

DIGITAL OMNIBUS SIMPLIFICATION MUST NOT BE TOOL FOR DEREGULATION

***Liberties' Response
to the European Commission's
Digital Omnibus Simplification
Agenda Call for Evidence***

TABLE OF CONTENTS

Introduction	3
Data Protection and Privacy	3
Artificial Intelligence Act	4
Calls to “stop the clock” must be rejected out of hand	5
Simplification must not be used as a tool for Article 6 derogation	6
Create robust fundamental rights impact assessments	7
Uphold Article 50 transparency requirements	7
Enforce existing Article 73 reporting requirements	8
Conclusion	9
Contact	10

Introduction

In recent years, the EU has passed several landmark laws that regulate the digital ecosystem and aim to protect both fundamental rights and EU values. During the previous parliamentary term, legislators updated the Union's rules for online platforms, with the Digital Services Act (DSA); for fair online competition and against digital gatekeepers, with the Digital Markets Act (DMA); and for the use of artificial intelligence, with the AI Act (AIA). And the General Data Protection Regulation (GDPR), despite its imperfections, is still the gold standard for data protection worldwide. It inspired new legislation across the globe and serves as a robust *lex generalis* for the EU, establishing high standards of data protection and providing safeguards against privacy violations by technology companies and third countries.

Liberties has joined other civil society organizations to support the EU's aim to pass stronger safeguards for fundamental rights, digital rights and EU values. However, the Digital Omnibus simplification process poses grave risks to fundamental rights and EU values. We are greatly concerned that it will result in protections being weakened, standards being diluted, and loopholes being widened in the name of "competitiveness." In short, we worry that the simplification process will instead become a deregulation process.

Instead of dismantling the EU's digital safeguards, the Commission should recognize that robust protection of fundamental rights and democratic values is not a burden but a foundation for sustainable innovation and public trust. Strong accountability rules make societies safer, fairer, and more resilient. The EU's credibility as a global leader in rights-based tech governance depends on upholding these principles rather than yielding to short-term commercial pressures.

Data Protection and Privacy

Data protection and privacy rules require stronger enforcement and better coordination between data protection authorities, not a "simplification" exercise. While part one of the Digital Omnibus focuses on non-personal data flow, its proposed "simplification" measures risk undermining the General Data Protection Regulation. We agree with the European Data Protection Board (EDPB) when it refers to potential "modifications to the GDPR to simplify and clarify the obligation to keep a record of processing are targeted and limited in nature and do not affect the core principles and other obligations under the GDPR" and their support to clarify in the recitals that a record of processing would only be mandatory for those processing activities "likely to result in a high risk".¹

1 European Data Protection Board (EDPR), *Joint Opinion 01/2025 on the Proposal for a Regulation on simplification measures for SMEs and SMCs, in particular the record-keeping obligation under Art. 30(5) GDPR* (July 9, 2025), available at: https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-012025-proposal_en.

We further agree with the EDPB and the European Data Protection Supervisor (EDPS) that this change would avoid the misunderstanding that a record of *all processing activities* is mandatory from the moment at least one of these processing activities is likely to result in a high risk. We also share their concerns on the newly proposed threshold that would only include companies employing more than 750 persons, removing record-keeping obligations for many companies based solely on their size.

Part two of the Digital Omnibus claims to only address cookie banners under Article 5(3) of the ePrivacy Directive. However, this paragraph is a foundational element of EU digital rights law, safeguarding individuals from arbitrary or disproportionate state or commercial surveillance in numerous contexts. With the ePrivacy Directive being the main piece of legislation tackling privacy and confidentiality of communications, and with the withdrawal of the ePrivacy Regulation (the much-needed update of the Directive), the EU is sending the signal to corporations and to politicians that our rights are open for negotiation. We regret that the Digital Omnibus minimizes this, given its central role in the right to privacy enshrined by the EU Charter. We find it surprising that the call for evidence suggests no negative fundamental rights consequences

from the Digital Omnibus despite strong evidence to the contrary.

Artificial Intelligence Act

The fourth part of the Omnibus considers amendments to the EU's AI Act, despite the nascent nature of its implementation and enforcement. Although the Act should have gone further in protecting fundamental rights, such as strongly prohibiting – without exceptions – the use of facial recognition technologies in publicly accessible spaces, as Liberties argued for,² it is still one of the most significant pieces of EU legislation in regulating the use of AI and protecting fundamental rights from AI's harms. The AIA offers certain provisions for AI system developers, providers and users that are necessary to mitigate bias and harm, to enhance transparency and accountability, and to ensure compliance with EU fundamental rights. Any delay or reduction in the AI Act's protections would introduce legal uncertainty and penalize providers committed to upholding fundamental rights.³

Although having clear, logical and easily followable laws sounds advantageous, the end result of the simplification process is fewer checks on businesses, wider loopholes to skirt regulation, and weakened protections for fundamental

2 Jonathan Day, Karolina Iwańska, Eva Simon, & Kerttu Willamo, *Packed with Loopholes: Why the AI Act Fails to Protect Civic Space and the Rule of Law* (April, 2024), available at: <https://www.liberties.eu/f/hjoz6a>.

3 European Digital Rights (EDRi), *Open Letter: The European Commission and Member States must keep AI Act national implementation on track* (September 23, 2025), available at: <https://edri.org/our-work/open-letter-european-commission-member-states-keep-ai-act-national-implementation-on-track/>.

rights. Liberties is greatly concerned that this is the future of the AI Act. Despite the critical importance of the AIA's fundamental rights protections, certain articles and elements of the Act are being targeted for simplification in a way that would pose grave threats to fundamental rights and render essentially meaningless many of the protections spelled out in the Act. We wish to draw attention to some of these threats and urge the Commission to not yield to industry or political pressure where the end result of simplification would weaken the law's fundamental rights protections.

Calls to “stop the clock” must be rejected out of hand

While the Commission's latest position, as reported in the media,⁴ appears to be that there will be no “stop the clock” delay of the AI Act's implementation, the simplification process provides another opportunity for AI deployers and providers, among others, to push for such a delay. Some business-sector groups are even calling for a 24-month pause.⁵ We therefore urge the Commission to maintain its firm commitment to the timely and uninterrupted implementation and enforcement of the Act, on schedule with what is elaborated in the Act

itself. Such a delay would also mean a delay of the fundamental rights protections provided by the law at the same time as potentially many AI systems are developed and put to market without deference to AI Act standards or the application of oversight and assessment mechanisms, such as a fundamental rights impact assessment, that are required by the AIA.

It is also important to consider that current calls to delay the AI Act follow a legislative process that was already heavily influenced by industry lobbying. Namely, critical implementation processes, such as the standardisation process⁶ and the GPAI Code of Practice,⁷ have been roundly criticized by fundamental rights and digital rights groups for being heavily influenced by industry representatives. Therefore, current calls to “stop the clock” because of certain standards not being available in time is both regrettable and frustrating, as industry actors are those mainly responsible for delaying this process. Standards and clear guidelines must continue to be adopted in concert with the implementation and enforcement of the Act so as not to risk leaving the fundamental rights protections of the law toothless.

4 Cynthia Kroet, *EU Commission rebuffs calls to press pause on AI Act* (Euronews, September 22, 2025), available at: <https://www.euronews.com/next/2025/09/22/eu-commission-rebuffs-calls-to-press-pause-on-ai-act>.

5 Bitkom, *AI Act Simplification: For Innovation and Feasibility* (June 2025), available at: <https://www.bitkom.org/sites/main/files/2025-06/bitkom-publication-ai-act-simplification.pdf>.

6 Corporate Europe Observatory, *Bias Baked into AI Act: How the EU's AI Regulation Could Undermine Democracy* (January 9, 2025), available at: <https://corporateeurope.org/en/2025/01/bias-baked>.

7 Corporate Europe Observatory, *Coded for Privileged Access: How Big Tech Influenced the EU's AI Code of Practice* (April 30, 2025), available at: <https://corporateeurope.org/en/2025/04/coded-privileged-access>.

Simplification must not be used as a tool for Article 6 derogation

Article 6 of the AI Act, which regulates high-risk artificial intelligence systems, is one of the most critical elements of the Act when it comes to protecting fundamental rights and EU values. It is imperative that the simplification process is not used as a tool to weaken, waterdown, or otherwise derogate the higher standards for high-risk AI systems, and the safeguards mandated under Article 6 or supporting articles, such as Article 27. Getting the simplification process right is particularly important for Article 6 in part because it contains extremely complex, industry-specific language.⁸

For example, consider the conditions that determine whether an AI system listed in Annex III may not be considered high-risk. The criteria for classifying AI systems as “high-risk” under Article 6(1) are multi-pronged: “(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 harmonization legislation listed in Annex I; (b) the AI system, when placed on the market or put into service, undergoes conformity assessment by a third party pursuant to the Union harmonisation legislation referred to in point (a).”

One must understand the concept of “Union harmonisation legislation” as well as the

processes of “conformity assessment” in order to fully grasp the meaning of this classification standard. Moreover, the recent guidelines from the Commission meant to facilitate effective application and enforcement of the AI Act do not offer specific clarifications or detailed explanations in this area. Although Annex III is mentioned in relation to high-risk areas, the relevant guidelines lack specific guidance on interpreting key terms, such as “narrow procedural task,” or how an AI system “improves” a human activity to qualify for an exemption from the high-risk classification.

If exemptions to the ‘high-risk’ classification are expanded through the simplification process and the idea of “material influence” is weakened, systems that indirectly shape decisions, such as ranking, recommendation, or scoring tools—could avoid proper oversight. Scholars have already noted that the current classification rules may be too limited, leaving out systems that should arguably fall under the high-risk category. For example, these conditions and limitations may make the scope of ‘high-risk’ too narrow,⁹ reducing the Act’s overall effectiveness. Further simplification that removes or weakens the need to justify exemptions would also make the process less transparent and reduce accountability.

8 Theodoros Karathanasis, *The AI Act: Balancing Implementation Challenges and the EU’s Simplification Agenda* (May 01, 2025), available at SSRN: <https://ssrn.com/abstract=5311501>.

9 Emilija Leinarte, *The Classification of High-Risk AI Systems Under the EU Artificial Intelligence Act*, Lexxion, Vol. 1 (2024) No. 3, pp.262-280, <https://doi.org/10.21552/aire/2024/3/4>.

Create robust fundamental rights impact assessments

The Commission must resist calls to weaken or even remove the requirement that high-risk systems undergo fundamental rights impact assessments (FRIAs). Despite the clear requirement for FRIAs under Article 27 of the AI Act, industry sources are nevertheless using the simplification process to call for derogation of Article 27.¹⁰ The mandatory FRIA under Article 27 exists to ensure that all high-risk AI systems deployed in the EU do not risk violating fundamental rights and the protections explicitly enshrined in the AI Act. In order to do so, the Commission needs to not only keep them, but to involve civil society in formalizing a template for FRIAs that is stringent enough to fulfill the objective assessments' objective of protecting fundamental rights.

Industry representatives point to overlapping impact-assessment requirements,¹¹ i.e. those required by the AI Act and those required by Article 35 of the General Data Protection Regulation (GDPR).¹² The FRIA for AI systems should not be removed or derogated simply because a different EU law requires a different impact assessment; the AIA FRIA will

be distinct from that required by the GDPR in both form and scope, and therefore, performing one should not exempt AI deployers from the other. Furthermore, calls to remove the obligation to notify authorities,¹³ as stipulated by Article 27(3) of the AI Act, simply because DPIAs under the GDPR do not have such a mandatory notification requirement, should be rejected.

Uphold Article 50 transparency requirements

The Commission has recently closed its feedback period for the code of practice on transparent generative AI systems. The AI Act's transparency requirements, primarily elaborated in Article 50, but also elsewhere (e.g. Article 13), are fairly seen as lacking clarity that will be provided by the finalized guidelines. Nevertheless, Article 50 does establish a number of key transparency requirements, such as that deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake must disclose that the content has been artificially generated or manipulated (Article 50(4)), and that deployers of an emotion recognition system or a biometric categorization system must

10 Bitkom, *AI Act Simplification: For Innovation and Feasibility* (June 2025).

11 Business Europe, *Simplifying the EU Digital Rulebook: Clarity, Simplicity, and Agility for Competitiveness* (July 17, 2025), available at: <https://www.buinesseurope.eu/wp-content/uploads/2025/07/2025-07-17-BusinessEurope-Paper-Simplification-of-the-Digital-Rulebook.pdf>.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

13 Bitkom, *AI Act Simplification: For Innovation and Feasibility* (June 2025).

inform all natural persons exposed to of the operation of the system, and shall process all personal data in accordance with the GDPR, Regulation (EU) 2018/1725 and the Law Enforcement Directive, among other critical transparency requirements.

It is crucial that there is no lag in the enforcement of these requirements, and that there is no derogation that could allow deployers to skirt them in cases clearly intended to be covered by the AIA. These requirements provide transparency that is necessary for consumers of AI-generated content or those who use certain AI systems to be fully informed of what they are being exposed to, and industry calls to postpone the applicability of these transparency requirements¹⁴ must be rejected.

Enforce existing Article 73 reporting requirements

Article 73 of the AIA covers the process for reporting “serious incidents” in the use of high-risk AI systems. This article serves multiple critical aims, including: creating an early-warning system that allows market surveillance authorities to identify harmful uses or flag potential risks of high-risk AI systems at an early stage; establishing accountability for providers of high-risk systems, ensuring that they take responsibility for the proper functioning and safety of their products; enabling market surveillance authorities to take action

and implement corrective measures in a timely manner to minimize the damage done when serious incidents do occur; and creating transparency in how these systems are used, which will help build public trust.

The reporting process set down by Article 73 must therefore be fully supported by the Commission and not subject to derogation through simplification. Calls by tech industry groups¹⁵ to remove Article 73 requirements by “streamlining” them with the reporting requirements of Articles 33 (notification of data breaches to supervisory authority within 72 hours) and Article 34 (in cases likely to result in a high risk to fundamental rights, also to the data subject) of the GDPR should be resisted. The inclusion of these requirements in the AIA was done for good reason, and the burden to report a serious incident involving high-risk AI to all relevant regulatory bodies – as when Member States have designated different regulatory authorities under each law – should fall on the providers, rather than be devolved to rely on regulatory bodies’ communication with each other, or between different offices within the same body.

¹⁴ *Ibid.*

¹⁵ ITI, *Simplifying the EU's Tech Rulebook* (July 2025), available at: <https://www.itic.org/documents/europe/EUSimplificationPaper.pdf>

Conclusion

The Digital Omnibus simplification process poses serious risks to fundamental rights and EU values. We are greatly concerned that it will result in fundamental rights protections that have been rendered toothless by weakening standards and widening loopholes in order to satisfy the desires of Big Tech. Instead, the Commission should recognize that strong protections for fundamental rights and EU values actually make society safer, more productive and better positioned to flourish. The modest protections for fundamental rights that made their way into EU digital legislation must remain fully intact, supported by processes and mechanisms that are not eroded or blunted for the sake of “competitiveness.”

Finally, we wish to express our disappointment with the flawed process of this call for evidence. It is now just less than two months until the Digital Omnibus proposal is scheduled, giving decision-makers little time to properly consider the arguments and warnings from civil society organizations, individual experts and others who flag significant threats to fundamental rights. Such a brief period for review strongly suggests that this call for evidence is little more than a box-ticking exercise in the guise of a proper consultation. We urge the Commission to give due consideration to the concerns raised herein, and to complete this simplification process in a way that prioritizes fundamental rights and EU values over purely commercial interests.

Contact

The Civil Liberties Union for Europe

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of 21 national civil liberties NGOs from across the EU.

c/o Publix, Hermannstraße 90

12051 Berlin

Germany

info@liberties.eu

www.liberties.eu