weizenbaum
POLICY PAPER

March 2026
20

Weizenbaum Institute and German Society for Law and Informatics

Structural Challenges of EU Digital Legislation and Targeted Simplification Through the Digital Omnibus Initiative

ABOUT THE AUTHORS

Melina Braun \\ Humboldt-Universität zu Berlin \\ Weizenbaum Institute
Prof. Dr. Malte Grützmacher \\ CMS Hasche Sigle
Prof. Dr. Christian Heinze \\ Universität zu Köln
Lisa Markschies \\ Humboldt-Universität zu Berlin \\ Weizenbaum Institute
Charlotte Mysegades \\ Weizenbaum Institute
Prof. Dr. Benjamin Raue \\ Universität Trier
Prof. Dr. Herbert Zech \\ Humboldt-Universität zu Berlin \\ Weizenbaum Institute

Authors listed in alphabetical order.

Contact: charlotte.mysegades@weizenbaum-institut.de

ABOUT THIS PAPER

This statement was developed through a collaborative process involving the Weizenbaum Institute and the German Society for Law and Informatics. The first part of the position paper analyses EU digital legislation, highlighting structural problems within the European digital regulatory framework. The second part comprises a statement on the European Commission's specific legislative proposals within the framework of the Digital Omnibus Initiative. Here, the authors comment in particular on provisions relating to the AI Regulation and the GDPR. Finally, the paper contains a summary of specific recommendations for further legislative action at EU level.

ABOUT THE WEIZENBAUM INSTITUTE

The Weizenbaum Institute is a joint project funded by the German Federal Ministry of Research, Technology and Space (BMFTR) and the State of Berlin. It conducts interdisciplinary and basic research on the digital transformation of society and provides evidence- and value-based options for action in order to shape digitalization in a sustainable, self-determined and responsible manner.

Weizenbaum Policy Paper

Structural Challenges of EU Digital Legislation and Targeted Simplification Through the Digital Omnibus Initiative

Weizenbaum Institute and German Society for Law and Informatics

Abstract

The EU Digital Legislation is characterised by a multitude of horizontal and sector-specific instruments, within the scope of data protection law, data law, platform regulation, cybersecurity law, product safety regimes, competition law, and artificial intelligence regulation. Taken individually, these instruments pursue broadly supported and normatively legitimate objectives, such as the protection of fundamental rights, market fairness, the strengthening of cybersecurity, and the enhancement of product safety, including the safety of artificial intelligence systems and models, the opening of data silos, and the promotion of innovation.

Despite these objectives, the application of EU digital law reveals structural deficiencies. The result is a growing degree of legal uncertainty and compliance complexity, which affects not only regulated entities but also regulators, courts, and legal advisors.

We welcome that the recent approach under the Digital Omnibus Initiative[1] signals an awareness of these problems and a political willingness to address them. On 19 November 2025, the EU Commission adopted proposals for two omnibus regulations: the 'Digital Omnibus Regulation' and the 'Digital Omnibus Regulation on AI'. The core of this legislative package concerns data law and AI regulation.

As the European Commission states itself, the EU has "pioneered digital regulation, and has set the golden standard for the highest level of protections for fundamental rights, consumer safety and the protection of European values."[2] In its Conclusions of 26 June 2025, the

[1] 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.

[2] Explanatory Memorandum (1), Digital Omnibus COM (2025) 837 final and Digital Omnibus on AI COM (2025) 836 final.

European Council also underlined the importance of 'simplicity by design' legislation, "without undermining predictability, policy goals, and high standards".[3]

Therefore, this paper argues that the targeted simplification with the two omnibus proposals should not decrease this 'golden standard', but be approached with a more systematic use of the Digital Omnibus initiative that could substantially improve the coherence, clarity, proportionality and operability of EU digital legislation and by this means to ensure Europe`s competitiveness, also, where appropriate, by reducing administrative and reporting burdens for businesses.[4] The goal should be to regulate in a coordinated and consistent manner, and to do so in as few legal acts as possible.[5]

The first part of the paper examines the legal architecture of EU digital legislation and analyses three categories of norm cumulation. Furthermore, it identifies four structural causes of legal uncertainty and their consequences for innovation, compliance, and enforcement.

The second part provides a statement on the Digital Omnibus Initiative concerning artificial intelligence (AI) and data protection, evaluating specific amendments to the two legislative proposals.

The paper concludes with recommendations for improving the proposals in the short and medium term, and for the EU Digital acquis as a whole in the long term.

[3] European Council, Conclusions, EUCO 12/25, Brussels, 26 June 2025, paragraph 30.

[4] European Council, Conclusions, EUCO 18/25, Brussels, 23 October 2025, paragraph 33.

[5] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin.

Contents

1 Part I: Remarks on the EU Digital Legislation

1.1 The Architecture of EU Digital Legislation

The EU Digital Legislation has evolved incrementally, rather than through a single, coherent codification process.[6] Responses to digitalisation in the form of regulation have emerged across different policy fields, each shaped by its own objectives, enforcement logic and institutional context. Consequently, digital technologies are now subject to simultaneous regulation by multiple legal regimes, each of which approaches the same or similar systems, data flows or business models that continue to develop while being subject to regulatory rules from a different normative angle.

This layered regulatory architecture is particularly evident in areas such as platform-based intermediation and content moderation, data governance, data access, and data re-use, software-enabled products and services, and the development and deployment of AI-systems.

While functional overlaps between legal regimes are, to a certain extent, unavoidable in complex regulatory environments, the EU digital acquis accumulates norms rather than coordinating norm interaction.

From our perspective, the problem does not per se lie with the regulations themselves. Quite often, it already lies in the quality and internal coherence of the regulatory framework. Therefore, we argue that deregulation will not solve the problems with the EU Digital Legislation.

1.2 Norm Accumulation

A recurring feature of EU digital legislation is the duplication of structurally similar obligations across different legal acts. Documentation duties, risk assessments, transparency requirements, and incident reporting obligations are imposed, often with only minor variations in scope, timing, or terminology. In many cases, these obligations pursue closely related regulatory objectives, such as risk mitigation, accountability, or oversight. Parallel rules significantly increase compliance costs and legal complexity.[7] Companies are required to establish multiple compliance processes for closely related obligations, while legal advisors and authorities face growing difficulties in providing consistent and predictable guidance. Nevertheless, even more problematic are situations in which parallel obligations interact in ways that may lead to normative tension or outright conflict.

---

[6] Zenner, Table 1: Overview of EU Legislations in the Digital Sector, https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world.

[7] Digital-Omnibus: Vorschlag zur Vereinfachung des EU-KI-Regelwerks, ESG 2026, 1.

Depending on their structure, norm accumulations may have different legal and practical consequences, which are shown in the categories below.

Categories:[8]

1.2.1 Parallel Rules without Regulatory Conflict

The first category comprises parallel rules that do not result in a regulatory conflict. In these cases, different legal instruments impose similar or even identical obligations on the same parties without contradicting each other. The relevant provisions can be applied cumulatively.

Typical examples include the repeated regulation of organisational, documentation, or due-diligence requirements across different regulatory regimes. Although no material inconsistency arises, the coexistence of parallel obligations results in an increased compliance burden for regulated entities. At the same time, such duplication may undermine the transparency and systematic coherence of the legal framework without producing an equivalent normative added value. Examples of parallel rules without regulatory conflict can be seen in the following: processing register (Art. 30 of the General Data Protection Regulation (GDPR)[9]) and record-keeping obligations (Art. 12, 19 of the Artificial Intelligence Act (AIA)[10]); Risk management system (Art. 9 AIA), fundamental rights impact assessment (Art. 27 AIA) and data protection impact assessment (Art. 35 GDPR); Reporting obligations (Art. 33, 34 GDPR; Art. 61, 73 AIA) and IT security requirements (Art. 32 GDPR/Art. 15 AIA/Cyber Resilience Act (CRA)[11]).

In our opinion, there are three possible solutions for parallel rules without regulatory conflict. The first option could involve harmonisation of substantive compliance standards, whereby fulfilment of the more general obligation leads to fulfilment of the more specific obligation. The second solution could involve formal harmonisation of procedures, whereby obligations are fulfilled through one uniform procedure, or several harmonised procedures. The third solution could involve limiting or deleting substantive compliance obligations. We urge the European Commission to pursue much more vigorously one of these solutions: Without the burden to comply with several parallel rules, the compliance burden decreases

---

[8] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin.

[9] 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).

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[11] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

significantly and the desired simplified procedures can be achieved, without abandoning the substantive level of protection.

1.2.2 Parallel Rules with Actual or Potential Regulatory Conflict

A second category encompasses parallel rules that give rise to an actual or potential regulatory conflict. In these cases, the relationship between the overlapping provisions is unclear or inconsistent, which makes it difficult to determine their respective scope of application or hierarchical relationship.

The central interpretative question concerns how *Rule A* relates to *Rule B*. This may require recourse to traditional principles governing norm conflicts, such as *lex specialis* or *lex posterior*, or to an understanding of one provision as constituting only a partial regulation of the relevant subject matter. In practice, however, the applicable legal texts often fail to provide sufficiently precise guidance to resolve these issues in a predictable manner. It is therefore left to the courts to decide such issues which takes years and significantly increases legal uncertainty until matters are finally (if at all) resolved by the Court of Justice.

Particular difficulties arise from generic clauses stating that one EU legal act applies *'without prejudice to'* another. Such formulations rarely clarify the normative relationship between overlapping legal regimes. Instead, they tend to leave the resolution of potential conflicts open to interpretation and enforcement, thereby creating more legal uncertainty for regulated entities, supervisory authorities, lawyers and courts.

1.2.3 Coordination of Rules without Factual Overlap

A third category consists of rules that do not overlap in a technical sense, but which require coordination. For example, the AIA and the (EU and national) rules on civil liability do not – in a technical sense – overlap as they address different issues. However, the rules of the AIA may and will still influence civil liability rules in a way which is difficult to predict. For example, it is unclear whether and to which extent the rules of the AIA for high-risk systems may also serve as a guideline or inspiration for courts where they deal with liability for AI outside the high-risk area. It is also not clear how rules which are of an organisational or institutional nature may impact civil liability. Moreover, even within the (revised) Product Liability Directive it is unclear how far it also applies to AI, in particular where AI is offered as a service and not implemented in a product. Therefore, we recommend that the EU legislator clarifies the relationship between AI regulation and liability and to which extent AI is covered by the Product Liability Directive.[12]

[12] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin.

1.3 Legal Uncertainty

Beyond the regulatory cumulations, contradictions and uncertainties, structural features of EU digital legislation contribute to legal uncertainty as well. Several structural causes can be identified:[13]

1.3.1 Linguistic and Logical Deficiencies

Numerous instruments suffer from unclear or vague legal terms or diverging definitions for similar concepts, e.g. the question of when someone is a "quasi-manufacturer".[14] In addition, there are circular references within obligations or exemptions, as well as inadequate or inconsistent translations in the various language versions, e.g. the use of different terms in Art. 25 Data Act; whereas the German translation uses the term *Übergangsfrist*, the English version uses the term *transitional period*, which would be closer to *Übergangszeitraum*. The German text also contains the word *Kündigung* instead of *Beendigung*, which would be closer to the English phrase *termination*.[15]

Furthermore, the quality of the translations from the negotiated English text into some of the equally binding other languages of the EU is remarkably poor. The German translations of the digital acts lack consistency and – unacceptably – contain obvious mistranslations of key elements in some provisions. The English and French versions of Art. 42 (2) DSA address 'very large online platforms' – the German version 'very large online search' (see also 5.a)dd)).[16]

These shortcomings undermine legal certainty and increase the scope for interpretation at both the advisory and enforcement levels.

1.3.2 Regulatory Misallocations

Certain regulatory approaches fail to align obligations with the actors or risks they are intended to address, resulting in compliance burdens that are disproportionate to actual risk profiles or market roles.

---

[13] Grützmacher, Compliance bei IT-Produkten und Diensten in der Praxis (EU-Gesetzgebung als "Hemmschuh" für Innovationen?), Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin.

[14] Further example: clarity regarding the provider vs. operator role and 'substantial changes' (Art. 25 AIA): It is currently unclear in which cases, according to Art. 25(1) AIA, the role changes from operator to provider in the case of GPAI systems, as the criticality of GPAI systems depends on the specific application case and often cannot be determined in advance.

[15] More examples of inconsistent translations: 'Kündigungsfrist' instead of 'Ankündigungsfrist,' English wording 'notice period' or the German term for 'where applicable' ('gegebenenfalls' in the German translation) with no equivalent word in the English version.

[16] For further examples see Hofmann/Raue, Digital Services Act – Gesetz über digitale Dienste, Einleitung mn. 34 (p. 39).

1.3.3 Insufficient Legislative Support Structures

The regulatory framework is further weakened by a lack of effective legislative support, including the persistent precedence of data protection law[17] without sufficient coordination with newer digital regimes, divergent regulatory approaches to structurally comparable problems[18], limited legislative guidance for contract negotiations in regulated data and platform environments[19], and unclear or insufficiently considered effects on national law and existing legal structures.

1.4 Consequences for Innovation, Compliance, and Enforcement

These structural features have a cumulative effect, resulting in a qualitative shift in the nature of compliance challenges. Legal uncertainty arises not only from unclear individual rules, but also from unclear interactions between rules. In such an environment, compliance becomes a matter of risk management under uncertainty.

This has broader implications: resources are diverted from innovation and development towards managing regulatory interfaces; legal advice becomes increasingly cautious and defensive; enforcement risks become harder to anticipate; and regulatory objectives may be undermined by inconsistent application.

1.5 Recommendations for the EU-Digital Framework.[20]

1.5.1 Immediate and Technical Measures

1.5.1.1. Alignment of Key Definitions by Reference/Annex

Where instruments regulate comparable actors or systems, new legislative directives and acts should introduce explicit cross-references to harmonised definitions (e.g. platform categories, AI system characteristics, provider roles), rather than maintaining parallel terminology. Moreover, the creation of a horizontal definition annex that defines key legal terms such as *'manipulative design practices'* or *'material changes'* across legal acts could greatly reduce existing interpretation problems.[21] Regarding the AIA, we agree with the point raised that it

---

[17] Grützmacher, Compliance bei IT-Produkten und Diensten in der Praxis (EU-Gesetzgebung als "Hemmschuh" für Innovationen?), Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin.

[18] For example: Art. 4(13) and Art. 4(14) Data Act (DA) and Art. 6(1) GDPR.

[19] Deutscher Anwaltsverein, Stellungnahme SN 37/24: NIS-2-directive; compare to § 30 Abs. 2 BSIG-E/NIS2-directive and Art. 32 GDPR (Art. 28 Abs. 3 S. 2 lit. c) GDPR), Art. 33 DSGVO (Art. 28 Abs. 3 S. 2 lit. f) GDPR), Art. 5 GDPR (Art. 28 Abs. 3 S. 2 lit. h) GDPR).

[20] Raue, DSA, P2B-VO, TCO, EMFA, Politische Werbung-VO, AVMD-RL, DSM-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin; Wybitul/Ziegler: Digital Omnibus: Harmonisieren, Entlasten, aber nicht Entwirren? BKR 2026, 73.

[21] Zenner, Der Digitale Omnibus der EU: Zwischen notwendiger Vereinfachung und blindem Aktionismus, EuDIR 2026, 42.

is important to recognise that the terms used in AI law have a dual legal and technical nature.[22]

1.5.1.2. "Once-Only" Compliance for Equivalent Obligations

Where documentation, reporting, or risk assessment duties pursue the same regulatory objective, the legislator should clarify that fulfilment under one instrument can under certain circumstances, if met, be deemed as sufficient for others, unless explicitly stated otherwise. The idea of uniform portability rules for compliance certificates should be assessed: mutual recognition of comparable audits between different legal acts would benefit European SMEs in particular due to their relatively higher bureaucratic costs.[23]

1.5.1.3. Consolidation of Transparency and Reporting Formats

Standardised templates and reporting cycles should be integrated across regimes, avoiding parallel transparency reports with marginal differences. This would be an advantageous approach, as similar questions arise in different regimes of law. This means that AI law, as well as digital law as a whole, are cross-cutting legal issues that can only be fully understood by examining the sub-disciplines collectively.[24]

1.5.1.4. Systematic Correction of Translation Errors

The European Commission should perform a comprehensive check of the correct translation of the EU digital acts into the languages of the Member States and formally correct translation inconsistencies that affect the application and the legal interpretation, thereby enhancing uniform application across Member States.

1.5.2 Medium-Term Measures: Substantive Coordination

1.5.2.1. Explicit Priority Rules for Overlapping Obligations

Instead of generic *'without prejudice'* clauses, the legislator should clarify which regime prevails in defined overlap scenarios, at least for frequently occurring constellations.[25] We recommend establishing clear priority rules instead of using 'without prejudice' clauses. [26]

1.5.2.2. Substantive Presumptions of Compliance

Where requirements are equivalent in substance (e.g. cybersecurity, risk management), compliance with one regime should give rise to a legal presumption of compliance with others.

---

[22] Heinze/Sorge/Specht-Riemenschneider: Das Recht der Künstlichen Intelligenz, KIR 2024, 11.

[23] Zenner, Der Digitale Omnibus der EU: Zwischen notwendiger Vereinfachung und blindem Aktionismus, EuDIR 2026, 42.

[24] Heinze/Sorge/Specht-Riemenschneider: Das Recht der Künstlichen Intelligenz, KIR 2024, 11.

[25] To the use of "without prejudice" clauses, see Steinrötter, Verhältnis von Data Act und DS-GVO, GRUR 2023, 216.

[26] Example for a clear priority rule: Art. 1(3) DGA:„In the event of a conflict between this Regulation and Union law on the protection of personal data (…), the relevant Union (…) law on the protection of personal data shall prevail.".

1.5.2.3. Legislative Support for Contractual Implementation

Due to rapid technological change, AI law has so far been shaped primarily by legislation and practice, and possibly by science, but hardly by case law. This creates legal uncertainty, as legislative requirements are, within the EU digital legislation, often shaped through abstract and vague definitions, and interpretations in the literature diverge naturally. Although the number of court decisions is set to increase in the coming years, there will still be uncertainties due to court interpretations. Regulatory guidelines, interpretation aids and practical guidelines, such as the codes of conduct (Art. 56 AIA) are welcome.[27] Therefore, we recommend, that the European Commission should be empowered to issue, where appropriate (e.g. in areas where markets are still developing and market developments must be revisited after a certain period of time), semi-binding model clauses or guidance addressing recurring compliance interfaces (e.g. data sharing, platform moderation, AI deployment).

1.5.3 Long-Term measures: Interoperability Checks for Digital Legislation

Future amendments should include a mandatory assessment of interaction effects with existing digital acts.

2 Part II: Statement on the Digital Omnibus Proposals Concerning Artificial Intelligence and Data Protection

2.1 Preliminary Remarks

The Digital Omnibus proposals aim to simplify and facilitate the application of EU digital legislation, in particular in the areas of data protection, data access and artificial intelligence. These objectives are welcome. At the same time, simplification does not by its nature come at the expense of fundamental rights protection, legal certainty, or the rule of law.

The Digital Omnibus initiative consists of two regulations: the 'Digital Omnibus on AI' (DOAI) and the general 'Digital Omnibus' (DO). The DOAI is intended to amend the AIA, while the DO is intended to amend the Data Act (DA)[28], the GDPR and existing cybersecurity laws (e.g. NIS-2, DORA).

The Digital Omnibus Initiative correctly identifies key implementation challenges and proposes targeted measures, including the streamlining of rules, a reduction in the number of applicable laws, the harmonisation of provisions, and a lowering of administrative burdens

[27] Heinze/Sorge/Specht-Riemenschneider: Das Recht der Künstlichen Intelligenz, KIR 2024, 11.

[28] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

through simplified requirements and procedures. These measures seek to ease compliance obligations for small and medium-sized enterprises (SMEs) across the data acquis and the AIA. At the same time, they seek to support a dynamic and innovation-friendly business environment by enhancing legal certainty and creating new opportunities, in particular with regard to data sharing and reuse, the processing of personal data, and the training of AI systems and models. Overall, these measures seek to reduce friction and significantly improve administrative efficiency.[29]

The European Commission argues that all proposed amendments by the Digital Omnibus Initiative are merely technical in nature and do not affect the substance of the regulations. However, the following analysis shows that amendments that are referred to as *'legal clarification'* change the level of protection or certain rights and interests in certain cases which is welcomed if this is appropriate.

Furthermore, the European Commission should take into account that the practical challenges that companies face on a daily basis lie less in the political ambition of individual legal acts and more in their structural deficiencies and complex interaction, as demonstrated in Part I of this position paper. For instance, when the same cyberattack simultaneously triggers GDPR reporting obligations, the NIS2 Directive and reporting and documentation obligations under the CRA and AIA, overlapping or conflicting compliance structures arise that consume time and resources without increasing the standard of protection for society and individuals.[30]

In view of the limited consultation period and the scope of the proposed amendments, the following remarks focus on selected, central aspects of the Digital Omnibus proposals relating to the AIA and the GDPR. In the analysis, we acknowledge that the Commission is conducting a Digital Fitness Check alongside the Digital Omnibus proposals, in which the focus is set on the engagement with stakeholders and a broader public consultation, leading to an analysis of areas that could be further aligned.[31]

---

[29] European Commission, Commission Staff Working Document, 19.11.2025, SWD (2025) 836 final (p. 3f.).

[30] Zenner: Der Digitale Omnibus der EU: Zwischen notwendiger Vereinfachung und blindem Aktionismus, EuDIR 2026, 42.

[31] Explanatory Memorandum (1), Digital Omnibus COM (2025) 837 final and Digital Omnibus on AI COM (2025) 836 final.

2.2 Evaluation of the Proposed Simplifications in the Digital Omnibus Initiative

2.2.1 Digital Omnibus on AI Act

The Digital Omnibus on AI (DOAI)[32] proposes targeted measures to the AIA. The goal is to ensure timely, smooth and proportionate implementation of certain aspects of the AIA.[33] The EU Commission has drafted more than 30 individual amendments.[34]

The proposed measures can be grouped into nine themes: (1) linking the implementation timeline of high-risk rules to the availability of standards (2) extending Small and Medium-sized Enterprises (SMEs) privileges to Small Mid-Caps (SMCs) (3) reframing the AI literacy obligation (4) increasing flexibility of post-market monitoring (5) removing certain registration obligations (6) centralising oversight in the context of GPAI (7) widening the personal scope of Art. 10(5) AIA (8) increasing regulatory sandboxes and real-world testing (9) clarifying interplay of the AIA with other EU legislation.[35] In addition to that and to support implementation even further, the European Commission is committed to non-legislative support through guidelines.[36]

The amendments raise important questions concerning proportionality, legal certainty and systemic coherence within the EU digital acquis.

2.2.1.1. Extension of SMEs Privileges

The extension of selected SME-specific privileges to SMC enterprises reflects an acknowledgment that regulatory burdens under the AIA do not scale linearly with company size. Consequently, the DOAI proposes measures to improve proportionality. Specifically, there are six fundamental provisions within this scope: Art. 1 (8), (9), (10), (22), (27) and (29) DOAI. Since they all pursue the same objective and are tightly connected, it is necessary to assess the provisions holistically.

Firstly, Art. 1(1) DOAI widens the scope of the purposes of the AI Act as stated in Art. 1(2) AIA by widening Art. 1(2) lit. g AIA-draft to include the concerns of SMCs in addition to SMEs. This change is mostly symbolic. It does not have any direct legal impact, i.e. it does not create or expand a regulatory privilege. Yet this change is welcome. When interpreting other provisions of the AIA, one might rely on Art. 1(2) lit. g AIA-draft and consequently lean towards an interpretation which is more SMC (and SME) friendly. So, indirect legal consequences could still arise. Those indirect impacts align with the overall purpose of the DOAI.

---

[32] Digital Omnibus on AI 2025 COM (2025) 836 final.

[33] Digital Omnibus on AI 2025 COM (2025) 836 final (p. 2).

[34] Heinze: Der digitale Omnibus zur KI-VO – kleine Schritte, wenig Wirkung, KIR 2026, 25.

[35] Digital Omnibus on AI 2025 COM (2025) 836 final (p. 2).

[36] Digital Omnibus on AI 2025 COM (2025) 836 final (p. 2 f.).

Secondly, Art. 1(3) DOAI inserts definitions for SMCs and SMEs into Art. 3 AIA. The proposed provision for SMCs and SMEs is aligned with other European regulations. They are also consistent with the proposed changes to the Data Act (Art. 1(2) lit. e DO). So, the proposal is a welcomed step, towards establishing a coherent and horizontal privilege for SMEs and SMCs across European Acts and Directives. Further, the proposed definitions are very legally certain.

Thirdly, Art. 1 (8), (9) and (21) DOAI either extend existing privileges for SMEs to SMCs or introduce new privileges for both of them. Regarding the former, Art. 1(8) DOAI extends existing privileges for SMEs for technical documentation (i.e. more simplified documentation practices) to SMCs by adjusting Art. 11(1) AIA. Regarding the latter, Art. 1(9) and (21) DOAI introduce granular privileges for SMEs and SMCs with regards to the requirements for quality management. Art. 1(9) DOAI firstly introduces privileges for both SMEs and SMCs (by adjusting Art. 17(2) AIA). Secondly, Art. 1 (21) DOAI introduces additional privileges just for SMEs by changing Art. 63 (1) AIA. Consequently, a system of two-tier privileges arises: highest level of privileges for SMEs and lower level of privileges for SMCs. Yet it should be noted that this two tiers only exists within the obligations regarding quality management.

From a proportionality point of view, increased granularity is welcome. Weaker economic actors (i.e. SMEs) are subject to decreased administrative hurdles in comparison to slightly stronger actors (i.e. SMCs) yet neither have to comply with the full amount of obligations. However, it surprises that this two-tiers only exist within the context of Art. 17 AIA. There seems to be no apparent reason explaining why this mechanism is not used e.g. within the context of Art. 11 AIA. If more proportionate administrative burdens are the intended purpose (as stated in the corresponding Recital 4 DOAI), even more granularity should follow naturally.

However, the creation of an additional category of beneficiaries also introduces threshold effects and borderline classification problems. In practice, SMCs may oscillate around the relevant size criteria, potentially leading to legal uncertainty and incentives for strategic corporate structuring. Given those considerations, a departure from the two-tier approach and simple privileges for SMEs and SMCs would be recommended. Therefore, an adaptation of Art. 1(9) and Art. 1(21) DOAI is required.[37] Further, from a more technical point of view, we recommend moving the additional SME privilege found in Art. 63 AIA-draft to Art. 17 AIA. Grouping all privileges into a single Article together increases readability and logical coherence. Lastly, the explicit requirement in Art. 1(29) DOAI to consider the interests of SMEs and SMCs when determining administrative fines under Art. 99(1) AIA reinforces a differentiated enforcement approach. While it enhances fairness and proportionality, it may also contribute to heterogeneous sanctioning practices across Member States if not accompanied by

[37] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin; Heinze: Der digitale Omnibus zur KI-VO – kleine Schritte, wenig Wirkung, KIR 2026, 25.

precise enforcement guidance from the European Commission. The risk of fragmented application remains inherent in sanctioning regimes that rely on discretionary balancing.[38]

2.2.1.2. Reframing the AI Literacy Obligation

The modification of the AI literacy provision in Art. 4 AIA as proposed in Art. 1(3) DOAI is symbolic of a broader shift from operator-centred obligations to policy-driven encouragement mechanisms. It does so by replacing a direct *'best efforts'* obligation for providers and deployers with a duty for the European Commission and Member States to *'encourage'* AI literacy.

The purpose of the original Art. 4 AIA can be found in Recital 20 of the AIA. According to it, AI-literacy is a necessary pre-condition to "obtain the greatest benefits from AI systems while protecting fundamental rights".[39] Given this position as fundamental base for the effective and efficient use of AI-systems, the efficacy of the proposed voluntary mechanisms (i.e. encouragement actions of the European Commission) is unclear. In the absence of concrete incentivisation or punishment mechanisms, it seems unclear why encouraging measures by the European Commission should have the impact that was intended by the legislator.

Moreover, under the current regime, the direct legal impact of the AI-literacy obligation for providers and deployers is not very high, as Art. 4 AIA is not subject to administrative fines under Art. 99 AIA or framed as a strict obligation. However, an obligation might still have indirect consequences, such as for the interpretation of other provisions of the AIA or other Directives or Acts of the EU Digital Legislation. Those indirect effects are still considerably stronger under a direct AI literacy obligation as found under the proposed regulation.

Similarly, the legal effect of the proposed changes is low, if an AI-literacy obligation of providers and deployers can be inferred from other provisions. There are four provisions from which an obligation for AI literacy could emerge. However, as will be shown, none of those provisions are an adequate alternative to Art. 4 AIA.

Firstly, an AI-literacy obligation could be inferred from Art. 26(2) AIA which states that "Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support".[40] According to Recital 91, this includes an "adequate level of AI literacy". Secondly, a sufficient level of AI-literacy could be read into Art. 14(5) AIA which states that for high-risk AI-systems according to No. 1(a) Annex III (remote biometric identification systems) the deployer must make sure that the systems are overseen by natural persons with necessary competence, training and authority. This necessarily implies that the natural persons overseeing the AI-system must have sufficient AI-literacy.[41] Thirdly, according to Art. 9(5)(c) and Art. 9(2)(d) AIA, risk management measures

[38] Heinze: Der digitale Omnibus zur KI-VO – kleine Schritte, wenig Wirkung, KIR 2026, 25.

[39] Recital 20 AIA.

[40] Similarly BeckOK KI-Recht/Denga, 4. Ed. 1.11.2025, KI-VO Art. 26 Rn. 36.

[41] Similarly BeckOK KI-Recht/Buchner, 4. Ed. 1.11.2025, KI-VO Art. 14 Rn. 24.

of high-risk AI systems might include ("where appropriate" Art. 9(5)(c) AIA) training of the deployers. This provision could be read to be understood as increasing AI literacy in order to be able to correctly assess and mitigate associated risks. Fourthly, according to Art. 14(1) AIA "high-risk AI-systems shall be designed [...] that they can be effectively overseen by natural persons". This is further specified in Art. 14(3) lit. b AIA and Recital 63 AIA to mean that the person supervising the AI-system must have the necessary competence. This could imply that the designer and developer of the provider must be schooled in AI literacy in order to enable human oversight further down the value chain.[42]

Nevertheless, neither of those provisions (each taken separately or as a whole) are an adequate substitute for the AI literacy obligation for deployers and providers according to Art. 4 AIA. Firstly, the provisions analysed above only mandate very specific AI literacy measures (e.g. for the context of human oversight or remote biometric identification systems).[43] Yet a broad and general literacy obligation is necessary to adequately work with AI systems, obtain the greatest benefits but at the same time protect fundamental rights (as mandated by Recital 20 AIA). Secondly, none of the analysed provisions specifically target staff and persons dealing with AI. The precise wording of the paragraphs is either "provider" and "deployer". This creates gameable loopholes where specific persons (e.g. due to a certain arrangement of employment contracts) might not be covered. Further, a wide circle of addressees is also intended according to Recital 20 AIA. As a consequence, none of the analysed provisions can adequately compensate for the proposed changes. To conclude, the proposed changes to Art. 4 AIA fundamentally alter the current approach to AI literacy, defeating the regulatory purpose of Art. 4 AIA.

Regarding the telos of the proposed new Art. 4 AIA draft; taking Recital 5 DOAI as a starting point, the proposed changes to Art. 4 AIA aim to eliminate a one-size fits all obligation to ensure AI literacy. According to the Recital, such an approach is ineffective since it does not provide the required flexibility for different kinds of providers and deployers. This reasoning, however, does not take into account the fact that the current version of Art. 4 AIA does not create a one-size fits approach at all. The wording of Art. 4 AIA is intentionally left unspecified ("shall take measures"). The corresponding Recital 20 AIA even explicitly states that "[the precise obligation] may vary with regard to the relevant context". Consequently, the identified regulatory efficiency intended to solve is not addressed by this change.

Consequently, the proposed changes defeat the original purpose of Art. 4 AIA. For that reason, we recommend reconsidering the proposed change to Art. 4 AIA and leaving it as is.

2.2.1.3. Processing of Special-Category Personal Data for Bias Detection and Mitigation

Art. 1(5) DOAI introduces a new Art. 4a into the AIA. The first paragraph of Art. 4a is in substance equivalent to Art. 10(5) AIA, which is therefore removed via Art. 1(7) DOAI. It serves as

---

[42] Similarly BeckOK KI-Recht/Buchner, 4. Ed. 1.11.2025, KI-VO Art. 14 Rn. 43.

[43] Hofer/Kirchmair: KI-Kompetenz in der Praxis: Compliance-Strategien für Unternehmen im Lichte der KI-VO, ZfPC 2025, 270, 274.

a legal basis for the processing of special categories of personal data for the detection and correction of bias in the context of high-risk AI systems. The second paragraph of Art. 4a AIA-draft extends the material scope to providers and deployers of all other AI systems (which includes GPAI).

Four issues must be raised in connection with Art. 1(5) DOAI. Firstly, the precise positioning of Art. 4a(1) AIA draft surprises and should be adjusted. Secondly, the overall intention of broadening the scope of the legal basis for processing special-category personal data is welcome. Thirdly, the practical impact of Art. 4a(2) AIA draft is low. Fourthly, the coherent interplay with the GDPR through the proposed changes in Art. 3(15) DO is welcome.

Starting off with the precise positioning of Art. 4a(1) AIA draft, in order to increase doctrinal clarity, the precise placements of paragraph 1 and paragraph 2 should be adjusted. Art. 4a(1) AIA draft specifically addresses the constellation of high-risk AI systems while Art. 4a(2) AIA draft widens the scope of the provisions for all AI systems by referencing paragraph 1. It is recommended to move the specific provision of Art. 4a(1) AIA draft to Chapter III, Section 2 ("Requirements for high-risk AI") specifically to Art. 10(5) AIA governing the requirements in relation to data (for testing data), where it was previously found. Art. 4a(2) AIA draft should stay within Chapter I "General provisions". This increases doctrinal clarity and improves readability by coherently grouping the obligations based on the risk-categories. This is also in line with the objective of the Digital Omnibus Initiative ("simplify, clarify and improve our common acquis"[44]).

The overall intention of the EU legislator to broaden the personal scope of the previous Art. 10(5) AIA exemption is welcome. Bias in training, validation and testing data leads to discriminatory output (direct or indirect discrimination or representational discrimination) and decreases output quality overall. This problem as such is not limited to high-risk AI systems but exists for all kinds of AI. For that reason, an extension of bias detection and mitigation mechanisms is welcome, provided that the obligation is subject to the principle of appropriateness for such additional systems, thereby ensuring that the effect on the freedom to conduct a business is adequately balanced.

Thirdly, despite welcoming the overall notion of the proposed changes, the practical impact of Art. 4a(2) AIA draft is expected to be low. The requirements according to Art. 4a(2) AIA draft in connection with Art. 4a(1) AIA draft are very high. Only in very limited situations will providers or deployers be able to fulfil those conditions. This is due to the nature of the link in Art. 4a(2) AIA draft "Paragraph 1 may apply [...] where necessary and proportionate". This link is most plausibly read to mean that the elements of paragraph 1 and 2 need to be fulfilled cumulatively (see Recital 6 DOAI). The burden to fulfil the requirements of the first paragraph is already very high ("necessary", "may exceptionally" and subsidiarity requirement in Art.

[44] European Commission, Commission Staff Working Document, 19.11.2025, SWD (2025) 836 final (p. 2).

4a(1) lit. a AIA draft).[45] The same applies to the necessity and proportionality requirements according to Art. 4a(2) AIA draft. Hence, the practical impact seems limited. If cumulation of the elements in paragraph 1 and 2 was not intended, the requirements of Art. 4a(1) AIA draft need not be fulfilled. Nevertheless, the necessity and proportionality clause in Art. 4a(2) AIA draft establishes a high burden. In order to specify the elements required and increase legal certainty, we recommend a further clarification. To conclude, due to the high requirements of Art. 4a(2) AIA draft, the expected impact is low.

Lastly, the interplay with the proposed Art. 3(15) DO is welcome. Art. 3(15) DO introduces a new Art. 88c GDPR draft which is intended to serve as a legal basis for processing personal information in the context of development and operation of AI. Assuming that development and operation include bias detection and mitigation, providers can rely on this basis for the processing of non-special category personal data. The proposed Art. 4a AIA draft adds to this by providing a specific legal basis for non-special category personal data for the specific context of bias detection and mitigation. This frictionless interaction between those two provisions is prima facie welcome. Nevertheless, the proposed Art. 88c GDPR draft raises certain obstacles for fundamental rights and issues related to legal certainty (as discussed below) that need further consideration.

2.2.1.4. AI Regulatory Sandboxes at the EU Level

Art. 1(17) DOAI contains several amendments to Art. 57 AIA. The AI real-world laboratories to be established in each Member State pursuant to Art. 57(1) AIA are intended to support providers of AI systems, in particular SMEs, in fulfilling their obligations under the AIA, in particular in connection with the conformity assessment for high-risk AI systems.[46]

The expansion of AI regulatory sandboxes and real-world testing environments is a useful instrument for innovation and regulatory learning and, in principle, welcome.

The proposed amendments to Art. 57 and 58 AIA introduce the possibility for the AI Office to establish EU-level regulatory sandboxes for certain AI systems, including those based on general-purpose AI models within the meaning of Art. 1(25) DOAI. These EU-level sandboxes would complement the regulatory sandboxes to be established at national level pursuant to Art. 57 AIA.

While Art. 57(10) AIA explicitly requires the involvement of national data protection authorities (DPAs) in national sandboxes where personal data is processed, and therefore, the fundamental right to informational self-determination under Art. 8 of the Charter of

---

[45] Ossmann-Magiera, Markschies, Data Governance under the AI Act in: Artificial Intelligence and Fundamental Rights, Raue / von Ungern-Sternberg / Kumkar / Rüfner (ed.), 75, 85. (https://irdt-schriften.uni-trier.de/index.php/irdt/catalog/book/6), p. 85; see also Surjadi, Die Rechtmäßigkeit der Verarbeitung sensibler Daten nach Art. 10 Abs. 5 AI Act – Ein Durchbruch für das Debiasing von KI-Systemen?, in Heinze and Steinrötter (eds.), KI und Daten: Digitalregulierung auf dem Höhepunkt?, 2024.

[46] Borges, Per Omnibus zur besseren KI-Gesetzgebung? - Zur Reform der KI-Regulierung im sog. „Digitalen Omnibus"-Paket, CR 2026, 131-141.

Fundamental Rights (CFREU)[47] is concerned, we recommend an equivalent provision that exists for EU-level sandboxes. Given that such sandboxes may equally entail the processing of personal data, we recommend clarifying in the AIA draft that competent DPAs should be associated with the operation of EU-level sandboxes and involved in the supervision and enforcement of the relevant data processing, in accordance with Art. 55 GDPR.[48]

Moreover, the identification of the competent DPA in the context of EU-level sandboxes, as well as the interaction with the GDPR cooperation mechanism remains unclear. Although Art. 58(1)(d) AIA mandates the European Commission to adopt an implementing act laying down common principles on the governance of regulatory sandboxes, issues relating to DPA competence and coordination should be addressed directly in the AIA. We therefore recommend amending Art. 57 AIA draft to explicitly refer to the advisory role of DPAs on data protection aspects.

The obligation introduced in Art. 57(14) AIA draft for national competent authorities to support the joint establishment and operation of regulatory sandboxes is welcome, as it may foster coordinated cross-border approaches. However, further clarification is needed as to how this obligation will be implemented in practice.

Finally, a clear distinction should be maintained between regulatory sandboxes for Union institutions, bodies, offices or agencies established by the EDPS under Art. 57(3) AIA, and the EU-level sandbox established by the AI Office under Art. 57(3a) AIA draft. According to Art. 57(3a) AIA draft the AI Office may establish an AI real-world laboratory for general-purpose AI (GPAI) systems within the meaning of Art. 75(1) AIA.[49] In line with Recital 14 DOAI, AI systems placed on the market, put into service or used by Union institutions would not fall within the scope of the EU-level sandbox under Art. 57(3a) AIA draft, as the EDPS remains the sole competent authority for such systems under Art. 74(9) AIA.

2.2.1.5. Registration Obligation in the EU Database and Required Amendments to Article 71 AIA

Art. 1(6), (14), (32) DOAI delete the obligation for providers to register AI systems in the EU database for high-risk AI-systems which are exempted from the high-risk AI obligations under Art. 6(3) AIA ("exempted systems"). Specifically, three changes are made within this context. Most centrally, the deletion of Art. 49(2) AIA through Art. 1(14) DOAI removes the registration obligation for exempted systems. Secondly, Art. 1(6) DOAI is a mere technical adjustment which eliminates the reference to Art. 49(2) AIA in Art. 6(4) 2nd sentence AIA. Lastly, Art. 1(32) DOAI removes Annex VIII section B of the AIA which specifies the required registration details for systems exempted under Art. 6(3) AIA.

---

[47] Charter of Fundamental Rights of the European Union, 2012/C 326/02.

[48] EDPB-EDPS Joint Opinion 1/2026, On the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).

[49] Borges, Per Omnibus zur besseren KI-Gesetzgebung? - Zur Reform der KI-Regulierung im sog. „Digitalen Omnibus"-Paket, CR 2026, 131-141.

A combined reading of the proposed changes with Art. 71(1) and (2) AIA leads to legal uncertainty. To avoid this, changes to those provisions are recommended.

Art. 71(1) 1st sentence AIA obliges the European Commission to set up a database for HRAI systems, including systems exempted from HRAI obligations under Art. 6(3) AIA but required to nevertheless register in the database due to Art. 6(4) 2nd sentence AIA. As explained, the Digital Omnibus on AI proposes to remove the registration obligation for exempted systems under Art. 6(4) AIA. This raises the question of how the still existing obligation of the European Commission to set up a database under Art. 71(1) 1st sentence AIA should be interpreted. Since the existing compulsory obligation for exempted systems to register is removed, the only explanation would be the possibility of voluntary registration. Hence, not the registration possibility as such is removed, only the obligation thereto. However, this reading of the law lacks support in the precise wording or the recitals. At the same time, there are valid arguments against such interpretation.

Firstly, the specificities of registration for exempted systems, which were previously found in Annex VIII, section B of the AIA are removed. This results in the following: even if a deployer wanted to make a voluntary registration, it is unclear which details would have to be submitted. Secondly, voluntary registration usually leads to legal consequences (i.e. privileges). Those are neither provided for in the AIA, nor in the Digital Omnibus on AI. Lastly, corresponding Recital 9 DOAI specifically states that the registration requirement is removed. There is no mention of a replacement with a voluntary obligation. To conclude, there are no substantive arguments for a voluntary registration option. For that reason and to increase legal certainty, Art. 71(1) AIA must be adjusted by removing "and AI systems that are not considered as high-risk pursuant to Art. 6(3) and which are registered in accordance with Art. 6(4) and Art. 49". Further, Art. 71(2) AIA refers to Annex VIII section B of the AIA. Due to the removal of this section via Art. 1(32) DOAI, the link is superfluous. This provision should also be adjusted by removing "and B".

By excluding AI-systems used solely for preparatory or ancillary activities from the EU database, the proposal aligns the registration obligation more closely with actual risk exposure.[50] Despite the targeted purpose of administrative relief, the proposed removal of registration obligations for certain high-risk AI systems in the EU database warrants critical scrutiny with regard to judicial and quasi-judicial contexts. Even AI systems that perform ostensibly technical or procedural functions in judicial proceedings may have a significant impact on the rights of affected persons. Transparency and traceability are therefore of particular importance in this area. Any relaxation of registration or documentation obligations should carefully consider the specific sensitivity of judicial applications and thus should be subject to review in some years' time.

[50] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin.

Furthermore, this adjustment may seem to enhance efficiency, but it also reduces the informational value of the EU database as a comprehensive oversight tool.[51] The database will therefore increasingly reflect a curated subset of high-risk AI systems, rather than the full universe of systems formally classified as high-risk under Annex III, which may limit its usefulness for supervisory coordination and systemic risk analysis.

2.2.1.6. Implementation Timeline of High-Risk-Rules

Another important element in the proposal is the proposed postponement of the temporal scope of application of the rules on high-risk AI-systems, pursuant to Art. 113 (2)(3) lit. c AIA, these rules are applicable from 2 August 2026 and 2 August 2027, respectively. In order to be in time to postpone these deadlines, the legislative process is under extreme time pressure: the Digital Omnibus on AI must be published by 28 July 2026 at the latest.[52]

Art. 1 (31) DOAI aims to remedy this situation. The provision provides for an addition to Art. 113 (3) AIA. The new lit. d) in Art. 113 (3) AIA draft, which differentiates between high-risk AI systems within the meaning of Art. 6 (1) and (2) AIA, makes the temporal applicability of Art. 6-27 AIA (Chapter III, Sections 1-3 of the AIA) dependent on two different criteria: according to the Art. 113(3) lit. d) AIA draft, the rules apply to high-risk AI systems within the meaning of Art. 6(2) AIA from 2 December 2027 at the latest, and to high-risk AI systems within the meaning of Art. 6(1) AIA, no later than 2 August 2028.

However, according to Art. 113 (3) lit. d) 1st sentence AIA draft, the rules may already be applicable before these dates if the European Commission determines by means of a decision that appropriate measures are in place to support compliance with Chapter III. In this case, Art. 6-27 AIA shall apply to high-risk AI systems within the meaning of Art. 6 (2) AIA six months after the adoption of this decision, and to high-risk AI-systems within the meaning of Art. 6 (1) AIA twelve months after the adoption of this decision, Therefore, the regulation postpones the temporal scope of application of the rules on high-risk AI systems by up to 16 months for high-risk AI systems within the meaning of Art. 6 (2) AIA and by up to 12 months for high-risk AI systems within the meaning of Art. 6 (1) AIA.[53]

The proposed postponement of the application of certain obligations relating to high-risk AI systems may be justified in light of the current lack of accompanying EU-level measures, such as the designation of competent authorities on a national level and the availability of harmonised European standards.[54]

---

[51] Ibid.

[52] Borges, Per Omnibus zur besseren KI-Gesetzgebung? - Zur Reform der KI-Regulierung im sog. „Digitalen Omnibus"-Paket, CR 2026, 131-141.

[53] Borges, Per Omnibus zur besseren KI-Gesetzgebung? - Zur Reform der KI-Regulierung im sog. „Digitalen Omnibus"-Paket, CR 2026, 131-141.

[54] To Harmonised Standards and Conformity Assessments, see Weizenbaum-Institute, Harmonised Standards and Conformity Assessments in the AI Act: Strengthening Independent and Participatory Oversight, 2025

Nevertheless, from our point of view, it is essential that such transitional arrangements remain temporary and proportionate. Delays in the application of core protective provisions must not result in a de facto suspension of fundamental rights safeguards unless justifiably in the light of other interests and fundamental rights. Due to the specific risks of AI[55] (or even just machine learning processes) including their unpredictability, technical autonomy, lack of transparency, poor training data quality and susceptibility to discrimination, the timely establishment of the necessary institutional and procedural framework, e.g. transparency, therefore remains imperative.[56] Protection deficits should be avoided by allowing reasonable adjustment periods for AI systems that have already been placed on the market.

2.2.2 Concluding remarks on the Digital Omnibus on AI: No Simplification at the Expense of Fundamental Rights Protection

The use of AI, particularly in sensitive areas, entails significant risks for fundamental rights and the rule of law. This applies especially to high-risk AI systems within the meaning of the AIA, including systems used in the administration of justice. While the objective of reducing administrative burdens is understandable, any simplification of the regulatory framework governing high-risk AI systems take into account an adequate level of protection of the affected EU fundamental rights. This is particularly important given the rapid technological developments since the European Commission's original proposal for the AI Act in 2021. Accordingly, the simplification of obligations relating to high-risk AI systems should be approached with particular caution.

In conclusion, the DOAI proposes some welcome concentrations in procedural law. The extension of the simplifications for SMEs to SMCs is welcome, even if the specific simplifications are likely to be of little practical significance. It also seems sensible to strengthen AI sandboxes, but with greater involvement of data protection authorities due to their fundamental rights expertise. The DOAI, however, will not lead a reduction of obligations and the associated compliance effort. In our view, this would require a clarification of the substantive obligations and/or a solution involving regulatory assurances combined with immunity from fines[57], or even a partial transition from ex ante regulatory control to ex post liability control.[58] Therefore, we urge the European Commission to consider beyond the existing proposals where the AIA is unclear or inconsistent with other EU digital legislation and where it lacks fundamental rights protections , and to recognise the importance of national implementation and the development of technical standards.

---

[55] Hacker NJW 2020, 2142 (2143); Zech, Risiken digitaler Systeme, Weizenbaum Series #2, 2020, S. 24 ff., 44 ff., 50 ff.

[56] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin

[57] Heinze, Donald Trump, das Ende der Ampel und die Stunde der Gerichte im KI-Urheberrecht, KIR 2024, 149.

[58] Heinze, Der digitale Omnibus zur KI-VO – kleine Schritte, wenig Wirkung, KIR 2026, 25.

2.2.3 Digital Omnibus on GDPR

2.2.3.1. Article 4 (1) GDPR – The Definition of Personal Data

The question of what constitutes personal data, and indeed what does not, is the focal point of the GDPR. After all, the GDPR distinguishes between personal data, to which it is applicable, and non-personal data, to which it is not. The correct differentiation between the two has been the subject of much discussion, particularly with regard to the concepts of pseudonymisation and anonymisation.

This has resulted in years of scholarly debate on whether anonymisation should be understood as absolute or relative. The CJEU rulings in the cases of *Breyer*[59] and *EDPS v SRB*[60] have been pivotal in shaping the understanding of anonymisation as a relative concept, albeit one subject to significant restrictions.

The Digital Omnibus Draft seems to aim at codifying the case law. Art. 3 (1) lit. a DO is introducing an addition to Art. 4 (1) GDPR: "Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates".

Concerns have already been raised that the proposed new definition of Art. 4 (1) of the GDPR goes beyond the CJEU's decisions.[61] Although the CJEU favoured a relative approach, it was nevertheless clear in setting high standards. In any case, the issue of a re-identification by third parties outside EU/EEC should be addressed.

Additionally, Art. 10 DO introduces a new Art. 41a to the GDPR. This allows the European Commission to adopt implementing acts that specify the means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities. This provision appears to have the potential to clarify the definition of personal data and thus make it more operable.

However, the practical impact of this provision is questionable, as the wording of Art. 41a(3) GDPR-draft suggests that compliance with the implementing act may be used as *an element* to prove that reidentification is not possible.[62] This suggests that even compliance with the implementing act is no guarantee that data is no longer personal, which would not lead to

---

[59] CJEU, C-582/14, ECLI:EU:C:2016:779.

[60] CJEU, C-413/23 P, ECLI:EU:C:2025:645.

[61] EDPB-EDPS, Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus); Hofman, This is Not Simplification, VerfBlog 2026/1/03; Noyb, Digital Omnibus - Analysis of Select GDPR and ePrivacy Proposals by the European Commission, Version 2.0.

[62] EDPB-EDPS, Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus).

the envisaged legal certainty, but would instead add another layer of complexity to the definition of personal data. Furthermore, such implementing acts could be subject to an action for annulment in accordance with Art. 263 TFEU is Art. 8 CFREU were to be infringed.[63]

2.2.3.2. Article 4 (38) GDPR – Definition of Scientific Research

Scientific research continues to be privileged. Further processing for scientific purposes will have to be considered compatible with the purpose pursuant to Art. 6(4) GDPR-draft; research itself is expressly recognised as a legitimate interest. In this case, the controller does not require a separate legal basis (cf. Recital 50, sentence 2 of the GDPR).[64] This facilitates data-based research, which we welcome.

Despite this, the definition of *'scientific research'* in Art. 4 (38) DO has more than 20 criteria. In our opinion, such a definition can partly contradict the goal behind a legal definition which is to clarify uncertainties. The definition is extremely broad as it says in the proposed legal text "any research which can support innovation". Therefore, it is read as if commercial scientific research is included as well, even though the ethical standards for their research are often drafted by industry itself which can lead to a conflict with Art. 8, 13 of the CFREU.[65] The vague and unclear criteria of the proposed definition will most likely lead to problems regarding the enforcement for the supervisory authorities. We welcome the approach to further privilege scientific research under the GDPR with the implementation of a legal definition as there are privileges in other digital laws as well, e.g. Art. 40 of the Digital Services Act (DSA). However, the legal definition in its current state may even have unwelcome repercussions on scientific research in cases it is not clearly supporting "innovation".[66] Therefore, we recommend taking expert's input into account for the drafting of a definition of *'scientific research'*.

2.2.3.3. Article 88c GDPR

The proposed introduction of a new Art. 88c GDPR, aimed at facilitating the use of the legitimate interests legal basis in the context of AI-related processing, is, in principle, welcome. Clarification and guidance in this area may contribute to greater legal certainty. However, the current drafting raises interpretative uncertainties. In particular, it remains unclear whether the provision is intended to establish a new legal basis, specify legal consequences, or merely clarify the application of Art. 6 (1) (f) GDPR.[67] Ambiguity arises from the partial duplication of the wording of Art. 6 (1) (f) GDPR combined with the introduction of new, open-ended criteria, such as "appropriateness". Without further clarification, this may either be interpreted as

---

[63] Noyb, Digital Omnibus - Analysis of Select GDPR and ePrivacy Proposals by the European Commission, Version 2.0.

[64] Wiegand/Hillert: Europas Digitalrecht auf dem Prüfstand: Mit dem Digitalen Omnibuspaket setzt die EU Kommission zum Kurswechsel an, ZD-Aktuell 2025, 01470.

[65] Charter of the Fundamental Rights of the European Union (2012/C 326/02)

[66] EDPB-EDPS Joint Opinion 1/2026, On the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

[67] Heinze, Vision Europäischer Digitalkodex: KI-VO, KI-Haftungs-RL, DSGVO, Geschäftsgeheimnis-RL, Vortrag gehalten auf der DGRI-Jahrestagung 2025, 13. und 14.11.2025, Berlin

raising the threshold for legitimate interests or as creating redundant and confusing parallel requirements.[68]

To avoid such uncertainties, the provision should be clarified by explicitly defining its normative function, specifying concrete assessment criteria, and emphasising the relevance of AI processing for access to justice and the protection of confidential legal advice and representation. Moreover, we recommend that the provision concerns the lawfulness of processing under Art. 5 (1) (a) and Art. 6 GDPR and does not exempt controllers from compliance with other GDPR obligations.

2.2.4 Recommendations for Improvements within the Digital Omnibus Initiative

2.2.4.1. Key Recommendations for the Digital Omnibus on the AI Act

1. Privileges for SMEs and SMCs

We recommend a departure from the two-tier approach and simple privileges for SMEs and SMCs. Therefore, an adaptation of Art. 1 (9) and Art. 1 (21) DOAI is required. Furthermore, we recommend moving the additional SME privilege found in Art. 63 AIA draft to Art. 17 AIA. Lastly, we recommend giving precise enforcement guidance to meet the requirement in Art. 1 (29) DOAI to consider the interests of SMEs and SMCs when determining administrative fines under Art. 99 (1) AIA.

2. Maintain AI Literacy in Art. 4 AIA as a Binding Obligation

We recommend retaining Art. 4 AIA as an operator-centred legal obligation. Replacing it with an encouragement-based approach as proposed in Art. 1 (3) DOAI would undermine its systemic role and weaken fundamental-rights safeguards.

3. Improve Bias-Mitigation Data Processing Rules

We recommend repositioning bias-related data provisions for high-risk AI-systems back into Art. 10 AIA and clarifying the applicability and thresholds of Art. 4a AIA. The European Commission should clarify whether the conditions of Art. 4a (1) and Art. 4a (2) AIA are intended to apply cumulatively or alternatively and should preserve the coherent interaction with the proposed Art. 88c GDPR draft.

4. Data Protection Oversight in EU-level AI Sandboxes

EU-level regulatory sandboxes should explicitly require involvement of competent data protection authorities, ensuring GDPR-consistent supervision and avoiding governance gaps.

---

[68] Ibid.

5. EU Database Provisions

We recommend adjusting Art. 71 (1) AIA by removing the following part of the sentence "and AI systems that are not considered as high-risk pursuant to Art. 6 (3) AIA and which are registered in accordance with Art. 6 (4) and Art. 49 AIA". Furthermore, the Commission should amend Art. 71(2) AIA by deleting the reference to Annex VIII, Section B, which is removed by Art. 1(32) DOAI. We recommend reassessing the exclusion of certain high-risk AI systems from the EU database where such systems are used in judicial or quasi-judicial contexts.

6. Keep Postponements of High-Risk AI Rules Temporary and Conditional

We recommend specifying in Art. 113 (3) (d) AIA time-limited conditions that are tied to objective readiness criteria (e.g. availability of standards, designation of authorities) with interim safeguards to avoid protection gaps; in particular for AI systems already placed on the market.

2.2.4.2. Key Recommendations on the Digital Omnibus Initiative regarding the GDPR

1. Definition of Personal Data in Article 4(1) GDPR in accordance with CJEU case law

We recommend revising the proposed amendment to Art. 4 (1) GDPR to ensure that the definition of 'personal data' is in accordance with CJEU case law.

2. Clarify the Legal Consequence of Implementing Acts under Article 41a GDPR

We recommend specifying that compliance with implementing acts adopted under Art. 41a GDPR has a defined legal consequence. Without such clarification, the provision risks adding complexity and may expose implementing acts to annulment risks under Art. 263 TFEU.

3. Redraft the Definition of 'scientific research' in Article 4(38) GDPR with expert input

While privileging scientific research is welcome, we recommend reducing the number of criteria and clarifying the definition of *'scientific research'*. Therefore, expert's input should be incorporated.

4. Clarify the Normative Function of Article 88c GDPR

We recommend that the Commission clarifies whether Art. 88c GDPR creates a new legal basis, specifies the application of Art. 6 (1) (f) GDPR, or provides interpretative guidance. Otherwise, redundant parallel tests will be the result.

3 Concluding Remarks

The consolidation of European digital legislation is both necessary and desirable in light of the growing complexity of the EU digital acquis. The two Digital Omnibus proposals represent an important step towards improving the practical applicability of EU digital regulation. At the same time, simplification measures in the fields of artificial intelligence and data protection must be carefully examined in order to preserve the existing level of fundamental rights protection where required and appropriate; overprotection should be avoided though. A meaningful streamlining effort should begin with greater clarity at the level of substantive rules. The different categories of norm accumulation continue to undermine legal certainty, and the Digital Omnibus Initiative only partially addresses these structural shortcomings. The EU Digital Legislation is welcomed in its objectives. A more coherent and systematically aligned digital regulatory framework would strengthen both the credibility and the global competitiveness of EU digital regulation. Legal clarity is a precondition for simplification, and therefore innovation.

Imprint

Weizenbaum Institute and German Society for Law and Informatics
Structural Challenges of EU Digital Legislation and Targeted Simplification Through the Digital Omnibus Initiative

Weizenbaum Policy Paper # 20
Berlin, March 2026

ISSN 2940-8490 \ DOI 10.34669/WI.PP/20

Weizenbaum Institute
Hardenbergstraße 32 \ 10623 Berlin \ Tel.: +49 30 700141-001
info@weizenbaum-institut.de \ www.weizenbaum-institut.de

COORDINATION: Dr. Moritz Buchner

DISCLAIMER: This publication presents research-based information. The contents reflect the views of the Weizenbaum Institute at the time of publication. Use of this publication is the sole responsibility of the reader. Under no circumstances shall the Weizenbaum Institute, its legal representatives, authors, editors or other parties involved be liable for any damages, whether direct or indirect, resulting from the use of this publication. All rights, including the right to reproduce excerpts, are reserved by the Weizenbaum Institute and the German Society for Law and Informatics. Weizenbaum Policy Papers provide scientifically grounded statements, position papers, and briefings on current political topics and decision-making processes.

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

weizenbaum institut

With funding from the:
Federal Ministry of Research, Technology and Space
BERLIN Senate Department for Higher Education and Research, Health and Long-term Care