Date: Apr 16, 2026 at 11:53 pm

Source: https://aipolicylab.se/aipex/

Rethinking the Digital Omnibus' Impact on the EU AI Act: Simplification or Dilution?

Rachele Carli, rachele.carli@umu.se
Tatjana Titareva, tatjana.titareva@umu.se
Virginia Dignum, virginia.dignum@umu.se

Introduction

The adoption of the European Union AI Act (hereafter AI Act) marks a milestone in the union's ambition to shape trustworthy, human-centric artificial intelligence (AI). It reflects an effort to ground innovation in fundamental human rights – an approach that has positioned the EU as a global standard-setter in digital regulation. The proposed Digital Omnibus represents an effort to streamline and harmonise an increasingly complex regulatory landscape.

However, as the Digital Omnibus Regulation Proposal directly affects the implementation of the AI Act and related data governance frameworks, it raises a number of critical cross-cutting concerns. In particular, certain simplification measures – introduced with the intention to reduce administrative burdens, facilitate compliance procedures, and improve regulatory coherence – may have unintended consequences on the consistency, traceability, and risk-sensitivity of the EU's digital regulatory ecosystem. These include potential reductions in the consistency of regulatory application, limitations in the traceability of data and AI systems, and a weakening of the granularity required for effective risk assessment within the EU's digital framework. Moreover, while these measures are designed to ease obligations for AI providers and developers, they may have the effect of shifting complexity downstream onto deployers and end-users. This could result in increased uncertainty for those responsible for the use of AI systems in practice, particularly in high-risk contexts where clear allocation of responsibilities and robust risk assessment remain essential.

These interactions are especially relevant where data processing rules, access to large-scale datasets, and incident reporting mechanisms intersect with the criteria used to assess and classify high-risk AI systems. Ensuring that these instruments remain coherent in their application is therefore essential to preserving both the safeguards and the credibility of the EU's risk-based approach.

In this context, the AI Policy Lab at Umeå University seeks to contribute constructively to the ongoing discussion by highlighting specific areas of concern and putting forward targeted

recommendations. The main objective is to ensure that the EU's regulatory ecosystem remains both effective and future-proof.

1. Amendments to the GDPR for AI training, Article 3 of the Digital Omnibus proposal

The Digital Omnibus proposal introduces clarifications regarding the legal bases and conditions under which personal data may be processed for the development and training of AI systems. In particular, it elaborates on the use of *legitimate interest* as a legal basis and introduces specific derogations for the processing of special categories of data (i.e., sensitive data such as health, biometric, or political information).

While these changes primarily concern data protection law, they have indirect but significant implications for the application of the AI Act – especially Article 6, which governs the classification of high-risk AI systems. This is due to the fact that the scope, nature, and volume of data used in training are key elements in assessing the risks associated with AI systems.

Several aspects of the proposal may inadvertently weaken the link between data governance and AI risk classification:

- The introduction of derogations for the processing of so-called "residual" sensitive data during model training (§33) risks expanding the volume of sensitive data that can be used without prior scrutiny. This could reduce the ability of regulators to accurately assess whether an AI system should be classified as high-risk under Article 6 of the AI Act.
- The broadening of legal bases for data processing in the context of AI training (§§30-31) may weaken the connection between the actual risks posed by a system and its regulatory classification, particularly in the absence of coordinated interpretative guidelines between data protection authorities – such as the European Data Protection Board (henceforth EDPB) – and AI governance bodies – such as the AI Office.
- The simplification of transparency obligations, including information notices and Data Protection Impact Assessments (henceforth DPIAs) (§36, §40), may reduce the level of detail available to regulators. This, in turn, could hinder a proper assessment of whether a system meets the criteria for high-risk classification.

Our Recommendations:

1. Introduce a specific notification requirement for AI models trained using the "residual sensitive data" exemption (§33) to preserve traceability of training datasets and support risk classification under the AI Act.

2. Provide a DPIA section dedicated to AI systems. This could help preventing the simplification of DPIA (single EU lists) from reducing the granularity necessary to assess AI risk.

2. Prevent the merger of the Data Act, Digital Governance Act, and Open Data Act from creating "shortcuts" for high-risk AI systems

The Digital Omnibus seeks to consolidate several existing legislative instruments – the Data Act, the Data Governance Act (henceforth DGA), and the Open Data Directive – into a single, more coherent framework governing access to and reuse of data, including data held by public authorities. This consolidation is intended to facilitate access to large datasets, including non-personal data, and to promote data sharing across sectors. While this can significantly support innovation and the development of AI systems, it may also have implications for how such systems are classified under the AI Act. Among these, it is important to highlight the following:

- Easier access to large volumes of data – including datasets that can be combined or enriched – risks enabling the development of AI systems whose purpose or context of use would place them within the scope of Article 6 of the AI Act (high-risk AI systems).
- There is a risk that the simplification of data access mechanisms could be interpreted, in practice, as a justification for lowering the perceived risk level of such systems. In other words, increased data availability risks inadvertently being used as an argument to downgrade regulatory scrutiny.

Our Recommendations:

1. Clearly establish that simplified access to data does not affect the criteria for high-risk classification under the AI Act. The availability of data should not be considered a mitigating factor in the assessment of risk.
2. Introduce an *ex ante* assessment requirement for cases where public or publicly accessible data is reused for AI systems that are likely to operate in high-risk domains (such as employment, education, healthcare, or access to essential services).
3. Require public administrations, when authorising the reuse of data for AI development, to explicitly indicate whether the intended use is likely to fall within the scope of Article 6 of the AI Act. This would provide greater legal clarity for developers and strengthen regulatory consistency.

3. Single-entry point for incident reporting (Article 6 and 9 of the Digital Omnibus proposal)

The proposal to establish a single European entry point for incident reporting constitutes a significant step towards simplifying and harmonising reporting obligations across multiple

regulatory frameworks, including NIS2 (cybersecurity), GDPR (data protection), DORA (financial sector resilience), eIDAS (digital identity), and the Critical Entities Resilience (CER) Directive. By centralising notifications through a platform managed at the EU level – specifically by the European Union Agency for Cybersecurity (ENISA) – the proposal aims to reduce administrative burdens for operators and improve the efficiency of information sharing across authorities.

However, the centralisation of notifications on a single platform managed by ENISA raises some critical issues that deserve careful consideration (in order to ensure the effectiveness of the system and the protection of operators subject to reporting obligations):

- Expanding ENISA's mandate to manage a unified reporting platform may lead to capacity constraints, given the anticipated volume of notifications. Any delays in processing or triaging reports could negatively affect incident response times and overall system resilience.
- The single-entry point is designed as a hub rather than a replacement for Member States' national competent authorities. However, without seamless technical and procedural interoperability with existing national systems, there is a risk of duplication, inefficiencies, or increased administrative complexity.
- The proposal does not sufficiently clarify the allocation of responsibilities between operators, ENISA, and national authorities in cases of system malfunction, delays, or errors. This lack of clarity risks exposing operators to legal consequences for circumstances beyond their control.
- The centralisation of incident-related data at the EU level also raises questions regarding data governance and technological sovereignty. In the absence of clear guarantees on data localisation, secure infrastructure, and Member State oversight, there is a risk that sensitive operational information – potentially critical for national security – may be insufficiently protected or subject to dependencies on non-EU technological backbones.

Our Recommendations:

1. Establish an independent annual audit mechanism to assess the functioning of the single-entry point. This audit should evaluate: (i) the system's capacity to handle notification volumes, (ii) the timeliness and accuracy of information processing, (iii) the cybersecurity of the platform, and (iv) its level of interoperability with national systems. Such an audit would help to ensure transparency, reliability and continuous improvement of the system.
2. Introduce a mandatory fallback protocol to be activated in the event of technical unavailability. This should include: (i) alternative reporting channels, (ii) clear criteria for demonstrating compliance efforts by operators, and (iii) automatic suspension of

notification deadlines during system outages. This would prevent operators from incurring violations due to circumstances beyond their control.

3. Clarify the liability framework by explicitly defining the division of responsibilities between ENISA, national authorities, and reporting entities. This should specify: (i) situations in which failures are attributable to the central system, (ii) the implications for operators' legal obligations, and (iii) the safeguards available in cases of technical malfunction. Clear and predictable rules are essential to ensure legal certainty and the consistent application of reporting obligations across the European Union.
4. Introduce explicit requirements ensuring that the infrastructure supporting the single-entry point is based on secure, EU-controlled technological backbones, with clear provisions on data localisation, access control, and Member States' oversight. This could include, for instance, reliance on trusted European cloud frameworks or "no non-EU backbone" requirements for particularly sensitive categories of incident data. Such safeguards would strengthen trust in AI systems and ensure alignment with broader EU objectives on digital sovereignty.

Conclusion

Overall, the Digital Omnibus proposal reflects a necessary and timely effort to streamline an increasingly complex regulatory framework and to facilitate its practical implementation across sectors. At the same time, the analysis above highlights the importance of maintaining a careful balance between simplification and regulatory integrity. Across the areas examined – namely **AI training data governance, access to public** and **non-personal data, and incident reporting mechanisms** – there is a common need to **preserve traceability**, **ensure risk-sensitive oversight**, and **safeguard legal certainty**, while also reinforcing the Union's strategic autonomy. The recommendations above by the AI Policy Lab at Umeå University are intended to support this balance by addressing specific gaps and ambiguities without undermining the overall objectives of the proposal. In doing so, they aim to contribute to a coherent, robust, and future-proof EU regulatory framework for AI and the data economy.

References

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333, 27.12.2022, p. 80–152.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER), OJ L 333, 27.12.2022, p. 164–198.

Date: Apr 16, 2026 at 11:53 pm

Source: https://aipolicylab.se/aipex/

Proposal for a Regulation of the European Parliament and of the Council establishing a Digital Omnibus for the simplification of Union digital legislation, COM(2025) XXX final.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services (eIDAS), OJ L 257, 28.8.2014, p. 73–114 (as amended).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR), OJ L 119, 4.5.2016, p. 1–88.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA), OJ L 333, 27.12.2022, p. 1–79.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 12.7.2024.