Converted reading copy — not an official PDF

Opinion of the European Economic and Social Committee on a) Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) (COM(2025) 836 final — 2025/0359 (COD)) and b) Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 and Directive (EU) 2019/1024 (Digital Omnibus) (COM(2025) 837 final — 2025/0360 (COD))

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025AE3929

Official HTML retrieved 2026-09-10. Converted 2026-09-10. The document text, tables and links are reproduced from the captured English HTML. Pagination and layout are newly generated; the decorative EU emblem is omitted. Consult the official source for the authentic publication and current status.

Official Journal of the European Union

EN

C series

C/2026/3225

2.7.2026

Opinion of the European Economic and Social Committee

a) Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

(COM(2025) 836 final – 2025/0359 (COD))

and

b) Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 and Directive (EU) 2019/1024 (Digital Omnibus)

(COM(2025) 837 final – 2025/0360 (COD))

(C/2026/3225)

Rapporteur:

Heiko WILLEMS

Co-rapporteur:

Angelo PAGLIARA

Advisors

Polina KHUBBEEVA (to the rapporteur)

Silvia BORELLI (to the co-rapporteur)

Legislative procedures	(a) EU Law Tracker (b) EU Law Tracker
Referrals	(a) European Parliament, 5.12.2025 Council of the European Union, 3.2.2026 (b) European Parliament, 18.3.2026 Council of the European Union, 3.2.2026
Legal basis	(a) Article 114 of the Treaty on the Functioning of the European Union (b) Article 114 of the Treaty on the Functioning of the European Union
European Commission documents	(a) COM(2025) 836 final – 2025/0359 (COD) (b) COM(2025) 837 final – 2025/0360 (COD)
Relevant Sustainable Development Goals (SDGs)	SDGs 8 and 9
Section responsible	Single Market, Production and Consumption
Adopted in section	11.2.2026
Adopted at plenary session	18.3.2026
Plenary session No	604
Outcome of vote (for/against/abstentions)	194/0/0

1. RECOMMENDATIONS

THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE (EESC)

1.1. The European Economic and Social Committee (EESC) takes note of the Commission's objective to simplify the digital rulebook in order to 'bring immediate relief to businesses, public administration and citizens alike'. The Digital Omnibus and AI Omnibus should foster a dynamic, fair and sustainable digital economy that benefits businesses, workers, consumers and society at large. Europe must strengthen its innovation capacity and global competitiveness by streamlining administrative processes, eliminating duplicative obligations or – where necessary – additional national requirements undermining the single market and ensuring consistent interpretation of digital regulations across the Member States. At the same time it must maintain essential and relevant frameworks of the GDPR and the AI Act, ensuring a high level of fundamental rights protection as well as the freedom of natural persons, in particular their right to privacy with respect to the processing of personal data, as enshrined in Article 8(1) of the Charter and Article 16(1) TFEU.

1.2. The proposed simplifications are a first step in the right direction. Further measures should be envisaged during the upcoming 'Digital Fitness Check'. All simplification measures should be developed and implemented in partnership with companies, workers, consumers, the scientific community, NGOs and civil society, respecting the better regulation principles, including the impact assessment, where appropriate. These measures must reduce legal uncertainty and administrative burden, reinforce Europe's competitiveness and sovereignty, ensure a level playing-field and uphold high social, environmental and consumer standards to ensure a fair and inclusive single market.

1.3. Outdated and overlapping rules can be repealed without lowering standards. Clarification provides legal certainty for everyone and reduces the risk of lengthy and costly litigation. In particular, the EESC calls for clear definitions of 'personal data', 'data holder', 'user', 'data processing service' and 'placing on the market' across all relevant acts. Moreover, where conflicts arise, safety and security legislation should, where necessary, take precedence over data-sharing obligations.

Digital Omnibus on AI – Proposal 2025/0359 (COD)

1.4. AI and AI robotics drive innovation in Europe. At the same time they must uphold safety, ethics and fundamental rights, including workers' protection and data protection for all users. The EESC supports risk-based, proportionate regulation, which should be lighter for industrial and B2B uses, provided that safeguards remain in place. Where specific risks arise, sectoral rules should be developed with the social partners and civil society, including for high-trust professional services, ensuring 'human in command', explainability where appropriate, and professional confidentiality.

1.5. The regulatory framework must ensure coherence among all horizontal EU digital acts and sector-specific legislation (such as the Machinery Regulation, the Medical Device Regulation and other product safety rules). It should further clarify legal bases, avoid overlapping or conflicting provisions (particularly around risk assessment, conformity and liability) and prevent costly and socially harmful litigation that damages companies, workers and consumers. A 'simplification by design' principle, complemented by a corresponding 'rights by design' approach, must guide all implementing acts, delegated acts and guidance to foster predictable, fair and innovation-friendly regulation across sectors. In particular, the guidance on such acts should assess the impact of digital technologies and AI systems on production processes, working conditions, health and safety, and quality of life.

1.6. A simple solution for AI use in an internal corporate environment should be provided. The protective measures mandated by the AI Act are mostly designed to address risks associated with public and consumer-facing services. For instance, a corporate privilege could be introduced whereby the AI Act only applies in certain intra-group scenarios while upholding fundamental or workers' rights, provided that this does not create liability or redress gaps and that responsibilities remain clearly allocated among providers, developers and deployers/users.

1.7. Any simplified regime should be conditional upon the full involvement of the social partners. In particular, the introduction or substantial modification of AI systems in the workplace should be subject to workers and their representatives being informed and consulted in advance, in accordance with Union and national law and practice. In this context, social dialogue at workplace level plays a central role in ensuring the responsible, trustworthy and rights-compliant use of AI at work.

1.8. The EESC acknowledges the need to simplify the regulatory framework applicable to small and medium-sized enterprises (SMEs) and small mid-caps (SMCs), in order to reduce administrative burden and support innovation and competitiveness. However, the EESC stresses that such simplified regimes should apply exclusively to undertakings that are not partner enterprises or linked to other undertakings, in accordance with Commission Recommendations 2003/361/EC and 2025/1099 EU.

1.9. The EESC recommends that application deadlines for high-risk AI obligations be aligned with the availability of harmonised standards developed by CEN/CENELEC – involving, where necessary, the social partners – as well as with notified bodies' capacities.

1.10. The EESC supports the establishment of regulatory sandboxes by the AI Office with strong cross-border cooperation between national authorities, including, where relevant, dedicated tracks for high-trust services (e.g. liberal professions). When workers' or citizens' rights are concerned, sandboxes should be developed in close consultation with the relevant stakeholders, in particular the social partners.

1.11. The EESC recommends that, for high-risk artificial intelligence systems, ex-ante control throughout the market placement process should be required, for example through regulatory sandboxes under the supervision of the competent national authorities or the AI Office, in order to ensure compliance with regulatory requirements and the protection of fundamental rights and workers' rights, with transparent KPI-based monitoring and reporting of outcomes.

1.12. The EESC supports the development, application and training of AI in Europe, ensuring responsible data use for AI training (including sensitive data for bias mitigation), under strict safeguards that protect fundamental rights, social values and privacy and mitigating risks by checking accountability, human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity and fairness.

1.13. The EESC acknowledges that the use of data is necessary for the development of AI systems. However, providers and deployers must assure that such systems are as transparent as technically feasible in order to allow effective oversight by the competent national authorities and adequate involvement of the social partners, particularly when AI is used in the workplace.

1.14. The EESC welcomes the empowerment of the AI Office with adequate resources and equipment as a central coordinating body for the implementation and oversight of the AI Act. Its mandate should include facilitating cross-border cooperation, providing clear and accessible guidance to companies, public authorities and the social partners, supporting SMEs and SMCs, and ensuring consistent interpretation and enforcement of AI regulations across the Member States, in consultation with all relevant stakeholders.

1.15. The EESC considers that it would be appropriate to ensure that, where a provider classifies an AI system as not high-risk pursuant to Article 6(4), appropriate transparency mechanisms vis-à-vis the competent national authorities are put in place. These mechanisms should include, where necessary, registration or notification procedures to enable effective oversight and the verification of the provider's assessment, and to prevent potential risks to fundamental rights, including workers' rights.

1.16. With regard to Article 4 of the AI Act, the EESC suggests maintaining an explicit obligation for providers and deployers of AI systems to ensure a sufficient level of artificial intelligence literacy among their staff, as well as among any persons responsible for the operation and use of AI systems on their behalf. Furthermore, AI literacy programmes for all should be envisaged.

1.17. The EESC urges the European Commission, the Parliament and the Council to prioritise the timely conclusion of trilogue negotiations on the AI Omnibus, ensuring that all stakeholders have clarity and sufficient time to adapt before high-risk AI obligations become binding. Furthermore, the EESC suggests close coordination with the legislative proposal on the European Business Wallet ([1]), as these two initiatives share the objectives of administrative simplification, interoperability, and coherence within the digital single market.

Digital Omnibus – Proposal 2025/0360 (COD)

1.18. The EESC strongly supports a genuinely interoperable EU 'single entry point' (SEP) covering NIS2, GDPR, DORA, eIDAS and CER reporting. In addition to the language of the Member State concerned, it should enable English-language submissions and the reuse of previously submitted information, and should also apply strict 'need-to-know' access controls for authorities; pilots should be co-designed together with industry and the social partners.

1.19. The EESC stresses that the definition of personal data, as set out in Article 4(1), is decisive in determining the scope of application of the GDPR and, consequently, the scope of the rules safeguarding the fundamental right to the protection of personal data, as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. In light of this, the EESC considers it essential that this definition is formulated in an objective and adequately broad manner, ensures legal certainty, prevents subjective or evasive interpretations, and guarantees a high and effective level of protection of fundamental rights, while allowing for the reasonable use of data.

1.20. The EESC calls for the European Commission to adopt implementing acts that clarify and specify the means and criteria for determining when pseudonymised data may be considered anonymised for other entities. The use of anonymised data is an instrument of great significance for industry, particularly for AI training, while also providing a mechanism to balance innovation with strong data protection and privacy safeguards.

1.21. The EESC stresses that the right of access to personal data constitutes an enabling right and is thus a prerequisite for the effective exercise of other fundamental rights. It therefore recommends that the right of access be fully ensured whenever the data subject pursues a legitimate purpose, in particular the protection of workers' rights or the safeguarding of health and safety at work. Furthermore, the burden to prove the existence of an abuse of rights by the data subject shall remain with the controller.

1.22. The EESC recommends that the definition of scientific research should remain in its commonly accepted meaning, but should enable innovation through industrial research. Referring to the case-law of the Court of Justice of the European Union, according to which any broad, unbalanced or absolute limitation of the rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union cannot be considered compatible with the Charter ([2]), the EESC calls for a just approach to the scope of scientific research.

1.23. With regard to Article 22(1) of the GDPR, the EESC stresses the need to fully respect the data minimisation principle enshrined in Article 5(1) of the GDPR ([3]). Automated decision-making systems should be implemented where they offer clear added value and efficiency, while ensuring that their use remains necessary and proportionate to the task. Where decisions can be reasonably made through non-automated means or less intrusive alternatives, human decision-making should be preferred.

1.24. With regard to the ePrivacy Directive, the EESC encourages the co-legislators to explore options for simplifying consent requirements in low-risk contexts. A proportionate, risk-based solution would preserve innovation capacity for technologies that offer clear societal benefits, while maintaining robust privacy protections.

1.25. The EESC supports extending the simplification of documentation, reporting and procedures to SMCs (in addition to SMEs and start-ups). Templates, examples and streamlined processes should be made available – and should be mandatory where personal data are not involved. All simplification measures should be developed in consultation with the social partners and civil society.

1.26. The EESC acknowledges the need to simplify the regulatory framework applicable to SMEs and SMCs, in order to reduce administrative burden and support innovation and competitiveness. However, the EESC stresses that such simplified regimes should apply exclusively to undertakings that are not partner enterprises or linked to other undertakings, in accordance with Commission Recommendations 2003/361/EC and 2025/1099/EU.

1.27. Mandatory data-sharing requirements under the Data Act should be limited to cases where strictly necessary, for instance in public emergencies or for protection of workers' and fundamental rights.

1.28. The EESC encourages the Commission to focus on incentives for voluntary data sharing, strengthen the European Data Innovation Board, and to foster the implementation of common European data spaces to uphold transparency, trust and public benefit.

2. EXPLANATORY NOTES

Arguments in support of recommendation 1.1 – 1.3

2.1. Europe's global competitiveness and technological sovereignty depend on rapid innovation and adaptability. Excessive bureaucracy and fragmented rules hinder digital progress and risk Europe falling behind. Streamlining regulation and reducing administrative burden, while upholding fundamental rights and social standards, frees up resources for research, skills and sustainable growth.

2.2. Ensuring coherent interplay between AI, data, privacy and cybersecurity rules will reduce litigation risks and compliance costs, while preserving high social standards. Reducing fragmented reporting requirements will free up resources for innovation, improve compliance and allow companies – especially SMEs and SMCs – to focus on core activities.

2.3. Legal clarity and harmonisation are essential for a functioning single market and for Europe's strategic autonomy. Ambiguous definitions and conflicting rules create uncertainty, increase compliance costs and can lead to legal disputes that undermine trust and slow down cross-border cooperation. Clear, harmonised definitions help ensure fair competition, protect fundamental rights and enable effective enforcement in order to fully guarantee fundamental rights, in particular those enshrined in Articles 7 and 8 of the CFREU.

Arguments in support of recommendation 1.4 – 1.17

2.4. A risk-based approach to regulation is essential in order to balance innovation with the protection of fundamental rights. By tailoring obligations to actual risk, the EU can foster responsible innovation, support SMEs and SMCs, and ensure that safety and fundamental rights are not compromised.

2.5. The AI Act was purposefully conceived as a horizontal framework designed to operate in harmony with existing sectoral safety standards like the Machinery Regulation (2023/1230), the Medial Device Regulation and the In Vitro Diagnostic Regulation. However, overlapping compliance obligations such as dual conformity assessments or unsynchronized risk definitions can lead to inconsistencies, cost burdens and certification delays for innovative products and systems embedded with AI.

2.6. The global race for AI leadership is intensifying, and Europe must ensure that its regulatory timelines are realistic and inclusive. Tight deadlines, especially for high-risk AI, risk excluding SMEs and SMCs from the market and slowing down innovation.

2.7. Regulatory sandboxes are a proven tool for fostering responsible innovation and testing new technologies in real-world conditions. By enabling cross-border cooperation and inclusive participation, including dedicated tracks for high-trust services (e.g. liberal professions) where relevant, sandboxes help Europe adapt to rapid technological change, support SMEs and ensure that new solutions meet high social, ethical and safety standards.

2.8. Despite the importance of data in training, testing and improving AI systems, the EESC stresses that data-driven AI must balance innovation and accountability. Providers and deployers should ensure as much as possible transparency about how these systems operate, what data they rely on, and how decisions or outputs are generated. Such transparency is a prerequisite for effective self-assessment and appropriate oversight by competent national authorities. It is also crucial to guarantee the meaningful involvement of the social partners, especially when AI is introduced in the workplace.

2.9. Legal certainty is a cornerstone of successful digital transformation and technological sovereignty. Delays in the legislative process can leave companies – especially SMEs – unprepared for new compliance requirements. The application deadlines for high-risk systems will come into force by as early as August 2026. By finalising the trilogue well before the August 2026 deadlines, the EU can ensure that the transition to high-risk AI regulation is inclusive and operational for companies, public services and civil society.

2.10. A strong and well-equipped AI Office is essential for the effective and harmonised implementation of the AI Act throughout the EU. Fragmented oversight and inconsistent application of rules risk undermining both innovation and fundamental rights. By acting as a central hub, the AI Office can bridge gaps between national authorities, industry and civil society.

2.11. The EESC calls for effective mechanisms to verify compliance with safeguards, including strong pseudonymisation or equivalent privacy-enhancing techniques, strict purpose limitation for data processing and the deletion of sensitive data once the intended purpose has been fulfilled. Workers' representatives should be involved, where appropriate, in dataset oversight or governance structures, in order to ensure transparency and trust.

Arguments in support of recommendation 1.18 – 1.28

2.12. Cybersecurity and resilience are central to Europe's technological sovereignty. A genuinely interoperable 'single entry point' for incident reporting will reduce duplication, improve situational awareness and enable faster, more coordinated responses to threats.

2.13. According to the Court of Justice of the EU, treating information *not* as 'personal data' would remove it entirely from the obligations, principles, and safeguards of data protection law ([4]). In that case, the data subject could neither exercise their rights (such as access) nor challenge the decision through a complaint, and national authorities would be unable to carry out oversight. For these reasons, the ECJ has consistently held that the notion of 'personal data' must be interpreted broadly ([5]), and that the likelihood of identification must be assessed in light of 'all objective factors' ([6]).

2.14. The ability to process and use data responsibly is a cornerstone of digital innovation and public interest. Clarifying when pseudonymised data can be considered anonymised is critical for legal certainty and innovation. Anonymised data enables companies to train AI systems without processing personal data, thereby reducing compliance risks, while maintaining strong privacy protections.

2.15. Where the implementing acts concern the use of data or AI systems in employment contexts or have implications for working conditions or workers' rights, the EESC stresses that they should be prepared and adopted in close consultation with the social partners, in accordance with Union law and established social dialogue practices.

2.16. The ECJ has clarified that the right of access must allow data subjects to verify that their personal data are accurate and processed lawfully ([7]). Moreover, not having to provide a specific reason for an access request helps data subjects exercise their rights more easily ([8]). As a result, any possibility for a controller to refuse an access request must be interpreted narrowly ([9]), and a refusal on grounds of excessiveness requires proof – based on all relevant circumstances – of an abusive intent by the data subject ([10]).

2.17. According to the EDPB, the term 'scientific research' shall 'not be stretched beyond its common meaning' ([11]). This is in line with the consolidated ECJ case-law, according to which 'the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary' ([12]).

2.18. The data minimisation principle in Article 5(1)(c) of the GDPR requires controllers to process only the personal data that are adequate, relevant and limited to what is necessary for a specific purpose. If a decision can be reasonably taken through non-automated means, deploying an automated system typically implies collecting, inferring or retaining additional data and creating new risks (e.g. profiling, opacity, bias and reduced contestability). For this reason, the use of automated decision-making should be limited to situations where it is necessary.

2.19. Under the current ePrivacy framework, access to data in terminal equipment, even in low-risk contexts, often requires user consent. While protecting privacy is essential, overly rigid consent requirements can unintentionally hinder innovation in areas that deliver significant societal benefits, such as vehicle safety and autonomous driving. In these cases, the inability to access relevant data can compromise progress on technologies that improve road safety and reduce accidents.

2.20. Reducing bureaucracy and extending simplifications to SMCs is vital for Europe's industrial backbone. SMEs and SMCs drive innovation, job creation and regional development, but are often disproportionately affected by complex compliance requirements.

2.21. Voluntary data sharing, supported by incentives and a strong European Data Innovation Board, is key to building a thriving data economy and to strengthening Europe's technological sovereignty. Common European data spaces enable collaboration, innovation and the responsible use of data across borders and sectors.

Brussels, 18 March 2026.

The President

of the European Economic and Social Committee

Séamus BOLAND

([1]) COM(2025) 838 final.

([2]) Judgment of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12, EU:C:2014:238, paragraph 38.

([3]) Judgment of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, C-252/21, EU:C:2023:537, paragraph 109.

([4]) Judgment of 20 December 2017, Peter Nowak v Data Protection Commissioner, C-434/16, EU:C:2017:994, paragraph 49.

([5]) Judgment of 7 March 2024, OC v European Commission, C-479/22 P, EU:C:2024:215, paragraph 45.

([6]) Judgment of 7 March 2024, OC v European Commission, C-479/22 P, EU:C:2024:215, paragraph 79. Judgment of 4 September 2025, European Data Protection Supervisor v Single Resolution Board, C-413/23 P, EU:C:2025:645, paragraph 79.

([7]) Judgment of 22 June 2023, Proceedings brought by J.M., C-579/21, EU:C:2023:501, paragraph 57.

([8]) Judgment of 26 October 2023, FT v DW, C-307/22, EU:C:2023:811, paragraph 50.

([9]) Opinion of Advocate General Szpunar of 18 September 2025, Brillen Rottler GmbH & Co. KG v TC, C526/24, EU:C:2025:723, paragraph 30.

([10]) Opinion of Advocate General Szpunar of 18 September 2025, Brillen Rottler GmbH & Co. KG v TC, C526/24, EU:C:2025:723, paragraph 41.

([11]) EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 5.

([12]) Judgment of 7 November 2013, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others, C-473/12, EU:C:2013:715, paragraph 39.

ELI: http://data.europa.eu/eli/C/2026/3225/oj

ISSN 1977-091X (electronic edition)