European Journal of Risk Regulation (2026), 1–18
doi:10.1017/err.2026.10121

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

From a Right-Based Approach to Competitiveness? The EU Digital Omnibus Reform

Giovanni De Gregorio[1] and Hannah Ruschemeier[2]

[1]Católica Global School of Law, Universidade Católica Portuguesa, Lisbon, Portugal and [2]Faculty of Law, Osnabrück University, Osnabrück, Germany

Corresponding author: Hannah Ruschemeier; Email: hannah.ruschemeier@uos.de

Abstract

The European Union has advanced its agenda towards regulatory simplification. At first glance, the Digital Omnibus can indeed be considered a recalibration of EU digital policy from a rights-based paradigm towards an approach increasingly shaped by competitiveness and efficiency. However, while the omnibus proposals raise legitimate concerns about the possible dilution of the Union's constitutionally oriented approach, they do not merely represent a simplification effort and a retreat from regulation. This paper argues that the approach towards simplification has not reduced the path towards the regulatory expansion of European digital policy. While focusing towards simplification, the Union approach seems to increase risks for fundamental rights and legal certainty while continuing to expand its digital agenda, as in the case of the Digital Services Act. This dual movement, presented as a coupling of simplification and regulatory expansion, is likely to make European digital regulation even more convoluted, thus increasing risks for fundamental rights and legal certainty. By looking at the goals of European digital constitutionalism, which focuses on the reframing of rights and power in the algorithmic society, the paper contends that the EU's priority should shift away from this dual track and should not rely on simplification as a way to address constitutional questions which would require a broader strategy as in the case of enforcement.

Keywords: AI Act; digital constitutionalism; GDPR; omnibus; regulation

I. Introduction

Things are moving fast in the field of EU digital regulation. In times of poly-crisis and unprecedented uncertainty in geopolitical relations, the pressure on institutions like the European Union is high. Political compromise, often hard-won, is increasingly complicated by external exigencies, and this is reflected in the pursuit of a regulatory framework for the digital age, meeting dynamics that lead the EU to question, at least externally, its approach.[1] Instead of waiting for the planned Digital Fitness Check intended to simplifying and reducing bureaucracy within EU digital law and regulation,[2] the Commission proposed various amendments in the Digital Omnibus package as a way to address questions of competitveness and strategic autonomy.

[1] F Bieker and K Nolan, European AI FOMO: The European Commission Sacrifices the Digital Acquis at the Altar of AI Hype, Verfassungsblog 2026.

[2] "An Agile Digital Rulebook for the EU | Shaping Europe's Digital Future" (26 March 2026) <https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook> (last accessed 31 March 2026).

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial licence (https://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original article is properly cited. The written permission of Cambridge University Press or the rights holder(s) must be obtained prior to any commercial use.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

The legislative processes of the Digital Services Act (DSA) and the AI Act[3] have been already accompanied by heated discussions about European sovereignty, security and competitiveness.[4] Since then, in the legal–political discussions nearly ubiquitously present Draghi report,[5] the European approach to digital regulation has changed. It has increasingly shifted from a self-conception as a global rule-setter, emphasising the Brussels effect,[6] centring fundamental rights and "European values" as the guiding principles,[7] to echoing calls for simplification and competitiveness. The Commission's 2030 "Digital Decade" policy program, which seeks to institutionalise a person-centred digital environment for the Union's citizens and enterprises and, in doing so, to lead to an explosion of European digital regulation, is under pressure.

This trend towards boosting the internal market has intensified to the point that over half of the Commission's 2026 proposals are structured as Omnibus acts. These instruments now try to intervene in a heterogeneous array of sectors, ranging from digital governance and environmental policy to taxation, automotive standards and the legal status of Union citizenship. Furthermore, these comprehensive packages of legislative amendments lead to extensive changes in regulatory content, especially in the protection of individuals and fundamental rights, to foster "innovation and competitiveness."[8] Calls for strategic autonomy and digital sovereignty seem mainly driven by the assumption that overly stringent rules may disadvantage European firms *vis-à-vis* global tech giants, thereby reshaping the balance between market integration and the EU's strategic positioning in the digital economy.[9] However, pursuing competitiveness through deregulation is a perilous strategy, given that it could increase complexity coming from interpretative challenges and, broadly, actively reward entities currently operating in bad faith while penalising those that have invested in rigorous legal compliance.[10] Moreover, this approach does not necessarily align with the approach towards strategic autonomy, which the Union considers as one of the priorities for competitiveness. Efficiency can also be a way to challenge the protection of fundamental rights and democratic values.[10] The previous approach of the Union towards digital constitutionalism, as also underlined in the Commission's 2030 "Digital Decade" policy program, which seeks to institutionalise a person-centred digital

[3] 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.

[4] See, for example: F Palmiotto, "The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation" (2025) 16 European Journal of Risk Regulation 770 <https://doi.org/10.1017/err.2024.97>; B Mueller, "How Much Will the Artificial Intelligence Act Cost Europe?" (2021) <https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe/> (last accessed 31 March 2026).

[5] M Draghi, *The Future of European Competitiveness: Part A: A Competitiveness Strategy for Europe* (European Commission ed, Publications Office 2024) <https://doi.org/10.2872/1823372>.

[6] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

[7] C.f. JHH Weiler, "The Transformation of Europe" [1991] Yale Law Journal 2403 <https://doi.org/10.2307/796898>; O Lynskey, "Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order" (2014) 63 International & Comparative Law Quarterly 569 <https://doi.org/10.1017/S0020589314000244>.

[8] A Alemanno, "The Omnibus Road to Constitutional Drift" [2025] Verfassungsblog <https://doi.org/10.17176/20251112-142022-0> (last accessed 23 February 2026).

[9] The following paper argues that the choice between innovation and regulation is a false dichotomy: A Bradford, "The False Choice Between Digital Regulation and Innovation" (2024) 119 Northwestern University Law Review 377.

[10] Ruschemeier, "The Omnibus Package of the EU Commission" (n 8); H Ruschemeier, "The Omnibus Package of the EU Commission" [2025] Verfassungsblog <https://doi.org/10.17176/20251118-142049-0> (last accessed 12 January 2026).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

environment for the Union's citizens and enterprises and, in doing so, to lead to an explosion of European digital regulation,[11] is under pressure.

However, this paper argues that the amendments introduced through omnibus proposals, although critical, should not be read simply as a common endeavour to move towards deregulation. Rather, they are complementary to a digital regulatory agenda that remains very much active and expanding. This reflects a double-edged development in the EU's approach. On the one hand, the Union is bundling diverse policy areas under the banner of simplification raising serious concerns regarding the potential weakening of fundamental rights protections and legal certainty. On the other hand, it continues to expand European digital regulation as in the case of the Digital Networks Act or the discussion on the Digital Fairness Act. The Digital Omnibus proposals indeed do not address all areas of digital regulation, leaving frameworks like the DSA untouched. Therefore, it would be inaccurate to consider the Omnibus approach as a simplification strategy changing the European approach to digital regulation, but it should be considered as a reshape in ways that may even further affect European constitutional values.

Moreover, this paper underlines how the Union's priority should shift away from this dual track and focus on enforcement, ensuring that existing rules are implemented consistently and achieve their objectives. The central challenge for the EU is no longer the proliferation or refinement of legislative instruments, but the capacity to ensure their effective enforcement. Rather than continuing to reshape an already dense regulatory framework or even expanding it, priority should be given to strengthening enforcement coordination and enhancing supervisory capacities in Europe. A streamlined enforcement strategy would not only improve legal certainty and compliance but also reinforce the credibility of the European digital agenda.

The first part of the paper analyses the main changes introduced through the first proposals of the Digital Omnibus strategy to key instruments such as the AI Act and the GDPR, highlighting how, even without touching the structure of these instruments, these amendments reshape core obligations, including adjustments to compliance timelines for high-risk AI systems. Second, the paper underlines that the EU digital regulatory agenda has not stalled. On the contrary, it has changed the way of expansion and diversification of the Union's approach to digital governance, underlining that the deregulatory tendencies in the Omnibus package should not be equated with the EU's broader digital agenda. Third, the paper argues that the EU should focus on enforcement challenges, as the increasingly complex and layered framework poses significant risks, particularly regarding the protection of fundamental rights and the rule of law.

II. The omnibus digital package: falling for AI Fomo and efficiency narratives

The amendments to the digital *acquis* via the Omnibus package have primarily succumbed to uncritical demands for deregulation.[12] The frustration with Europe's perceived lag in AI enterprise development is an expression of the tech industry's successful innovation narrative. This mindset adopts a techno-deterministic view, in which innovation is seen as a self-evident good to be pursued without restriction, and any regulatory framework is dismissed as a structural hindrance to technological advancement.[13] Innovation is

[11] M Müller and MC Kettemann, "European Approaches to the Regulation of Digital Technologies" in H Werthner and others (eds), *Introduction to Digital Humanism: A Textbook* (Springer Nature Switzerland 2024) <https://doi.org/10.1007/978-3-031-45304-5_39> (last accessed 23 February 2026).

[12] R Mahieu, "The Ominous Omnibus" [2025] Verfassungsblog <https://doi.org/10.59704/a5de32786423a76c> (last accessed 31 March 2026).

[13] H Ruschemeier, "The De-Regulatory Turn of the EU Commission" [2025] Verfassungsblog <https://doi.org/10.59704/b61325ec5f72184a> (last accessed 23 February 2026).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

frequently weaponised as an all-encompassing good that trumps specific legal protections. This narrative thrives because AI-inflicted harms are notoriously difficult to prove or prevent, leading to a discourse that favours abstraction over accountability.

Within this framework, the regulation of data and AI stands at the centre of current political discussions. Even as the EU broadens its digital acquis through other regulatory measures, the GDPR remains the cornerstone of digital governance, applying to all personal data processing regardless of the medium. In this sense, the GDPR is the operational embodiment of the Union's constitutional values, specifically proportionality, fundamental rights, and democratic accountability.[14] Furthermore, the AI Act was intended to be the first horizontal regulation, explicitly addressing the risks posed by AI and establishing a European framework for AI governance.[15] As we will show with the following examples of amendments to the AI Act and the GDPR, the Digital Omnibus proposal is first a deregulatory turn by the Commission, succumbing to AI Fomo and efficiency narratives, even if, as underlined in the following section, it has not slowed down the path of European digital policy and regulation.

1. Revising the GDPR

The Omnibus amendments of the GDPR have the potential to shake up European data protection to its core. Despite the multitude of regulatory acts in the field of digital regulation, the GDPR remains the cornerstone since it addresses the processing of personal data – an inherent feature of many digital technologies.[16]

The proposed amendments of the GDPR would change the scope of application and curtail fundamental rights protection. Nevertheless, the EU does not abandon or change the individual-rights-centred approach of data protection. This would not be possible even through an amendment to secondary law, simply because the scope of protection is enshrined in primary law under Article 16 TFEU and Article 8 of the Charter of Fundamental Rights.

Against this background, it is notable that the working staff document accompanying the Omnibus proposal does not address fundamental rights or data protection at all. Instead, the changes to the GDPR are discussed solely in terms of businesses and compliance costs as the main issues.[17] Furthermore, it explicitly refers to the potential cost savings of the GDPR amendments.[18] The proposed changes include more than a dozen provisions of the GDPR, and a detailed discussion of all amendments lies beyond the scope of this paper.[19] Instead, we focus on specific provisions that are particularly relevant to digital constitutionalism and the protection of fundamental rights.[20]

[14] E Celeste and G De Gregorio, "Digital Humanism: The Constitutional Message of the GDPR" (2022) 3 Global Privacy Law Review <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2022002.pdf> (last accessed 28 March 2026); R Mühlhoff and H Ruschemeier, "Predictive Analytics and the Collective Dimensions of Data Protection" (2024) 16 Law, Innovation and Technology 261 <https://doi.org/10.1080/17579961.2024.2313794>.

[15] C Chang, "The First Global AI Treaty: Analyzing the Framework Convention on Artificial Intelligence and the EU AI Act" [2024] U. Ill. L. Rev. Online 86.

[16] PL Lau, "The AI Act and Data Protection: The Interplay Between Artificial Intelligence and Data: The AI Act and the GDPR" in VL Raposo (ed), *The European Artificial Intelligence Act: Promises and Perils?* (Springer Nature Switzerland 2025) <https://doi.org/10.1007/978-3-031-98406-8_12> (last accessed 28 March 2026).

[17] "Digital Omnibus Regulation Proposal | Shaping Europe's Digital Future" <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal> (last accessed 4 March 2026), p 34 et seq.

[18] Ibid., p 36.

[19] See for a detailed overview of all GDPR changes: "NOYB Omnibus Report V.3." (NOYB 2026) <https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf>.

[20] Even as consumer-friendly perceived changes like the new Article 88b are supposed to come into force only 6 months to 4 years (paragraph 6) following the entry into force of the new GDPR.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

However, the proposals in the digital omnibus risk eroding the GDPR's protection standards, break with the GDPR's principle of technological neutrality, and further complicating data protection requirements for researchers. Moreover, the extent to which European enterprises, particularly SMEs, are intended to benefit remains opaque, while online platforms and AI providers as data controllers stand to gain from the retroactive legalisation of their business practices.[21] Furthermore, the objective of simplifying the dense EU regulatory framework remains unfulfilled, as evidenced by the interplay between Article 9 of the GDPR and Article 10 of the AI Act.

a. Changing the definition for personal data

Amendments to the GDPR, especially those affecting its scope and definition, will have far-reaching consequences for data protection in Europe. The proposed amendment does not merely implement recent CJEU case law.[22] Indeed, this case law already demonstrates that an amendment to the statutory wording is not required to interpret the concept of personal data in a relative and contextual manner. Rather, the amendment sacrifices the legal certainty established by years of CJEU jurisprudence. The Omnibus proposes to change the definition of personal data under Article 4(1) GDPR by adding the following paragraph to the current provision[23]:

> 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.

Under the current definition, information related to an identified or identifiable natural person is considered personal data. Anonymised data, on the other hand, falls outside the scope of the GDPR, which requires a risk assessment: focusing on under what circumstances can data still lead to the re-identification of individuals. The understanding of anonymisation under the GDPR requires a normative, not a purely technical assessment.[24] Following this, the prevailing definition of "identifiability" is rooted in objective criteria derived from Article 8 of the CFR and CJEU jurisprudence. Under a

[21] "Article by Article, How Big Tech Shaped the EU's Roll-Back of Digital Rights | Corporate Europe Observatory" <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights> (last accessed 13 February 2026); N Helberger and others, "EU Consumer Protection 2.0" [2021] Structural Asymmetries in Digital consumer Markets. Joint Report from EUCP2. 0 Project BEUC; Mühlhoff and Ruschemeier (n 16); Kollnig (Konrad) and others, "Before and after GDPR: Tracking in Mobile Apps" (21 December 2021) <https://doi.org/10.14763/2021.4.1611> (last accessed 15 May 2026).

[22] A Golland, "Datenschutzrechtliche Auswirkungen Des Digital Omnibus" [2026] Zeitschrift für Rechtspolitik 2.

[23] Art. 4(1) states: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

[24] M Finck and F Pallas, "They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR" (2020) 10 International Data Privacy Law 11 <https://doi.org/10.1093/idpl/ipz026>; V Rupp and M von Grafenstein, "Clarifying "Personal Data" and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection" (2024) 52 Computer Law & Security Review 105932 <https://doi.org/10.1016/j.clsr.2023.105932>.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

framework dating back to the Data Protection Directive, data loses its "personal" status if re-identification by the controller or a third party is improbable. Specifically, the CJEU's *Breyer*[25] ruling established that identification is unlikely if the risk is "de facto insignificant", meaning the process is either legally prohibited or practically unfeasible due to excessive time, cost, or effort. However, the Court clarified that data remains identifiable if the controller has a legal pathway to obtain necessary supplemental information, such as through state authorities or publicly available information. The proposed changes narrow the understanding of personal data significantly, which creates at least three new problems.

First, from a general regulatory perspective, the change in the definition of personal data poses a high risk of creating legal uncertainty. While others argue that clarifying undefined terms is a drafting question or should be clarified by courts, this illustrates even more clearly that these changes are unnecessary. A change of the definition of personal data invalidates decades of ECJ case law on the GDPR and the Data Protection Directive.[26] Since such changes affect the scope of the GDPR, an immense amount of uncertainty would arise for courts, regulators, data subjects, operators, industry and research, encompassing all areas where the GDPR applies. Many entities that have created GDPR-compliant business models would have to re-evaluate them. It is unclear how the competitiveness of the European economy would profit from that. Rather, it is highly likely that actors whose business models do not comply with the GDPR could profit from new legal uncertainty regarding the regulation's scope.

Second, the proposal bifurcates responsibility by tethering the probability of re-identification strictly to the individual data controller. The working staff document claims that the amendments take the "recent case-law" of the CJEU into account and address the SRB ruling[27] indirectly.[28] While the changes align with the intuitive principle that one cannot be held liable for factors outside their control – and ostensibly mirror the CJEU's *SRB v EDPS* ruling – this interpretation is arguably reductive. In *SRB v EDPS*, the court specifically addressed a narrow scenario involving the matching of IDs with comments, yet it explicitly reaffirmed the *Breyer* standard: personal data status does not require all identifying information to be held by a single entity (para. 99). As the EDPD/EDPS pointed out, the GDPR, including the foundational definition of personal data, must be interpreted in light of the CJEU's comprehensive body of jurisprudence. The Proposal's attempt at selective codification, by extracting a single element from an isolated case, fails to account for the necessary judicial context and risks distorting the settled interpretation of data protection law.[29] Conversely, the current draft dismisses the potential to identify subsequent recipients, even when such means are reasonably likely. This creates a "diffusion of responsibility" in which entities lacking technical re-identification capabilities might claim that pseudonymized data falls entirely outside the GDPR's ambit. By fragmenting processing procedures to circumvent obligations, this approach risks

[25] *Patrick Breyer gegen Bundesrepublik Deutschland* [2016] ECJ Rechtssache C-582/14.

[26] Finck and Pallas (n 25).

[27] Case C-413/23 P: Judgment of the Court (First Chamber) of 4 September 2025 – EDPS v SRB (Concept of personal data) (Appeal – Protection of natural persons with regard to the processing of personal data – Procedure for granting compensation to shareholders and creditors of a banking institution following the resolution of that institution – Decision of the European Data Protection Supervisor finding that the Single Resolution Board failed to fulfil its obligations relating to the processing of personal data – Regulation (EU) 2018/1725 – Article 15(1)(d) – Obligation to inform the data subject – Transmission of pseudonymised data to a third party – Article 3(1) – Concept of personal data – Article 3(6) – Concept of pseudonymisation) 2025.

[28] "Digital Omnibus Regulation Proposal | Shaping Europe's Digital Future" (n 8), p 38.

[29] "EDPB-EDPS Joint Opinion on the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI) | European Data Protection Supervisor" (12 February 2026), p 10. <https://www.edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/2026-01-20-edpb-edps-joint-opinion-simplification-implementation-harmonised-rules-artificial-intelligence-digital-omnibus-ai> (last accessed 11 February 2026).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

eroding data subjects' rights and core principles like purpose limitation and accountability, leaving subjects unable to exercise rights over processing they are not even aware of.

Third, attempting to redefine "personal data" through negative definitions risks generating severe legal uncertainty rather than resolving it.[30] Such a negative framing inevitably creates grey areas regarding which datasets fall outside the scope of the law, complicating compliance for data processors and regulatory authorities. This uncertainty is exacerbated by the proposition that the European Commission could be entrusted to determine, via implementing acts, what no longer constitutes personal data post-pseudonymisation. Granting the Commission such power is highly problematic from a constitutional standpoint, as it effectively allows an executive body to dictate the material scope of application for EU data protection law. Furthermore, justifying such sweeping regulatory shifts by claiming a change in judicial direction is legally baseless. The CJEU, in its landmark EDPS v. SRB judgment, did not fundamentally alter the established jurisprudence or the core understanding of the definition of personal data. Consequently, manipulating this foundational definition via executive or legislative shortcuts creates a dangerous precedent that undermines the very predictability of the EU digital acquis.

The proposed amendments to the definition of personal data contributed to creating a conflict with the current logic of European data protection law, as also based on the jurisprudence of the CJEU. Furthermore, it remains entirely unclear how the competitiveness of European enterprises that have already developed data-compliant business models is to be strengthened by altering the definition of personal data. The proposed amendment in no way reflects a risk-based approach, which would, for instance, privilege SMEs over massive data controllers, as online platforms.

b. Legal basis for AI training and deployment

The proposed changes to Articles 9 and 88c GDPR pursue the clearly politically motivated goal of retroactively legitimising existing data processing practices in the context of AI, particularly by large model providers which are not in compliance with the GDPR.[31] On the one hand, this represents a capitulation of the previous legal situation to Silicon Valley's motto of "move fast and break things" or simply "break the law". On the other hand, it is completely unclear how the European AI economy in particular is supposed to benefit from these amendments.

The proposed Article 9(2)(k) and (5) introduces a novel derogation from the general prohibition on processing sensitive personal data outlined in Article 9(1). Under this new provision, such processing is permissible when carried out specifically for the development and operation of an AI system, as defined in the AI Act. Paragraph 5 calls for "appropriate" organisational and technical measures in the case of AI training and operation with sensitive data.

The design of this new provision alone is worthy of remark, since the norm not only imposes a mandatory obligation but also offers a "Plan B" to take effect if that obligation is not fulfilled.[32] Initially, the permission to process special categories of personal data only applies if 'appropriate organisational and technical measures' have been implemented to avoid the collection and processing of sensitive data altogether. However, if the controller nonetheless finds sensitive data in the datasets despite such measures, they must remove it. This demonstrates, first, that the measures taken to avoid such data were evidently not appropriate, which is a contradiction of the provision's requirement. Second, it is unclear

[30] Ibid.; p 10.

[31] H Ruschemeier, "Generative AI and Data Protection" (2025) 1 Cambridge Forum on AI: Law and Governance e6 <https://doi.org/10.1017/cfl.2024.2>.

[32] N Forgó, "Editorial" (*KIR*) <https://rsw.beck.de/zeitschriften/kir/editorial> (last accessed 29 March 2026).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

how these data, which strictly speaking should not exist at all, are to be reliably and, above all, verifiably searched for and identified by a controller who will have little interest in doing so. If the removal of such incidental findings were only possible with disproportionate effort, the controller does not have to delete such data after all, but merely must reliably and without undue delay "effectively protect" them from being used for the output of the AI system or model, disclosed to third parties, or otherwise made accessible. It remains unclear who determines what proportionate measures are or how they relate to the rights of (non-identifiable) data subjects.

From a fundamental rights perspective, the proposed changes are not justifiable in their generality, as they entail a clear reduction in the level of protection for particularly sensitive data, which is offset only by a vague assumption of "AI innovation". Introducing an AI privilege clearly breaks with the GDPR's established technology-neutral approach without substantial justification.[33] The assumption that deploying any kind of AI system outweighs the protection of special categories of personal data is not in line with the constitutional value of data protection. The proposal disproportionately favours AI over other technologies without providing any prior risk assessment or the requirement to demonstrate the benefits of the system. Furthermore, the reference to "training an AI system" lacks the necessary normative precision to serve as a distinct regulatory category, making also compliance harder for public and private actors.

Introducing a broad exception for AI training and operation would largely place inference-based profiling of sensitive data outside Article 9, contrary to the aim of protecting Article 8 ECFR and to CJEU jurisprudence. This amounts to a legitimisation of prominent AI and ad-tech practices, while leaving legal uncertainty and compliance burdens largely intact for smaller controllers.[34]

The CJEU has furthermore clearly established that processing based on Article 9 of the GDPR is "lawful only if it complies not only with the requirements resulting from that provision, but also fulfils at least one of the conditions for lawfulness set out in Article 6(1)".[35] This is intended to be guaranteed by the redefinition of legitimate interest under the new Article 88c. This new provision similarly generates greater legal uncertainty rather than simplification. As the EDPD/EDPS opinion has laid out, Article 88c simply states that processing in the context of the development and operation of AI systems may be pursued for legitimate interests, a statement that does not bring any legal clarification.[36] Furthermore, the problem that relying on legitimate interest as a legal basis for the processing of personal data requires assessing the three-step test established in the CJEU's jurisprudence remains. It specifically requires weighing the data subject's interests against the controller's. Therefore, it is necessary to identify data subjects and their interests to determine whether the controller's interests predominate. This kind of normative assessment relies on identifying fundamental rights positions and individuals and cannot be conducted in mass data processing, such as undifferentiated web scraping for AI training.[37]

While the proposal of Article 88c introduces a right to object, specifically "providing data subjects with an unconditional right to object to the processing of their personal data", it remains entirely unclear how this right is to be exercised. This operational

[33] On the background of technological-neutral regulation: EJ Koops, "Should ICT Regulation Be Technology-Neutral?" in BJ Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2006). On the GDPR specifically: N Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) 10 Law, Innovation and Technology 40 <https://doi.org/10.1080/17579961.2018.1452176>.

[34] Besides the questions of GDPR compliance, the problems of copy right law and AI training remain unsolved since the Omnibus does not touch upon this matter.

[35] CJEU C-667/21.

[36] "EDPB-EDPS Joint Opinion on the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI) | European Data Protection Supervisor" (n 29), p 16.

[37] Ruschemeier, "Generative AI and Data Protection" (n 32).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

ambiguity arises precisely because personal data cannot be easily extracted and erased once it has been integrated into a trained model.

c. Definition of scientific research

The GDPR addresses privileges for scientific research in different provisions, e.g., in Articles 5(1)(b) (e), 9(2)(j), 14(5)(b), 17(3)(d), 21(6), and 89 GDPR. Nevertheless, the GDPR has not provided a legal definition of scientific research in its regulatory text to date. In contrast, a very broad definition of "scientific research" is newly introduced in the new Article 4 No. 38. This definition encompasses any (type of) research, provided that it contributes to existing scientific findings or applies existing knowledge in a novel way and is conducted in compliance with relevant ethical standards with the aim of contributing to the growth of general knowledge and the well-being of society. Additionally, this shall include research carried out for commercial purposes in addition to these purposes. The aim is to clarify that scientific research constitutes a legitimate interest within the meaning of Article 6(1)(f) GDPR.[38] It is also proposed to extend the exceptions from the information obligation for processing under Article 13 by stipulating that, when the provision of information proves impossible, would involve a disproportionate effort, or would render the achievement of the objectives of that processing impossible or seriously impair it, the controller does not need to provide the information.

The proposed broadening of the definition of "scientific research" to encompass commercial "innovation" poses significant interpretative risks and threatens to dismantle core data protection safeguards. By introducing vague criteria, such as whether a project "can" lead to innovation, the proposal fails to answer who defines these relevant "ethical standards" or what threshold of probability is required. As the EDPD has strictly cautioned, the notion of scientific research "may not be stretched beyond its common meaning," maintaining that it must refer to a project "set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice". Abandoning this strict methodological boundary in favour of a nebulous "innovation" standard creates a dangerous loophole. It carries the potential to systematically undermine the principle of purpose limitation and the right to erasure, while simultaneously diluting the very academic privileges that the original research exemption was designed to protect.[39] Ultimately, rebranding commercial R&D as "scientific research" achieves regulatory relief at the cost of fundamental rights.

2. *Revising the AI Act*

The amendments proposed in the Omnibus package revising the AI Act come at a delicate moment in the evolution of the EU digital regulatory framework. These proposals come just a short time after the adoption of the AI Act, and most of the relevant obligations are not yet enforceable, particularly for high-risk AI systems. Although the Commission seems to be serious in revising the AI Act, in practice, the proposed amendments focus on specific and detailed areas, raising questions about the effectiveness of this simplification effort.

The proposals aim to streamline implementation of the AI Act by tying timelines for high-risk obligations to the availability of standards and support tools, extending SME-style simplifications to small mid-caps, easing documentation, monitoring, registration and penalty requirements, and shifting AI literacy obligations toward support from the

[38] "Digital Omnibus Regulation Proposal | Shaping Europe's Digital Future" (n 18).

[39] R Mühlhoff and H Ruschemeier, "Updating Purpose Limitation for AI: A Normative Approach from Law and Philosophy" (2025) 33 International Journal of Law and Information Technology <https://doi.org/10.1093/ijlit/eaaf003> (last accessed 29 March 2026).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

Commission and Member States rather than broad compliance duties. They also seek to centralise oversight of certain large-scale AI systems within the AI Office, expand access to regulatory sandboxes and real-world testing, enable safer use of sensitive data for bias detection and correction, and clarify how the AI Act interacts with other EU laws to improve overall implementation and operational efficiency.

These proposals signal an attempt by the European Commission to address early concerns about regulatory complexity and compliance costs while maintaining the regime's broader architecture. At the same time, they raise fundamental questions, some of which are addressed in this section, about whether these targeted interventions contribute to simplification or whether they instead reinforce an already intricate regulatory landscape without addressing structural tensions, which were already highlighted before the adoption of the AI Act.[40]

a. Revising rules for high-risk AI systems

The extension of the schedule for the entry into force of high-risk AI systems obligations,[41] also known as "stop-the-clock" mechanisms, reveals underlying tensions in the regulatory approach. The extension of the entry into force of these rules is primarily connected to delays in designating national competent authorities and conformity assessment bodies, as well as a lack of harmonised standards for the high-risk requirements. According to the AI Omnibus proposal, rather than requiring immediate implementation according to the timetable of the AI Act,[42] the amendments link the application of Chapter III, Sections 1 to 3, to the availability of supporting instruments such as standards, common specifications or Commission guidance. This represents a shift from purely formal regulatory readiness to operational readiness, acknowledging that providers and conformity assessment bodies require concrete interpretive and technical tools before high-risk AI obligations can be effectively implemented. Moreover, the proposal expands real-world testing to systems listed in Annex III and to systems covered by Union harmonisation legislation in Section A of Annex I, while creating a new legal basis for voluntary real-world testing agreements for certain Section B Annex I systems.

Moreover, the implementation timeline for the certain rules governing high-risk AI systems will apply from 2 December 2027, while for systems integrated into products such as lifts or toys, the rules will apply from 2 August 2028. This approach aims to ensure more legal certainty and to avoid that the lack of technical standards and other support tools delay the entry into force of the rules on high-risk AI systems. However, this extension risks extending the scope of Article 111(2) AI Act, which consider high-risk AI systems already placed in the EU market excluded from the scope of the Act unless they are subject to significant changes.

At the same time, the AI Omnibus proposal focuses on the proportionality of compliance obligations, especially for small and medium-sized enterprises and small mid-caps.[43] The proposal introduces simplified technical documentation possibilities and requires quality management systems to be implemented in a manner proportionate to the provider's size, while maintaining the required level of protection. This adjustment shows how the risk-based logic of the AI Act has been untouched, and the changes address limited proposals that do not limit administrative burdens for smaller actors. Indeed, the

[40] M Veale and F Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act: Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach" (2021) 22 Computer Law Review International 97.

[41] Ibid, Art. 1(30)(a).

[42] AI Act, Art. 113. The provisions governing high-risk AI systems included in Annex III will be applicable starting from 2 August 2026, while the ones under Annex I from 2 August 2027.

[43] Ibid, see, e.g., Art. 1(8).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

adjustments for small and medium-sized enterprises, which aim to address the regulatory burden of complying with the AI Act, operate within an already dense regulatory environment, which the Digital Omnibus contributes to expanding with further amendments.

Nonetheless, some of the simplification measures do not seem necessarily to lead to a better framework for legal certainty. According to the EDPS and the EDPB,[44] the proposed removal of registration obligations for certain AI systems in Annex III would weaken accountability mechanisms that are central to the AI Act's risk-based approach. In their view, public registration plays an important role not only in informing regulators and fundamental rights authorities, but also in enabling deployers and affected individuals to scrutinise providers' claims that a system should not be treated as high-risk. The EDPB and EDPS further question the assumption that company size is an appropriate basis for lighter compliance obligations. Given the scalability and potentially far-reaching effects of AI systems, they contend that even small providers may deploy technologies capable of causing significant harm to health, safety or fundamental rights. Consequently, they express reservations about simplifying product safety and compliance obligations primarily on the basis of staff headcount or turnover, warning that such an approach could dilute safeguards without generating meaningful administrative efficiencies.

Despite the relevance of flexibility driving the simplification efforts, the proposed rules for high-risk AI systems are likely to undermine the effectiveness of the regulatory framework, which aims to protect people from high-risk AI systems, and, from an internal market perspective, it can affect investments already made to align with the AI Act due to uncertainty about the enforcement timeline. Moreover, while some of the proposals for delaying the entry into force and simplifying obligations for high-risk AI systems they may ease certain obligations, they do not substantially simplify the broader legal framework interacting with the AI Act.

b. Bias detection between the GDPR and the AI Act

Among the proposed amendments, the Commission aims to expand the possibility of processing personal data for the purposes of bias detection and correction, which constitute a substantial public interest because they protect natural persons, particularly from discrimination.[45] According to Article 10(5) AI Act, providers of high-risk systems may exceptionally process special categories of personal data to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in accordance with the requirements of Article 10(2)(f) and (g) AI Act, including appropriate safeguards for fundamental rights and freedoms. The AI omnibus proposal would extend this rule also to deployers and to all AI systems and models. Given that discrimination might also result from those other AI systems and models, it is therefore welcome that this extension to AI systems is not limited to high-risk ones.

In this case, the EDPS and the EDPB took the position that the processing of special categories of personal data in AI systems should remain an exceptional measure under EU data protection law and must be subject to strict safeguards.[46] They warn that the proposed AI Act amendments risk broadening access to sensitive data processing for bias detection and correction in non-high-risk AI systems without sufficiently clear limits. In particular, they argue that the existing standard of strict necessity in Article 10(5) should be maintained for all providers and deployers covered by the new Article 4a, rather than

[44] 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), 20 January 2026 <https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf>

[45] Ibid, Art. 1(4).

[46] EDPB-EDPS Joint Opinion.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

weakened to a lower "necessary" or "necessary and proportionate" threshold. They also stress that any use of sensitive data should be narrowly confined to cases involving serious risks to health, safety, fundamental rights or unlawful discrimination, and criticise the proposal for failing to provide concrete guidance or examples to prevent misuse and ensure legal certainty.

At the same time, this intervention remains relatively limited in scope and is not about simplification but rather about expanding the scope of the AI Act in this case. The proposal links the AI Act objectives to Article 9(2)(g) GDPR, which permits the processing of special categories of personal data where necessary for reasons of substantial public interest and subject to appropriate safeguards. In this sense, the proposal does not displace the GDPR, but, it seeks to create a sector-specific legal basis within the AI Act that operates in compliance with, and as a complement to, the GDPR.

While addressing the interplay between the GDPR and the AI Act is a welcome step, the AI Act cannot solve the underlying problems at the intersection of data protection and AI. Moreover, while it expands the conditions under which particular categories of personal data may be processed, it does not fundamentally address other pitfalls of the GDPR in relation to the processing of particular categories of data in the age of AI, particularly purpose limitation and discrimination,[47] thus prioritising continuity over structural refinement, or even simplification.[48]

Detecting and mitigating algorithmic bias often requires the processing of sensitive attributes such as ethnic origin, health data, religion, or sexual orientation in order to assess whether an AI system produces discriminatory outcomes across different groups. Yet the GDPR is built on principles, particularly purpose limitation and data minimisation, that restrict the reuse and large-scale processing of such data beyond the specific purposes for which they were originally collected, thus leading to a structural paradox. On the one hand, AI providers and developers may need access to sensitive data to identify and prevent discriminatory effects; on the other hand, the GDPR simultaneously limits the lawful availability and reuse of precisely that data.

This fundamental conflict cannot be resolved through simplification or by merely cross-referencing the two regulations. Consequently, the AI Act fails to address the pivotal question of the extent to which a departure from data protection principles should be permissible in favour of AI training and development. As a result, unresolved conflicts and structural enforcement deficits persist in this field.

c. The enforcement centralisation

Simplification is also reflected in the centralisation of enforcement powers within the AI Office, as outlined in the AI Act. For instance, the proposed amendments in the AI Omnibus aim to streamline oversight by consolidating authority. Specifically, the proposal suggests modifying Article 75 to designate the AI Office as the sole competent authority responsible for supervising and enforcing regulations concerning AI systems that are based on general-purpose AI models. These are systems where the model and the deployed system are both developed by the same provider, excluding AI systems that fall under the scope of Annex I product legislation. This centralisation of enforcement is connected with the proposal of the Commission to adopt an implementing act to define the enforcement powers and the procedures for the exercise of those powers of the AI Office, including its ability to impose penalties, such as fines or other administrative sanctions, in accordance with the conditions and ceilings identified in Article 99.

[47] B Hohmann and K Gergő, "Reflections on the Data Protection Compliance of AI Systems under the EU AI Act" (2025) 11(1) Cogent Social Sciences.

[48] Ruschemeier, "Generative AI and Data Protection" (n 32).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

Likewise, the AI Omnibus proposal aims to align enforcement between the AI Act and the DSA.[49] The proposal aims to strengthen the authority and effectiveness of the European Commission, especially in enforcing the rules established by the DSA in relation to very large online platforms (VLOPs). This approach involves increasing the Commission's direct oversight of AI systems integrated into these VLOPs, with the goal of minimising regulatory fragmentation across jurisdictions. Additionally, this strategy reflects an understanding of the often overlapping competencies between various regulatory bodies, as in the case of platforms and AI regulation.

A further example is pre-market control. For high-risk AI systems falling within the amended Article 75 scope and requiring third-party conformity assessment, the Commission would also contribute to the organisation and performance of conformity assessments and tests before the systems are placed on the Union market or put into service. These tests and assessments shall verify that the systems comply with the relevant requirements of the AI Act and may be placed on the market or put into service in the Union. Nonetheless, this assessment can be delegated to notified bodies designated under the AI Act, thus making the system of conformity assessment more articulated.

The centralisation is not only about who supervises, but it is also about which powers the Commission can exercise when performing its functions. The proposal states that, when exercising these tasks, the AI Office would have all the powers of a market surveillance authority under the AI Act and Regulation 2019/1020, and could take appropriate measures and decisions to exercise those powers. National authorities would still cooperate, especially where enforcement action must be taken on a Member State's territory, but they would do so in support of the AI Office rather than as the primary authority for the covered systems.

However, these developments do not lead to a rethinking of enforcement structures. The framework for enforcement remains scattered, with coordination outside this particular context still resembling a patchwork of supranational and national authorities working independently or with limited collaboration. The persistent challenges posed by having multiple authorities at both the European and national levels continue to complicate enforcement efforts, especially in cross-border cases where jurisdictional overlaps and differing legal standards create additional overlaps.[50] While the approach moves in the right direction, it does not fully address the structural weaknesses in enforcement within the EU digital framework.

III. The evolving digital agenda: the case of the DSA

The proposed amendments are unlikely to promote simplification or greater effectiveness, but risk making the regulatory framework even more complicated and undermining the fundamental safeguards that the EU has long been working to establish. While "simplification" is framed as neutral, such interventions could make the system of European digital regulation even more intricate, thereby affecting fundamental rights, technological development, regulatory oversight, and enforcement.[51]

Stepping back from the specific deregulatory tendencies of the Digital Omnibus regarding the GDPR and the AI Act to view the European digital regulation agenda as a

[49] Digital Omnibus on AI, Art. 1(25)(b).

[50] P de Hert and P Hajduk, "EU Cross-Regime Enforcement, Redundancy and Interdependence. Addressing Overlap of Enforcement Structures in the Digital Sphere after Meta" (2024) 2024 Technology and Regulation 291 <https://doi.org/10.71265/fydwsg59>.

[51] "Op-Ed: 'The Digital Omnibus and the Future of EU Digital Governance: Simplification or Strategic Dilution?'" (*EU Law Live*, 16 January 2026) <https://eulawlive.com/op-ed-the-digital-omnibus-and-the-future-of-eu-digital-governance-simplification-or-strategic-dilution/> (last accessed 29 March 2026).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

whole reveals a more nuanced picture. The EU has adopted numerous other legislative acts in the field of digital regulation, and is introducing and planning further measures that remain unaffected by the Omnibus package,[52] thus expanding the scope of European digital regulation.

One of the most central and practically relevant regulations, the DSA, was, rightly so, omitted from the Omnibus package. It appears that the Commission intends to address demands for a more business-friendly environment through the Omnibus package, while simultaneously maintaining its foundational agenda of digital regulation. This dual approach is explained by the fact that compliance costs for both the GDPR and the AI Act have been the primary focus of criticism, alongside the powerful role accorded to supervisory authorities and the central importance of safeguarding fundamental rights.

At the same time, the enforcement of the DSA has taken a decisive turn through the European Commission's proceedings against X.[53] In its preliminary findings adopted in 2024, the Commission identified several areas of infringement, from misleading design practices related to the verification system (notably the "blue checkmark") to restrictions on access to publicly available data for vetted researchers, which raise systemic risk concerns. In this case, the Commission has not only articulated how platform design and governance choices may infringe on the DSA's due diligence obligations but also underlined its intent to enforce the DSA strictly. Broadly, the X case further illustrates the Union's intent not to slow down in reducing its approach to a simple narrative of simplification or deregulation. Rather than focusing on individual instances of illegal content, the Commission showed its intention to determine whether, despite parallel initiatives framed under the banner of simplification, core areas of the EU digital acquis, such as the DSA, remain actively enforced and even expanded in their practical reach.

A further, equally relevant enforcement action concerns Meta, in relation to its platforms Facebook and Instagram, on which the European Commission adopted preliminary findings in 2025 regarding compliance with obligations on advertising transparency.[54] According to the Commission, Meta may have failed to ensure that its advertising repository provides complete, accurate, and searchable information about online advertisements, thereby limiting users' and researchers' ability to scrutinise advertising practices and detect risks such as disinformation or manipulative campaigning. In particular, shortcomings were identified in the accessibility and reliability of the data made available, raising concerns about the effectiveness of the DSA's transparency framework.

A parallel and equally important enforcement action concerns TikTok, where the Commission adopted preliminary findings in 2026 regarding the platform's compliance with its risk mitigation obligations.[55] According to the Commission, TikTok may have failed to adequately assess and address systemic risks stemming from certain design features, such as infinite scrolling, autoplay, and push notifications, capable of fostering addictive behaviour, particularly among minors, thereby raising concerns under the DSA's provisions on the protection of fundamental rights and user well-being. The case highlights how the Regulation extends beyond content moderation to encompass the broader design and

[52] See, for example, the table overview of EU digital legislative acts: <https://www.bruegel.org/sites/default/files/private/2023-07/Tables_Scott_Kai.pdf>.

[53] Commission fines X €120 million under the Digital Services Act, <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934>; M Fabbri, "What the EU's X Decision Reveals About How the DSA Is Enforced" Tech policy Press 11 February 2026.

[54] Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act, <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503>.

[55] Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act, <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-tiktoks-addictive-design-breach-digital-services-act>.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

functioning of digital services. Procedurally, both cases reflect the European Commission's central role in enforcing the DSA against VLOPs, reinforcing the idea that key pillars of the EU digital *acquis* remain firmly operational despite parallel narratives of simplification. In each instance, the adoption of preliminary findings opens a structured phase of dialogue, allowing the platforms to exercise their rights of defence and potentially adjust their practices, while considering the risk of financial penalties, up to 6 per cent of global annual turnover.

Furthermore, the Commission announced that it had preliminarily found Meta in breach of the DSA due to alleged weaknesses in how Facebook and Instagram prevent children under 13 from accessing the platforms.[56] The Commission's concern is that Meta's age-verification and age-assurance measures may not be effective enough, allowing underage users to create or keep accounts despite the platform's minimum-age rules. The Commission's preliminary view is therefore not simply about individual underage accounts, but about whether Meta has put in place sufficiently robust systems to manage child-protection risks at scale. Although the finding is still provisional, this case provides another example of the European approach to digital regulation.

These enforcement actions are only some examples reflecting the more complex trajectory of the Union's digital regulatory agenda. If the omnibus-style reforms may bundle different policy objectives and raise concerns about potential trade-offs between efficiency and fundamental rights, these cases demonstrate that the EU is not retreating from regulation. Instead, it continues to expand its digital regulatory agenda through enforcement.

IV. Rethinking European digital regulation: from rulemaking to enforcement

The Digital Omnibus proposal represents a missed opportunity to advance structured system of digital regulation. Instead of clarifying the law, the proposed amendments exacerbate legal uncertainty by leaving the precise relationship among the various legal acts unaddressed. This failure to harmonise the regulatory framework fosters ambiguous conditions, particularly regarding the interplay between the AI Act and the GDPR, while expanding the enforcement of the European digital agenda. If enforcement is a critical part of the European digital agenda, the digital omnibus could be an opportunity to improve the enforcement process rather than focusing solely on simplification.

The challenges of digital regulation in Europe do not stem solely from the proliferation of rules or regulatory overlaps that call for simplification, but also from structural uncertainty in enforcement.[57] The European Union has, over the past decade, developed an extensive and sophisticated digital regulatory framework. However, the effectiveness of this framework is primarily linked to the enforcement structure spanning EU institutions, notably the Commission, and multiple authorities across Member States, each with distinct expertise, resources and political constraints. This multi-layered architecture, while reflecting a degree of power distribution, risks leading to divergent enforcement practices across Member States and policy areas, and is amplified by simplification efforts.

A significant unresolved challenge remains the enforcement of the GDPR.[58] Rather than pursuing a deregulatory agenda, the focus should shift toward strategically strengthening the existing enforcement architecture. Under the current "one-stop-shop" mechanism,

[56] Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook, 29 April 2026 <https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920>.

[57] S Demkova and G De Gregorio, "The Looming Enforcement Crisis in European Digital Policy." A rule-of-law centered path forward Verfassungsblog 2025.

[58] FB Bastos and P Pałka, "Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?" (2023) 19 European Constitutional Law Review 487.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

the Irish Data Protection Commission (DPC) has emerged as a structural bottleneck due to the concentration of Big Tech headquarters in its jurisdiction. The structural bottleneck observed in the Irish Data Protection Commission and its enforcement of the GDPR is not an isolated flaw but rather a symptom of a broader systemic failure. As has been argued elsewhere, the EU's expanding digital rulebook has resulted in a fragmented ecosystem in which national enforcement disparities undermine the uniform application of the law. Imposing rigid, prolonged timelines rather than addressing this institutional inertia risks entrenching a looming enforcement crisis.[59]

While the recent provisional agreement among EU institutions aims to harmonise cooperation between national authorities, its efficacy is questionable. The introduction of standardised timelines, extending up to 27 months for complex cases, and the 'early solution mechanism' have been criticised as overly protracted. Far from streamlining the process, these rigid procedural requirements risk exacerbating the administrative burden and further marginalising the interests of the data subjects they are intended to protect.[60]

Against this background, the emergence of omnibus strategies to simplify the EU digital rulebook risks making the entire framework of digital regulation even more articulated and intricate. While such initiatives have been presented as a necessary response to regulatory complexity, they address specific areas, raising even more questions for competent authorities. The Union has conflated simplification with questions of efficiency and effectiveness. However, defining these concepts solely in terms of competitiveness overlooks the intricate interplay between regulation, legal certainty, fundamental rights and, broadly, the economic development which the Digital Omnibus aims to target.

The introduction of these omnibus measures is also likely to generate new interpretative uncertainties, particularly where they interact with different regulatory instruments. In other words, the Union risks exacerbating, rather than resolving, enforcement challenges. Simplification of substance does not necessarily translate into simplification in practice, especially considering the challenges in the European enforcement architecture.[61] As long as the EU relies on a decentralised network of national authorities with overlapping mandates, such as data protection boards clashing with AI market surveillance bodies, any attempts at mere simplification are likely to fail. Without structural harmonisation of the European enforcement landscape, new layers of legislation will only create further overlaps and procedural bottlenecks.

Different issues affect the enforcement of European digital regulation. One of the central limitations of current reform efforts is their insufficient attention to enforcement structures. The EU digital regulatory framework continues to rely heavily on national authorities, whose capacities and priorities vary significantly.[62] Despite the Commission's expansion in European digital regulation, differences in capacity across Member States can significantly affect enforcement outcomes. The Digital Omnibus could be an opportunity for the Union to consider mechanisms to support capacity-building for enforcement at the national level. In the absence of these steps, supposed simplification may merely shift complexity from the legislative to the enforcement stage.

Moreover, the continuous introduction of new instruments requires enforcement authorities to adapt to evolving legal frameworks, often at the expense of consolidating interpretation. This dynamic can contribute to a gap between regulatory ambition and

[59] S Demková and G De Gregorio, "The Looming Enforcement Crisis in European Digital Policy" [2025] Verfassungsblog <https://doi.org/10.59704/c4fc2ec9cb2b9ba5> (last accessed 29 March 2026).

[60] H Ruschemeier, "Reforming the GDPR" [2025] Verfassungsblog <https://doi.org/10.59704/fb55ac14da765078> (last accessed 12 January 2026).

[61] G De Gregorio and A Vicinaza, The Enforcement of European Digital Regulation: Conflicts and Patways, SSRN 2026.

[62] European Union Agency for Fundamental Rights, "GDPR in Practice – Experiences of Data Protection Authorities." <https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities>.

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

practical implementation on the enforcement level. In this context, the EU's focus should shift away from continuous legislative recalibration and towards a more systematic rethinking of enforcement. Rules that face enforcement challenges do not provide greater protection for European constitutional values, including the protection of fundamental rights and the functioning of the internal market.

Among potential steps, the Commission could support the coordination mechanism among existing authorities, such as structured dialogue, joint guidelines and informal consultations.[63] Although non-binding, these tools can foster convergence and reduce interpretative conflicts, especially when supported by institutional forums like digital clearinghouses. At the same time, more formalised coordination could also be considered as an additional step. A meta-regulatory framework could clarify competences and ensure more predictable enforcement by establishing rules on jurisdiction and mandatory consultations. Even looking further, limited centralisation may be appropriate in cross-border cases. Building on the DSA, assigning certain cases to an EU level body could mitigate disparities in national capacity, as with the one-stop-shop mechanism, and prevent forum shopping. At the same time, close attention should be paid to the concentration of power within the Commission, which functions simultaneously as an enforcement body and a political actor.

These challenges have been neglected by the Digital Omnibus agenda, underscoring that the EU's approach to simplification is unlikely to achieve the purpose of fostering freedoms in the internal market and enhancing innovation. It could be an opportunity for opening a regulatory conversation on enforcement, which, considering the expansion of technology in society, is likely to increasingly become a pressing point.

V. Conclusions

The evolution of the European digital regulatory framework would not deserve a dilution towards a simple narrative of deregulation or retreat. The rise of Omnibus instruments reflects a more complex and ambivalent trajectory, in which efforts toward simplification coexist with the continued expansion and recalibration of the Union's digital *acquis*. Certain amendments, particularly to the AI Act and the GDPR, signal responsiveness to political pressures around competitiveness and innovation, but they also risk undermining legal certainty and fundamental rights, while the Union is still expanding European digital regulation. Rather than genuinely simplifying the framework, these interventions often introduce new layers of interpretative ambiguity, thereby complicating both compliance and enforcement.

These proposed changes are unlikely to substantially alter the EU constitutional orientation. Core principles, such as the risk-based approach and the emphasis on fundamental rights, remain untouched. While this continuity may be welcomed, the focus on highly specific aspects of the framework risks making the GDPR and the AI Act even more intricate, while indicating how the Union has not focused on the structure. This focus on detailed adjustments, rather than on more structural questions, suggests that the Union has not fundamentally changed but has reshaped its approach to the European digital agenda. In this sense, despite some exceptions as in the case of the GDPR definition of personal data, the proposed amendments remain largely of detail, leaving the core structure unchanged.

Changing these regulations appears more as a reaction to the current political discussion on over-regulation and competitiveness. Particularly, the proposal to delaying the AI Act before it comes into force risks weakening the credibility of EU law making. To now delay these determinations through an omnibus legislative package fails to respect the significance

[63] De Gregorio and Vicinanza (n 64).

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press

of the underlying substantive debates and regulatory steps achieved by the Union. By echoing the deregulatory rhetoric prevalent across the Atlantic, the Commission risks abandoning the path towards European digital constitutionalism. Despite legitimate concerns regarding bureaucratic efficiency and its impact on SME competitiveness, the solution is not an abdication of oversight and constitutional safeguards. Rather, the democratic articulation of legal norms is one of the most relevant safeguard to protect fundamental rights and limit powers in the algorithmic society.

However, the European Commission does not seem to slow down on the European digital agenda. The growing emphasis on enforcement under the DSA underlines a trajectory that runs counter to a purely simplification-driven strategy. Rather than reducing regulatory intensity, the EU is deepening its intervention through active supervision and the scrutiny of systemic risks. This approach demonstrates that simplification at the legislative level does not equate to a retreat from regulation. On the contrary, it is accompanied by a more operational form of governance. The DSA thus exemplifies how the Union is not scaling back its digital ambitions, but reconfiguring them, shifting from expanding rules on paper to enforcing them more rigorously in practice.

The solution to the current enforcement crisis is not a retreat from regulation, but a commitment to making it work. Instead of diluting substantive protections to ease the burden on authorities like the Irish DPC, the EU must invest in the structural harmonisation of its oversight bodies. The true strength of the European model lies in recognising its primary competitive advantage: the protection of fundamental rights and the principled enforcement of the rule of law. Competitiveness cannot be measured solely by scale, but rather by the normative capacity to articulate a positive vision for a sustainable digital society.

Despite the focus on enforcement, the central challenge facing EU digital regulation is no longer legislative proliferation, but institutional effectiveness. The persistence of fragmented enforcement structures and divergent national capacities undermines the practical impact of even the most sophisticated regulatory instruments. In this context, the focus on legislative recalibration, exemplified by the omnibus approach, appears increasingly misplaced. Without addressing structural enforcement deficiencies, attempts at simplification risk displacing complexity rather than resolving it. The EU's ability to uphold constitutional principles will hinge less on the number of its rules than on its capacity to ensure they are applied meaningfully.

Cite this article: G De Gregorio and H Ruschemeier, "From a Right-Based Approach to Competitiveness? The EU Digital Omnibus Reform". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10121

https://doi.org/10.1017/err.2026.10121 Published online by Cambridge University Press