

A Comment on the EU Digital Fitness Check

Coherent and Time-Consistent Rules for a Competitive Digital Single Market

Anselm Küsters, Philipp Eckhardt and Henning Vöpel



© shutterstock/illus_man

- ▶ The EU Digital Fitness Check comes at the right time: After years of ambitious digital legislation, Europe must evaluate the effectiveness of its digital acquis. Since 2020, there has been an abundance of new digital legislation – ranging from the DMA and DSA to the AI Act, Cyber Resilience Act, Data Act and the revised PLD – that has led to a fragmented regulatory environment characterised by competing definitions and diverging enforcement logics of EU and national authorities.
- ▶ In particular, the Digital Markets Act’s interoperability obligations conflict on a technical level with the EU’s own commitments in the areas of data protection and cybersecurity. The underlying conflicts cannot be resolved solely through enforcement.
- ▶ Research conducted at the Centre for European Policy in recent years has clearly shown that legal certainty and cross-border coherence are structural prerequisites required for a functioning digital single market and a competitive European economy. Accordingly, politicians must prioritise these issues in the coming months, rather than simply dismissing current calls for simplification and deregulation as self-interested demands of the industry that must be resisted.

Content

1	Background.....	3
2	A Regulatory inventory with uncomfortable results	3
3	Where the DMA meets its limits	5
4	Cybersecurity: the blind spot the Fitness Check cannot afford	5
5	cep agenda for the Digital Fitness Check	6

Note: This publication was originally conceived as a news item and subsequently expanded into an Adhoc comment format. As a result, it contains direct quotations intended for use by media outlets.

1 Background

When the European Commission launched its consultation on the Digital Fitness Check, as part of a broader Digital Simplification Package, at the end of 2025,¹ the political mood in Brussels had visibly shifted – from *what* should be regulated to *whether* the existing rulebook, after years of rapid legislative output, could function coherently as a whole. Will this shift in tone and ambition lead to substantive reform? This will be the decisive question in the months to come. Henning Vöpel, Director of the Centre for European Policy, comments: “A market economy needs rules that are intelligible and enforceable. The EU’s digital framework has expanded more quickly than its coherence and time-consistency has been able to keep up with. This is the main problem the Digital Fitness Check must solve, and it is a more fundamental challenge than any single piece of legislation it touches”. Below, we highlight a number of points we consider particularly worth addressing in the design and execution of the Digital Fitness Check, without aiming for a comprehensive treatment.

2 A Regulatory inventory with uncomfortable results

Since 2020, the EU has adopted more than a dozen major legislative instruments targeting the digital sector. Each was designed to address a genuine problem. But together, they now constitute a complicated regulatory map including numerous EU and national bodies that carry some form of responsibility for digital oversight. For companies operating across the single market, this means overlapping compliance obligations, definitions and regulatory concepts sometimes borrowed from adjacent legal domains, and enforcement decisions that produce unintended consequences. The resulting trade-offs – in competitiveness, compliance costs, geo-political alignment, and legal predictability – are systematic, yet they rarely feature in legislative texts or impact assessments.²

So far, one main response to this complexity has been quantitative, such as counting obligations or applying “one in, one out” principles.³ This logic sounds intuitive but is, in the long run, inadequate. Regulatory burden does not always correlate with legislative volume; it correlates with definitional ambiguity, norm conflicts that generate litigation rather than compliance, and concepts transplanted from one legal domain into another.⁴ To capture these problems, EU lawmaking needs better diagnostic tools to assess legislative quality across the *acquis* as a whole. Anselm Küsters, Head of Digitalisation at the Centre for European Policy, notes: “For the first time, generative AI gives regulators a scalable instrument for reading their own rulebook the way practitioners do: across instruments, across languages, across legal domains simultaneously. The question is whether the Commission will build that capability into the legislative process”. The research frontier is already moving in this direction: Researchers have shown that genAI models can be systematically benchmarked for their ability to read

¹ For more information on the Digital Fitness Check consultation, see [here](#).

² Anselm Küsters und Cecilia Emma Sottilotto, „Coping With the Digital Trilemma? Trade-Offs and Risks in EU Digital Policy“, *European Policy Analysis*, Oktober 2025, epa2.70023, <https://doi.org/10.1002/epa2.70023>.

³ On counting obligations as a regulatory burden measure: Jean-Edouard Colliard und Co-Pierre Georg, „Measuring Regulatory Complexity“, *Journal of Financial Economics* 174 (Dezember 2025): 104186, <https://doi.org/10.1016/j.jfineco.2025.104186>.

⁴ Some have argued that OIOO is “a tool for less, not better, regulation” and unsuitable for genuine better law-making. See: Xanthaki, H. (2023). [The “One In, One Out” Principle](#), European Parliament, JURI Committee.

and apply complex regulatory standards across domains;⁵ whereas others have documented the utility of LLMs in compliance monitoring and cross-instrument legal text analysis,⁶ i.e. precisely the diagnostic function that EU regulatory oversight currently lacks.

Another existing response to the fragmented regulatory framework in the digital field is to simply fine-tune and streamline existing regulatory provisions. In doing so, however, the Commission is often trapped by path dependencies and lacks the courage to make a fresh start. In order to fundamentally review the concepts underlying individual regulations, such a fresh start would be necessary more often. One example is the EU Data Act, which introduced uniform, horizontal rules on data usage, and comprehensive obligations to share data across connected products and user groups, despite there being no evidence of widespread market failure (see [cepPolicyBrief](#)). Furthermore, such fine-tuning and streamlining was and is often not based on comprehensive impact assessments, due to political pressure to deliver quick wins in connection with the EU's competitiveness agenda. Thus, it often misses important aspects, as can be seen with the proposed introduction of a Single-Entry Point (SEP) mechanism under the Digital Omnibus legal act designed to make it easier to fulfil mandatory incident reporting obligations across various EU legal acts, where reporting is only centralised but the obligations as such are not altered.⁷ Another example in this regard is the recent EU Inc. proposal, published on 18 March 2026⁸: While the introduction of an optional 28th-regime corporate legal framework pursues an important objective for increasing European competitiveness, the proposal rests on a legally precarious foundation. The Commission bases its proposal on Article 114 TFEU, i.e. the internal market competence, primarily to avoid the unanimity requirement in the Council. Yet as our cep colleague Anja Hoffmann has pointed out,⁹ the Commission's repeated invocation of "harmonisation" serves above all to justify that choice of legal basis: EU Inc. does not align existing national company law frameworks, it establishes an optional parallel regime alongside them. This, in turn, will create further legal uncertainty.

Furthermore, we critically observe a tendency to bundle numerous legal acts into one, with the aim of eliminating the current patchwork of legal acts, simplifying regulatory compliance, and ensuring coherence. While this effort is welcome in general, it comes at a cost that should not be underestimated. Firstly, such bundling creates an opportunity for counterproductive package deals, as different issues are now dealt with under one legislative process. A prominent example is the Digital Networks Act (DNA) released earlier this year, which now unites even more different topics like spectrum policy, network access regulation, net neutrality or supervision topics in one "Act".¹⁰ Horse-trading may be the result, potentially leading not to the most suitable and effective result. Second, bundling as such does not make the digital acquis any simpler or better. And third, the strategy may inhibit future fine-tuning of very specific legal provisions as opening a legal act that combines many different aspects in the digital field, would almost always open the door to change other provisions as well. Clearly, regulatory stability is a major prerequisite for investment and innovation activities. Yet, bundling several

⁵ Joseph Marvin Imperial u. a., „Standardizing Intelligence: Aligning Generative AI for Regulatory and Operational Compliance“, Version 1, preprint, arXiv, 2025, <https://doi.org/10.48550/ARXIV.2503.04736>.

⁶ See the survey in: Fatemeh Dehghani u. a., „Large Language Models in Legal Systems: A Survey“, *Humanities and Social Sciences Communications* 12, Nr. 1 (2025): 1977, <https://doi.org/10.1057/s41599-025-05924-3>.

⁷ COM(2025) 837, Proposal for a Regulation on a Digital Omnibus, 19.11.2025, see [here](#).

⁸ COM(2026) 321, Proposal for a Regulation on the 28th Regime Corporate Legal Framework - 'EU INC.', 18.3.2026, see [here](#).

⁹ Europe.Table, 23.03.2026, see [here](#).

¹⁰ COM(2026) 16, Proposal for a Regulation on a Digital Networks Act (DNA), 21.1.2026, see [here](#).

legal acts may inhibit necessary adaptations in the digital acquis, although it's a field with a very high degree of dynamism.

3 Where the DMA meets its limits

The Digital Markets Act (DMA) was conceived as a necessary structural intervention. Ex-post competition enforcement alone proved unequal to the dynamics of entrenched digital platform markets.¹¹ This underlying rationale was initially welcomed, including in our own assessments,¹² and is still sound. However, three years of implementation have surfaced some tensions that the DMA's architects left unresolved. It is crucial that the Digital Fitness Check does not sidestep these tensions in the name of political convenience.

For instance, the DMA's interoperability obligations require designated gatekeepers to open technical interfaces to third parties. The stated goal, namely reducing lock-in and lowering barriers to market entry, is to be welcomed from the perspective of the European market and its principle of undistorted competition. But the same technical openness that serves those objectives can simultaneously undermine data protection guarantees the GDPR was designed to provide and erode intellectual property protections that sustain innovation incentives. These are not hypothetical tensions: they have materialised in specific enforcement proceedings and produced trade-offs that neither the DMA's text nor its governance structures are equipped to resolve. The appropriate response is not to abandon the DMA's objectives. Rather, the Commission must establish cross-regulatory mechanisms that allow these trade-offs to be identified and managed, before enforcement decisions force improvised outcomes.

4 Cybersecurity: the blind spot the Fitness Check cannot afford

One dimension of the debate has received insufficient attention: the cybersecurity consequences of mandated platform openness. The Cyber Resilience Act, which entered into force in 2024, established highly welcome binding security-by-design obligations for products with digital elements (see [cepPolicyBrief](#)). Simultaneously, DMA interoperability specifications have required platform operators to expose system-level interfaces to third-party access. This implies that regulatory decisions taken in one policy domain might effectively be overriding engineering decisions mandated by another. According to Philipp Eckhardt from the Centre for European Policy: "Interoperability mandates that extend into a platform's core security architecture require regulators to make explicit trade-off judgements between competition and security objectives. Leaving those judgements to be settled after the fact, or not settled at all, is a structural risk. Such issues should be addressed more thoroughly in advance rather than afterwards."

The broader democratic implication of this problem should not be underestimated. Unresolved regulatory conflicts do not simply disappear; they typically migrate into the discretionary decisions of platforms or enforcement bodies, far from public scrutiny.¹³ We emphasise that this is one of several conditions that might feed criticism of EU digital governance as technocratic. Therefore, ensuring that

¹¹ See: Anselm Küsters und Isabel Oakes, „Taming Giants: How Ordoliberal Competition Theory Can Address Power in the Digital Age“, *Schmollers Jahrbuch – Journal of Contextual Economics* 141, Nr. 3 (2021): 149–88.

¹² See our initial assessment from 2020: Andrea De Petris, Alessandro Gasparotti, Lukas Harta, Matthias Kullas, Victor Warhem, *The Digital Markets Act*, cepInput, (11.24.2020); and, more recently: Anselm Küsters, *Small is beautiful 2.0: Mit digitaler Dezentralisierung zu einer menschlicheren Wirtschaft*, 1. Auflage (Verlag Herder, 2026).

¹³ For platforms, see: Vili Lehdonvirta, *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control* (The MIT Press, 2022).

trade-offs between competition and security are resolved transparently, with explicit political guidance and accountability, is not only a matter of good regulatory design, as set out in the EU's Better Regulation principles, but ultimately also a prerequisite for democratic legitimacy in an area where public trust is already fragile.

5 cep agenda for the Digital Fitness Check

From a perspective of “thinking in orders” (*Ordnungspolitik*), the main value of the Digital Fitness Check lies in restoring the proper framework for the digital and emerging AI-based economy. In short, the idea is to focus political efforts on creating a coherent and time-consistent (anticipatory) legal framework within which new digital markets and innovation can actually take shape and operate. From our perspective, four priorities stand out.

First, the liability framework for software distribution and AI-based products requires clarification.

Product safety rules conceived for physical goods are being applied to digital platforms in ways that misallocate responsibility and impose disproportionate burdens without demonstrably improving safety outcomes. Similarly, the question who bears responsibility when an AI system causes harm across a chain of commercial relationships has not been fully resolved by the AI Act. This gap is sharpest for agentic AI systems operating autonomously and without continuous user interaction, which the AI Act was simply not designed to govern, leaving their regulatory status formally unresolved despite growing Commission acknowledgement that dedicated rules may be necessary.¹⁴ A legally precise liability framework is a precondition for both market confidence and legitimate consumer protection. Walter Eucken's liability principle remains as instructive here as anywhere in economic law: those who take decisions and capture the resulting benefits must bear the corresponding risks. This principle must be also applied to the digital economy.

Second, the EU should consider whether incremental reform is sufficient or whether the underlying institutional architecture requires more fundamental change.

The current enforcement model – distributed across national competent authorities and Commission DGs, each with their own political principals and enforcement cultures – generates arbitrage and inconsistency. An independent European Digital Enforcement Authority, operationally insulated from the Commission's trade and industrial policy functions, would produce consistent legal interpretation¹⁵ and, critically, project a form of institutional neutrality that the current model cannot. Its mandate should cover, at minimum, the two instruments where cross-institutional coherence is most consequential: the DMA, where the Commission currently acts simultaneously as the sole enforcer while also being an active trade and industrial policy actor – a structural conflict of interest that no procedural safeguard within the same institution can fully resolve – and the DSA, where the split between Commission-level VLOP supervision and nationally fragmented oversight of mid-tier platforms creates coordination gaps and uneven enforcement intensity across the single market that the European Board for Digital Services has so far been unable to close. The AI Act's enforcement architecture compounds this problem further: built on a hybrid model that splits GPAI supervision exclusively to the Commission while delegating risk-based AI oversight to Member States (many of which had still not designated their national authorities by the August 2025 deadline),¹⁶ it reproduces, by design, precisely the decentralised inconsistency that an

¹⁴ See: Claudie Moreau and Maximilian Henning, “Could agents be the next stumbling block for Europe's AI rules?”, <https://www.euractiv.com/news/could-agents-be-the-next-stumbling-block-for-europes-ai-rules>.

¹⁵ For this proposal, see also: Ben Brake, “Europe's real debate on competition”, in: Europe.Table, 19.03.2026, see [here](#).

¹⁶ For this analysis, see: Tristan Marcelin, [Enforcement of the AI Act](#), Members' Research Service (March 2026).

independent enforcement body would be needed to correct. Over time, and with appropriate institutional safeguards, coordination with AI Act market surveillance or data protection authorities could thus be brought within its remit. In the context of escalating transatlantic friction, the distinction between legal regulation and political leverage is more important than ever. The ECB demonstrates that insulated technical authority at European level can be both politically achievable and institutionally durable.

Third, the Fitness Check should mandate a shift in how legislative quality is assessed, namely from quantitative audits to semantic analysis of the acquis itself. Generative AI models capable of contextual legal reasoning across large multilingual document sets now make it possible, for the first time at scale, to identify definitional drift between instruments and flag provisions that establish conflicting obligations. This should be adopted both retrospectively, i.e. to map existing incoherence, and prospectively, as a structured requirement within legislative impact assessments for new proposals. In a regulatory environment as complex and consequential as the EU's digital framework, that capability will soon become a governance necessity.

Fourth, the Fitness Check should allow for more fundamental discussions. Discussions should not just focus on amending existing digital legislation here and there. There should also be discussions on the regulatory concepts themselves and whether they are fit for purpose. In this respect, the main parts of the Data Act (see [cepPolicyBrief](#)) and the Proposal for a Financial Data Access Regulation (FIDA, see [cepPolicyBrief](#)) should be reconsidered, for instance. In both areas, voluntary frameworks may be more valuable than the binding obligations the two Regulations set out. These mandatory obligations may not be the best solution in every case.

Overall, the coming Digital Fitness Check will be judged by whether European businesses and consumers end up operating in a more coherent and competitive regulatory environment.

**Authors:**

Dr. Anselm Küsters, LL.M.
Head of Department Digitalisation and New Technologies
kuesters@cep.eu

Philipp Eckhardt
Head of Department Financial Markets and Information Technology
eckhardt@cep.eu

Prof. Dr. Henning Vöpel
CEO and Board
voepel@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4205 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Free of vested interests and party-politically neutral, the Centres for European Policy Network provides analysis and evaluation of European Union policy, aimed at supporting European integration and upholding the principles of a free-market economic system.