsibilities assigned by it to market surveillance authorities. The AI Office shall also be exclusively competent for the supervision and enforcement of the obligations under this Regulation in relation to AI system that constitute or that are integrated into a designated very large online platform or very large online search engine within the meaning of Regulation (EU) 2022/2065.
>
> When exercising its tasks of supervision and enforcement under the first subparagraph, the AI Office shall have all the powers of a market

(additional proposed text not included here)

Analysis

The main change we object to is that the AI Office now gets exclusive competences for a broad class of high-risk AI systems, taking these competences away from the national competent authorities.

One of our worries is that, with this change, national authorities can no longer investigate **deployers** who are directly using ChatGPT or other frontier LLMs in their company. This refers to situations where a company relies solely on the generic, publicly available version of the system accessed through the provider's website, rather than a tailored or integrated AI solution. For example, a HR start-up uses the general ChatGPT website interface to upload

all of its candidates data and filter the CVs. This would be the case even in extreme cases where OpenAI has explicitly forbidden the use of ChatGPT for annex III applications. As a result, enforcement responsibility would be shifted to the AI Office for a large number of small scale deployment cases overloading it with work that would be more appropriately handled by National Authorities.

Another worry we have is that the AI Office will simply not have the competence and capacity to deal with complaints that an Annex III high-risk AI system, as created by a provider and/or deployed by a deployer, violates fundamental rights. We foresee that many Annex III high-risk AI systems will be specifically designed to support government bodies or small and medium companies operating inside of a single Member State. To investigate claims that those systems create unfair outcomes, which violate fundamental rights, it will often be required to look specifically at what is considered fair or unfair according to the customs and laws of that Member State. National competent authorities have the competence and knowledge to carry out such assessments in their jurisdiction. By contrast, the proposed changes would place this responsibility at Union level and would also give the AI Office sole responsibility to supervise and enforce AI systems deployed by Member States. We expect that the AI Office would struggle, both in terms of funding and developing sufficient member state specific expertise, resulting in huge backlogs and a detrimental effect on the protection of fundamental rights.

The GDPR demonstrated the pitfalls of concentrating enforcement in a single “lead authority.” For example, if you were a German facebook user and had a complaint, you had to file it before the Irish DPA because the German DPA had no authority (since Facebook's European headquarters is in Dublin, Ireland). The AI Act deliberately corrected this mistake by allowing national authorities to take action even if the provider is based elsewhere. The change to Article 75 re-introduces the same bottleneck.

There is also a possible loophole here where an Annex III high-risk AI system provider can just integrate a small GPAI model into their system, and national authorities would lose competence over supervising them. Finally, because of this enforcement shift it seems to incentivize the use of widely available commercial GPAI over narrow systems. These models are mostly US or China based, going against the EU's plan of encouraging the use of narrow systems developed by EU companies.

In addition to the above exclusivity proposal, (25) part (c) (1c) creates duties and exclusive rights for the Commission to act as a notified body for a small sub-set of high-risk AI systems using biometrics. It is unclear to us whether the Commission is seeking this right, also

because the biometrics functions of a high-risk AI system that happens to include a general purpose AI model may not at all be located inside of that general purpose AI model. If the Commission wants to make an argument that the regular system for creating notified body competences for this particular case is failing, and that the AI Office will need to step in, then it should do so more explicitly.

Recommendation

We recommend that the co-legislators aim to either a) reject the entire proposed change (25) to the AI Act, or to b) make this change based on different wording. The main goal of the co-legislators should be that Annex III high-risk AI system providers can always be investigated by national competent authorities, no matter what technologies they use inside their systems. We consider it useful if the AI office also has investigation and enforcement rights over providers of such high-risk systems if these incorporate GPAI models that meet the Systemic Risks threshold.

For option b) above, we propose the following specific wording (change marking indicated where the wording is different from the Commission omnibus proposal):

(b) paragraph 1 is replaced by the following:

1. Where an AI system is based on a general-purpose AI model **with systemic risk**, with the exclusion of AI systems related to products covered by the Union harmonisation legislation listed in Annex I, and that model and that system are developed by the same provider, the AI Office shall **also** be ~~**exclusively**~~ competent for the supervision and enforcement **towards the provider** of that system with the obligations of this Regulation in accordance with the tasks and responsibilities assigned by it to market surveillance authorities. [The rest of the Commission proposed text under (b) remains as is.]

No matter whether option a) or b) are chosen, we have no strong opinion on keeping part (c) (1c) as an amendment to the AI Act. Given the fact that part (c) (1c) is not well motivated, we are inclined to recommend the co-legislators to reject it.

(31) Article 113

Analysis

The commission proposes a delay of the entry into force of the High-risk AI requirements for the AI Act. Given delays in various preparations needed to enforce these requirements, we believe this is somewhat reasonable. We have no strong opinion on the choice of the exact dates proposed by the Commission.

However, the Commission also proposes a mechanism where it can decide to trigger entry into force earlier than some deadlines. We believe (like many other parties who have commented on the Commission' s proposal) that the existence of this mechanism would create a lot of confusion and uncertainty for parties subject to the Act, having a net negative effect on both the cost of compliance and the timing of when good compliance can be expected to happen. As participants in the JTC21 standards effort in support of the AI Act, we also believe that the introduction of this uncertainty would also have a net negative effect on the operations inside JTC21, potentially leading to further delays.

Recommendation

We recommend that the co-legislators aim to change EC's proposed omnibus article 1(32) text as follows to delete the triggering mechanism:

(31) Article 113

(a) in the third paragraph, point (d) is added:

'(d) Chapter III, Sections 1, 2, and 3, shall apply ~~following the adoption of a decision of the Commission confirming that adequate measures in support of compliance with Chapter III are available, from the following dates:~~

~~(i) 6 months after the adoption of that decision as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and~~

~~(ii) 12 months after the adoption of the decision as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I.~~

~~In the absence of the adoption of the decision within the meaning of subparagraph 1, or where the dates below are earlier than those that follow the adoption of that decision, Chapter III, Sections 1, 2, and 3, shall apply~~:

(i) on 2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and

(ii) on 2 August 2028 as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I.';

(b) in the third paragraph, point (e) is added:

' 3. Articles 102 to 110 shall apply from [the date of entry into application of this Regulation].';

2. Proposals for additional targeted amendments to the AI Act

The digital omnibus process offers an opportunity for all co-legislators to amend specific provisions of the AI Act. In this section we put forward a very curated set of targeted amendments, not included in the Commission proposal, that would address a few key shortcomings of the AI Act.

2.1 On the exemption for models developed purely for scientific research and development in AIA Article 2(6)

Proposal:

We propose amending Article 2(6) to clarify that the scientific research and development exemption ceases to apply where an AI model or system is subsequently placed on the market or put into service for non-research or commercial purposes, whether by the original developer or by a third party.

We propose that the co-legislators seek to amend Article 2(6) as follows:

> "6. This Regulation does not apply to AI systems or AI models, including their output, that are specifically developed and put into service solely for the purpose of *scientific research and development* **and used exclusively in a controlled research environment. Where such an AI system or AI model is subsequently placed on the market or put into service for purposes other than scientific research and development, the actor performing such placement or putting into service shall be considered the provider for the purposes of this Regulation and shall be subject to its obligations.**

Along with the above we propose that the co-legislators seek to disambiguate further by adding a definition of scientific research and development by amending Article 3 as follows:

> 3(69) 'scientific research and development' means systematic activity aimed primarily at generating generalisable knowledge or advancing the state of the art, conducted in accordance with a research protocol and with an intention to disseminate results in the public interest, and which is not aimed at developing or improving a product or service for commercial deployment.

[This definition is inspired by the OECD Definition of R&D, adapted to the AI Act language, context and specific legal objective.]

Explanation:

Article 2(6), Recital 25, and Recital 109 are intended to promote innovation that serves the public interest by safeguarding genuine scientific research and development and promoting open science. This objective is legitimate and should be preserved.

However, the current wording risks creating an **overly broad and easily exploitable exemption**. As drafted, it doesn't sufficiently distinguish between research conducted in the public interest and model development that is effectively oriented toward future commercial deployment. This creates the risk that companies may use the scientific research exemption to avoid compliance obligations that should apply to them as commercial actors in the internal market.

A particularly concerning risk is **"open-science washing"**: situations where private entities initially frame model development as purely scientific, benefit from regulatory exemptions, and later commercialise the same models once they have achieved scale, market penetration, or societal relevance. In such cases, the exemption would function not as a temporary safeguard for research, but as a mechanism to delay or bypass regulatory oversight.

This risk is not theoretical. Broad exemptions under research purposes have been exploited before for commercial reasons in other digital regulations. In the recent ***LAION v Kneschke*** German court ruling[1], LAION, a dataset provider, scraped Kneschke's content, even though Kneschke had enforced his right to opt-out (in accordance with Art. 4 of the Digital Single Market Directive). **LAION was deemed to be not-for-profit despite the fact that LAION's dataset had been used by Stable Diffusion, a commercial AI provider, to train one of its models following a paid collaboration agreement with LAION**. The effect of LAION being categorised as a not-for-profit entity led to the opt-out right being unenforceable under a "research" exception created by the DSM Directive. This illustrates how formal research labels can mask de facto commercial exploitation.

Finally, to avoid accountability gaps, the AI Act should clarify that where a research model is later put into service for non-research or commercial purposes, the actor that carries out that deployment assumes the role of provider and the full set of obligations under the AI Act.

2.2 On the Classification rules for Annex I high-risk AI systems in AIA Chapter III Article 6(1):

Proposal

To prevent unwanted over-reach in classifying products which have non-safety-critical AI functions only (e.g. smart phones, watercraft built-in voice activated entertainment systems) as being Annex I high-risk AI systems, we propose amendments to Article 6(1) as follows:

1. Irrespective of whether an AI system is placed on the market or put into service independently of the products referred to in points (a) and (b), that AI system shall be

[1] https://www.euipo.europa.eu/en/law/recent-case-law/germany-hamburg-district-court-310-o-22723-laion-v-robert-kneschke

considered to be high-risk where ~~both~~ **all three** of the following conditions are fulfilled:

(a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I;

(b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I~~.~~**;**

(c) the AI system is itself a product covered by the Union harmonisation legislation listed in Annex I, and its design is such that, when the system is used in accordance with its intended purpose, or under conditions of reasonably foreseeable misuse, the failure or malfunctioning of

i) a system component performing inference, or
ii) a system component that performs a safety function by processing inputs to, or outputs from, a system component performing inference,

will endanger the health and safety of persons or property, or the fundamental rights of persons.

Comments and justification

We believe that Article 6(1) in its current form creates too high of an administrative burden on many companies, by incorrectly classifying many products as high-risk AI systems, even though these products do not in fact pose any significant AI related threats to health, safety, or fundamental rights. This incorrect over-classification of products as high-risk AI systems triggers, among other, documentation and reporting obligations which are unnecessary. We would like the omnibus package to fix Article 6(1), by amending the classification scheme.

The root cause of the problem is that the Article 6(1) classification logic contains no test on whether a product that is also an AI system has any AI-based components that work as safety components. Products (e.g. modern smart phones) that contain AI components with no safety functions at all will be classified as AI systems under the very broad AI system definition in Article 3(1), and then as high-risk AI systems because they are subject to some form of third party conformity assessment under at least one Annex I regulation (in case of a smart phone, this would be the radio equipment directive).

We believe that this over-classification problem cannot be fixed by just relying on soon to be published ‘guidelines specifying the practical implementation of this Article’ as considered in Article 6(5), as such guidelines cannot overrule the faulty logic in Article 6(1).

We recommend that the omnibus package amends Article 6(1) to include an explicit test that the AI product in question actually has safety-critical AI-based or AI-related

functions inside that, if they fail, can be a threat to health, safety, or fundamental rights.

Our specific proposal approaches this test by leveraging the fact that in the AI Act, the defining difference between AI and non-AI systems is that only AI systems are capable of 'inference'. E.g. recital (12) says that 'the capacity of an AI system to infer transcends basic data processing'. The exact interpretation of 'inference' further grounded by the guidelines published by the Commission at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application. Our proposed new text was written to align with the logic of other parts of the AI Act, using phrasings from the definition of 'safety component' and from Article 9.

2.3 On aligning the AI Act incident reporting with recent EU safety frameworks and International Standards

Proposal:

Amend the end of Article 3(49) of the AI Act to **explicitly include near-miss events.**

Article 3(49) 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**,**
> **or an incident or malfunctioning of an AI system that had a significant potential to lead to any of (a)-(d) above.**

Explanation

The AI Act definition of "serious incident" **requires a direct or indirect link to an actual harm**. This results in that events which clearly demonstrate dangerous system behaviour, but do not yet result in death, injury, rights violations, or property damage, **fall outside the reporting obligation**.

For example, under the current wording, an explosion or catastrophic malfunction caused by an AI system that does not result in casualties or material damage would not trigger a reporting obligation. This makes Article 3(49) different from recent safety EU frameworks and international standards which do include incident reporting obligation for potential harms and near-miss events eliminating any anticipatory or preventive reporting logic:

- **ISO/IEC 27035-1:2016** defines an information security incident as:
  "*One or multiple related and identified information security events that can harm an*

organization's assets or compromise its operations."

- **ISO 22301:2019** defines an incident as:
  "*Event that can be, or could lead to, a disruption, loss, emergency or crisis.*"

- **Medical Device Regulation (EU) 2017/745** defines an incident as:
  "*Any malfunction or deterioration in the characteristics or performance of a device… as well as any inadequacy in the information supplied by the manufacturer…*"

- **Critical Entities Resilience Directive (EU) 2022/2557** requires notification of incidents that **"significantly disrupt or have the potential to significantly disrupt"** essential services, and defines an incident as:
  "*an event which has the potential to significantly disrupt, or that disrupts, the provision of an essential service.*"

The current AI Act also stands in contrast with the OECD AI framework which was has been explicitly referenced as an inspiration for the AI act reporting obligations as it omits a central OECD concept, **'**AI hazards**'** which recognises that certain system failures create plausible risks of serious harm, even if those harms have not yet occurred.

> "*an event, circumstance or series of events where the development, use or malfunction of one or more AI systems could plausibly lead to an AI incident.*"

Finally, the exclusion of potential harms is particularly concerning from an enforcement and evidence perspective. In cases of alleged non-compliance, demonstrating a failure to report will require proof not only that a malfunction occurred, but that the provider knew or should reasonably have known not only about the incident itself but that such incident had already resulted in concrete harm. In practice, this creates a high evidentiary threshold for authorities.

As a result, providers may be able to avoid reporting, and subsequent scrutiny, even when they are aware of serious system failures, by claiming uncertainty as to whether those failures actually caused harm or claiming they were not aware users had been affected. In many scenarios, establishing a clear causal link ex-post will be difficult or impossible, effectively allowing significant risks to remain unreported until damage materialises.