



PRIORITIES FOR THE

European Commission's Digital Fitness Check

UPDATED OCTOBER 2026

Contents

Introduction and executive summary.....	3
Twelve recommendations for the Digital Fitness Check.....	6
Overlapping and incoherent obligations.....	8
Persistent regulatory fragmentation.....	10
Lack of proportionality and risk-based approaches.....	11
Unrealistic timelines and administrative burdens.....	14
Failure to align with international standards.....	18
How should these problems be addressed?.....	19
Is a rule still necessary?.....	19
If a rule is necessary, can it be modernised?.....	20
How can new policy tensions be avoided?.....	21
Make the DFC-scope sufficiently broad.....	23

Contact information:

Carola Ekblad carola.ekblad@svensktnaringsliv.se

Carolina Brånby carolina.branby@svensktnaringsliv.se

A series of thin, orange, curved lines that sweep across the bottom right corner of the page, creating a dynamic, abstract graphic element.

Introduction and executive summary

Europe has faced a prolonged period of weak economic growth, which has opened up an increasing gap between US and European GDP. This creates a set of existential challenges for the EU: not only to its economy, but also to its security and its ability to deliver the social contract.

Europe's problem is its lack of productivity growth. Mario Draghi is clear that digital technology plays a fundamental role in delivering this productivity. Europe must, of course, catch up and become a leader in the frontier technologies that will drive future economic growth, despite its poor position in most strategic technologies like AI. But – just as importantly – Europe must ensure the take-up of new technologies by European businesses across all sectors of the economy to improve their productivity. This is especially true for innovations like AI, which is a valuable tool to help speed up the process of innovation itself.

There are many factors holding back the innovation and take-up of technologies in Europe. But there is widespread acceptance that the volume, quality, consistency and cumulative burden of regulation is one of the most important barriers.

In this context, the European Commission is pursuing two parallel processes to simplify the digital rulebook. The first comprises the Digital Omnibus and AI Omnibus initiatives, which address a subsection of the most urgent problems with the digital rulebook in a highly targeted fashion.¹ The second is the Digital Fitness Check (DFC), which aims to provide a more comprehensive assessment of the coherence of EU digital laws – including both its substantive and institutional aspects.

This dual-track process was recommended by Enrico Letta in his recent report on the single market. Letta's recommendation was to tackle in Omnibus packages only the most pressing and widely-accepted examples of “redundant, obsolete, and inconsistent” regulation – while acknowledging that achieving competitiveness requires a more fundamental reassessment of EU tech laws.² The DFC provides the opportunity for this fundamental reassessment – and an opportunity to re-examine whether the Commission's new legislative proposals, like the Digital Networks Act (DNA), the revised Cyber-security Act (CSA2), the Cloud and AI Development Act (CADA), and Chips Act 2.0, will contribute to the need for a simpler and more innovation-friendly rulebook.

1 At the time of writing the AI Omnibus, which amends the AI Act to simplify compliance for some firms and to delay implementation timeframes for deployers of high-risk AI systems, had been passed by the co-legislators. The Digital Omnibus seems likely to continue to be debated for the rest of 2026.

2 Enrico Letta, 'Much More Than a Market', April 2024, p 130.

The Omnibus initiatives include some important improvements – but they do not examine the cumulative impact of regulation, tackle concerns with the institutional arrangements underpinning Europe's digital rules, or grapple with overarching questions about how to better align EU digital laws with the principles of better regulation. These are all structural issues which stifle Europe's ability to compete globally.

The Omnibus proposals are therefore only a tentative first step at modernising regulation. The DFC remains essential and is more important: while the Omnibus packages tackle individual isolated examples of poor regulatory practice, the DFC is a once-in-a-generation opportunity to address these problems in a more systematic way, and in doing so to restore the EU's competitiveness. This does not require the EU to lower its regulatory standards. Instead, the DFC is an opportunity to modernise regulation: making it simpler, more agile, proportionate, and innovation-friendly. To deliver this vision, the Commission needs ambition. Europe cannot afford the competitiveness agenda to stop with the "quick fixes" in the Omnibus proposals. The existing rules, and initiatives which are currently making their way through the legislative process like the DNA, CSA2 and CADA, should all be reviewed as part of the DFC, especially since many of these initiatives add new complexity and burdens for innovative firms.

Swedish Enterprise has already contributed to the discussion of how to improve regulation in its position papers on the [GDPR](#)³, [ePrivacy Directive](#)⁴, [Digital Omnibus](#)⁵, and [AI Omnibus proposals](#).⁶ We have also participated in a [BusinessEurope position paper](#) on simplifying the digital rulebook,⁷ another on making the GDPR more effective,⁸ and we are signatories to a [joint business statement](#) on the proposed Council compromise position for the Digital Omnibus.⁹ This paper complements those documents by identifying the most pressing issues and proposing improvements to the whole digital rulebook, in line with the DFC's broad scope.

We urge the Commission to be ambitious in the DFC. That does not mean lowering Europe's regulatory standards. It means returning to the basics of ensuring that tech laws:

- » contribute to the single market;
- » are coherent and provide legal certainty; and
- » are as simple, proportionate, flexible and technology-neutral as possible.

3 'GDPR simplification – Nordic position paper', October 2025.

4 Swedish Enterprise, 'Digital Omnibus relating to the ePrivacy Directive', March 2026.

5 Swedish Enterprise, 'Digital Omnibus on the EU Data Act', 3 February 2026.

6 Swedish Enterprise, 'Digital Omnibus on AI', 3 January 2026.

7 Business Europe, 'Simplifying the EU Digital Rulebook', July 2025.

8 Business Europe, 'Making the General Data Protection Regulation More Effective', February 2026.

9 'Joint Business Statement: Stop the Council Compromise on Digital Omnibus!', 24 June 2026.

The most serious overarching cross-cutting problems which the DFC must tackle – and which the Omnibus proposals will not properly address – are the following:

1. Overlapping and incoherent obligations

Today, the relationship between different policy objectives and different laws is unclear. This creates an unpredictable regulatory environment. Investors and firms cannot easily understand how laws will be implemented and how they will apply to innovative new business models and technologies.

[Read more on page 8](#)

2. Persistent regulatory fragmentation

The economic value of a genuine digital single market would be immense.¹⁰ But EU rules often fail to deliver – either by allowing inconsistent interpretation, or because member-states gold-plate or do not properly adopt EU law.

[Read more on page 11](#)

3. Lack of proportionality and risk based approaches

The design of the EU rulebook needs to reflect well-understood principles of better regulation. Regulation needs to be compatible with innovation and experimentation – giving firms the freedom to identify how to most efficiently reach the desired regulatory outcomes, and ensuring law does not lock in particular technologies or business models.

[Read more on page 11](#)

4. Unrealistic timelines and administrative burdens

Rules today do not always impose commercially and technologically reasonable requirements. They also impose complexity, administrative and cost burdens which are unnecessary to protect consumers and society.

[Read more on page 15](#)

5. Failure to align with international standards

If the EU's rules are idiosyncratic globally and developed with scant regard to international standards, then European tech firms will be less likely to use the continent as the launching pad for global success.

[Read more on page 18](#)

¹⁰ Studies illustrate that the benefits of the single market could reach €2.8 trillion per year: European Parliamentary Research Service, 'Increasing European added value in an age of global challenges', February 2023. The International Monetary Fund estimates that if internal barriers to trade in the EU were at the same level of those in the US, then labour productivity could increase by 7% over seven years. International Monetary Fund, 'Europe's Declining Productivity Growth: Diagnoses and Remedies', 2024.

Twelve recommendations for the Digital Fitness Check

It is widely recognised that the EU's GDP is falling further behind that of the US – even if the precise degree of the gap and the right way to measure it remains disputed. This amounts not only to a problem of digital policy but creates a broader set of existential challenges for the EU.

Our current rate of productivity growth can only barely compensate for our aging workforce – meaning GDP is on track to stagnate until 2050. In turn, this impacts our democracies and social stability – as lack of growth means public budgets will be increasingly unable to support the European social contract. In the meantime, our inability to produce innovations on which the rest of the world depends means that the EU's international leverage and economic security is in decline.

Regulation is not the only reason for this problem – factors like strong capital markets play an important role – but there is widespread acceptance that the volume, quality, consistency and cumulative burden of regulation is one of the most important barriers.

Approximately 69% of businesses across Europe cite regulation as a barrier to investment and growth:¹¹ a figure which has grown significantly in recent years.¹² Regulation is often cited as among the most important of all the obstacles to growth.¹³ For example, 40% of Swedish companies state that regulatory burden and bureaucracy are among the top two significant obstacles to growth.¹⁴ And European businesses are more likely than US firms to cite regulation as a major obstacle to doing business.¹⁵

Mario Draghi is clear that digital technology will have to play a fundamental role in delivering growth, through increasing productivity. A large part of Europe's 'growth gap' with the US is down to Europe's weakness in both innovating and incorporating digital technologies into firms' working practices to boost efficiency.¹⁶ Europe must, of course, catch up and become a leader in frontier technologies that will drive future economic growth. But – just as importantly – Europe must ensure the take-up of new technologies by European businesses across all sectors of the economy to improve their productivity. This is especially true for innovations like AI, which is a valuable tool to help speed up the process of innovation itself. Yet while Europe needs to rely on cutting-edge technology to grow, its share of the global ICT market nearly halved over

11 EIB, 'EIB Investment Survey 2025 – EU Overview', p 29. For example, almost 40% of Swedish companies consider regulatory burdens a barrier to growth: Swedish Enterprise, 'Företagens Regionala Utveckling', 2025.

12 For example, the figure from the 2023/24 EIB report was 60%: see European Investment Bank, 'Transforming for Competitiveness', Investment Report 2023/24.

13 Regulatory burdens and bureaucracy are perceived as the second biggest obstacle to growth in Sweden, after difficulties in finding staff with relevant skills: Swedish Enterprise, 'Företagens regionala utveckling', 2026.

14 Swedish Enterprise, 'Företagens regionala utveckling', 2026, p 17.

15 EIB, 'EIB Investment Survey 2025 – EU Overview', p 29.

16 B Van Ark, M O'Mahoney, and M Timmer, 'The Productivity Gap between Europe and the United States: Trends and Causes' (2008) 22(1) Journal of Economic Perspectives 25.

the period 2013-22.¹⁷ It is lagging the US and China in seven of the eight most strategic technologies, which are likely to be essential to future growth.¹⁸

This is why the quality and volume of Europe's tech regulation – which can unnecessarily hold back technological innovation and adoption – poses a fundamental constraint on Europe's ability to thrive.

The Commission has progressed Omnibus proposals which represent a first step in simplifying regulation. However, there is widespread recognition that the Omnibus proposals are insufficient to address the systemic problems with the EU's rulebook. And at the same time the Commission has progressed a range of new initiatives like its Tech Sovereignty Package, the upcoming Digital Fairness Act proposal, new limitations on access to digital services by minors, and new cybersecurity laws, which risk adding to the existing complexity.

Alarmingly, some of these would add significant new complexity and constraints on innovation. For example:

- CADA would introduce significant constraints on cloud computing firms that wish to compete for public procurement contracts, imposing requirements like data localisation and origin-based supplier requirements. Overbroad requirements impose significant costs on the sector – which could undermine the competitiveness of smaller European providers, who are less able to carry these costs than their larger foreign competitors – and also raise the cost and complexity of procuring cloud computing services to boost public sector productivity. CADA should instead focus on improving investment conditions for cloud, AI and data centres — for example through simpler, faster and more certain permitting processes; through improving access to energy and grid connections; through increasing access to skills and capital; and through regulatory predictability.
- Similarly, the DNA should avoid imposing excessively prescriptive rules which could result in a “levelling-down effect” for countries like Sweden which have forged ahead the fastest in developing advanced connectivity markets. Instead, the focus should be on simplifying end-user, market power and cybersecurity rules and ensuring coordination with, rather than duplication of, existing EU frameworks.
- CSA2 risks imposing very significant costs and risks for businesses, for example by demanding the phase-out of certain ICT components. While we are firmly behind the need for strong cybersecurity standards, far-reaching and high-cost regulatory interventions risk creating legal uncertainty and having unintended effects on investment, business continuity and competitiveness. And any new obligations imposed should only be considered in the context of the extensive set of existing cybersecurity laws in Europe, to avoid unnecessary cost and duplication.

BusinessEurope has published 140+ concrete proposals to significantly reduce the burdens that hold back European businesses, and 29 high-priority reforms impacting the digital sector.¹⁹ In progressing reforms, the Commission must prioritise those which will have the highest impact. In this section we identify the most urgent categories of problems, and specific illustrations of problems within those categories.

¹⁷ European Commission, 'Long-term competitiveness of the EU: Looking beyond 2030', March 16th 2023.

¹⁸ DigitalEurope, 'The EU's Critical Tech Gap: Rethinking economic security to put Europe back on the map', 2024.

¹⁹ Business Europe, 'Reducing regulatory burden to restore the EU's competitive edge', 18 December 2025; Business Europe, 'Simplifying the EU Digital Rulebook: clarity, simplicity, and agility for competitiveness' July 2025.

1. **Overlapping and incoherent obligations**

There is a growing sense of policy uncertainty, incoherence and lack of coordination across the digital rulebook. The sheer complexity of interactions between laws is significant. The Commission recently conducted a review recognising that the Digital Services Act (DSA) interacts with 54 other EU laws, for example.²⁰ This is evidence of significant and growing complexity, posing specific challenges for small and medium-sized enterprises. In the last political cycle, 116 laws relevant to digitalisation were proposed or enacted²¹ involving a vast number of different policy objectives.²² Proposals were progressed in silos by legislators. Conflicting goals between laws were not identified or resolved by law-makers, often leaving supervisory authorities to sort out issues at the implementation and enforcement stage. At the implementation level, authorities or Commission teams tend to be responsible only for implementing or enforcing one particular law (or in some cases, even just one section or article of a law). They therefore have little mandate to grapple with how their approach might fit with other legal obligations. This deters investment, since companies and investors need clear and stable rules to take long-term risks.

The Commission should comprehensively review policy tensions and overlaps – and provide clear, cross-instrument guidance on how different obligations interact.

Protect European firms' intellectual property and trade secrets

One critical example of a policy tension is between laws that aim to promote data portability or a 'data economy' (like the Data Act and DMA) and those that focus on personal data protection or protection of IP (such as GDPR, which imposes strict constraints on the commercialisation of personal data).²³

A fundamental component of European competitiveness is the ability of firms to protect their trade secrets – including their confidential information and innovative business practices and processes. The Data Act, however, directly undermines this protection by requiring firms in certain economic sectors to hand over their data, even if the data include or would enable the recipient to ascertain trade secrets, commercially sensitive data or know-how.

The Data Act envisages that data holders can take steps to require recipients to preserve the confidentiality of trade secrets – however it provides insufficient safeguards to ensure that recipients are trustworthy. It allows firms to stop providing data if the recipient misuses the information, but this is of little assistance when significant data has already

20 European Commission, 'Report on application of Article 33 of Regulation (EU) 2022/2065 (DSA) and the interaction of that Regulation with other legal acts', 17 November 2025, available at <https://digital-strategy.ec.europa.eu/en/library/report-application-article-33-regulation-eu-20222065-dsa-and-interaction-regulation-other-legal>.

21 J Scott Marcus, Kamil Sekut and Kai Zenner, 'A dataset on EU legislation for the digital world', Bruegel dataset, 16 November 2023.

22 These ranged from enhancing digital competition (such as the Digital Markets Act (DMA) and Data Act), to protecting consumers (for example, the Digital Services Act (DSA)), to boosting privacy and cybersecurity (including the Cyber Resilience Act, Cybersecurity Act and NIS2), to supporting strategic European economic activities like chip design and AI (the Chips Act).

23 An example of the tension is the European Commission and European Data Protection Board, 'Joint guidelines on the interplay between the Digital Markets Act and the General Data Protection Regulation', version for public consultation, 2025. The draft guidelines, for example, require DMA gatekeepers to transfer to third parties "personal data of individuals other than the end user" even if the individual did not consent to the transfer.

been transferred – particularly if the recipient of the trade secret is an actual or potential competitor.

This requirement risks having a chilling effect on innovation in Europe, dissuading firms from collecting data. However, this is not only a question of undermining European firms' incentives to invest in data collection and follow-on innovation: it is also a question of economic security, as European firms are forced to hand over commercially sensitive data to a potentially limitless number of third parties, including potentially to countries that do not share European values or which are economic and geopolitical rivals to the EU.

The Digital Omnibus makes some welcome amendments – but it does not solve the underlying problem. It would allow data holders to refuse disclosure if there is a “high risk of unlawful dissemination” to actors in third countries with weaker or non-equivalent protections compared with the EU. However, the Digital Omnibus does not go far enough. The Omnibus would still require European firms to incur unnecessary costs and uncertainty by assessing the level of trade secret protection in foreign jurisdictions and demonstrating the risk of exposure.

Thus, the EU's approach to trade secrets is not yet consistent. On the one hand, the Digital Omnibus acknowledges the risk of unlawful acquisition, use or disclosure of trade secrets and introduces an additional refusal mechanism where disclosure to certain third-country actors would create a high risk. On the other hand, the underlying Data Act logic still pushes companies towards mandatory disclosure of commercially sensitive data, including trade secrets, in broad circumstances. This sends contradictory signals: the EU cannot simultaneously recognise trade secrets as essential to competitiveness and economic security while maintaining rules that force companies to share them without sufficiently strong safeguards. The Digital Fitness Check should therefore assess all EU data-sharing obligations against a clear principle: mandatory access to data must not undermine trade secrets or confidential business information.

Trade secrets should not be treated as ordinary data that can be shared subject only to contractual safeguards. Once they are disclosed, the commercial harm may be irreversible, particularly where the recipient is a competitor or where enforcement of confidentiality obligations is uncertain. The starting point of the Data Act should therefore be that trade secrets and know-how are protected from mandatory disclosure, rather than disclosed unless the data holder can meet demanding refusal conditions.

Recommendation 1: Revise the Data Act to so that data holders have a clear and effective right to refuse to disclose data where access would reveal trade secrets, commercially sensitive information or know-how. Protecting these is key to ensuring economic security and global competitiveness.²⁴ Protection should not depend on companies carrying out burdensome case-by-case assessments of third-country enforcement systems after a data request has already been made. At the very least, the Commission should urgently issue guidance on trade secret protection under the Data Act, as previously promised.

²⁴ Swedish Enterprise, 'Digital Omnibus on the EU Data Act', 3 February 2026.

Recommendation 2: Prioritise completing the revision of the Trade Secrets

Directive, announced in the Commission's 2020 data strategy, to further strengthen the protection of trade secrets.

A single and coherent approach to cross-border data transfers

Another example of incoherence is the relationship between the GDPR and Article 32 of the Data Act regarding international data transfers and third-country governmental access to data. GDPR has long provided a regime governing how EU firms can send datasets which contain personal data outside the EU. However, the Data Act (article 32) introduced an entirely new regime for offshore transfers of industrial data. Together, GDPR and the Data Act require firms to comply with two parallel regimes which use different thresholds and rules, introducing unnecessary complexity and cost burdens. This is unnecessary since almost all scenarios where protection is required in fact involve transfers of personal data.²⁵ Even worse, the standards required for cross-border dataflows under the Data Act are vague, providing little certainty for businesses which want to use foreign tech services or engage in digital trade.

Virtually all European businesses rely heavily on cross-border data flows. The Commission has long recognised that cross-border data flows have a significant positive impact on the EU economy. Removing unnecessary and unduly complex overlapping rules on cross-border dataflows is therefore essential, especially since – where personal data is not involved – businesses can normally be assumed to know how to manage risks associated with transfers of their own data. The Digital Omnibus does not address this problem.

Recommendation 3: The Commission should remove or substantially revise article

32 of the Data Act, which governs international transfers of non-personal data and access to data by third party governments. Firms should not have to comply with two parallel regimes for data transfers: one for personal/mixed datasets and one for other non-personal/industrial data. At minimum, the Commission should clarify that GDPR adequacy decisions and existing transfer safeguards provide a relevant benchmark also for non-personal industrial data, so that firms are not forced to navigate two parallel transfer regimes for the same or closely connected data flows.

2.

Persistent regulatory fragmentation

EU digital laws have failed to support European firms to grow and scale their operations across Europe. European firms in the tech sector incur double the costs of firms elsewhere in the economy when doing business across EU member-state borders.²⁶ Divergences emerge through national 'gold plating', where law-makers add new or

²⁵ See Digital Europe, 'Data transfers in the Data Strategy: Understanding myth and reality', 2022.

²⁶ Erik van der Marel, 'Band-Aids on Bureaucracy: Why GDPR Reform Isn't Enough', European Centre for International Political Economy, October 2025.

additional requirements (or retain pre-existing requirements) that are more onerous than the EU standards. Divergence can also emerge through different interpretations of EU law across member-states. These raise unnecessary barriers to digital firms trying to take an EU-wide approach. A real digital single market could contribute 2% to GDP growth.²⁷

For EU law to deliver a genuine single market in practice, the Commission must conduct a comprehensive review of where member-states (or their authorities) have diverged from, supplemented or failed to implement or consistently interpret EU digital laws. The Commission should either (i) amend EU law so these divergences are resolved; and/or (ii) commit to take enforcement action against those member-states which unlawfully fail to faithfully adopt EU law.

Deliver a true Single Market for data and data protection

A particularly problematic example of single market fragmentation is the GDPR. Despite the GDPR's objective of harmonisation, businesses continue to face divergent interpretations, inconsistent enforcement and national variations across the EU.²⁸ Together with the ePrivacy framework, this creates legal uncertainty, increases compliance costs and undermines the functioning of the Digital Single Market.

Recommendation 4: As part of the DFC, the Commission should conduct a targeted review of the GDPR and ePrivacy framework to address fragmentation, remove unnecessary barriers to the use of data and AI, and to reduce disproportionate administrative burdens and compliance costs for businesses. Creating a more consistent and predictable regulatory framework for businesses should be prioritised before introducing additional data-related or digital regulatory requirements.

3. Lack of proportionality and risk-based approaches

The pace of new law-making has meant that law-makers have paid insufficient attention to ensuring recent laws meet the standards of better regulation. Rather than improving, the EU tech rulebook is becoming less proportionate and risk-oriented and more burdensome over time. Effective innovation and use of technology to deliver productivity growth requires experimentation and sensible risk-taking. Yet the EU rulebook contains too many prescriptive rules – such as requirements on the use of AI – which lock in particular ways of doing business and make it unnecessarily onerous for firms to find new and more efficient ways of working. The Commission should review the rulebook to ensure a proportionate and risk-based approach is applied consistently.

²⁷ European Commission, 'A Digital Single Market Strategy for Europe - Analysis and Evidence', 6 May 2015, SWD(2015) 100.

²⁸ Mario Draghi, 'The future of European competitiveness', September 2024, part B, p 319.

Restoring a genuinely risk-based and proportionate framework for privacy and data protection rules

To become a leader in the AI age, European businesses must be able to freely use data, so long as fundamental rights are protected. At present, the GDPR and the ePrivacy framework together risk making it unviable for firms to use data for innovative purposes, such as to train and fine-tune AI models – even when this serves important public policy goals, such as making AI more representative, accurate and unbiased, and when the risks to individuals are very low.

The GDPR was intended to be risk-based and proportionate. For example, a fundamental requirement of the GDPR is that businesses protect EU citizens' data by implementing "appropriate" measures that take into account "risks of varying likelihood and severity".²⁹

The problem is that, over time, the GDPR – together with the ePrivacy Directive, which governs privacy in the electronic communications sector – has been interpreted to set absolute limits on the use of data. Data protection authorities consequently take a "zero tolerance" approach, emphasising protection where there is little practical risk and without regard to economic and innovation costs.³⁰ They hinder innovation where speed and ingenuity matter – not least because in strategically important fields like developing AI models, access to data is an essential ingredient. And they impose high administrative burdens where costs define competitiveness. This burden is disproportionately felt by SMEs.³¹

As examples of disproportionate approaches, firms are currently required to treat pseudonymised data as personal data, even if the risk of re-identification is very low.³² Similarly, sensitive data can only be processed under specific circumstances, even if the processing is taking place for low-risk and socially beneficial purposes such as to address discrimination and bias in AI systems.³³ And GDPR puts strict limits on how firms can "repurpose" data they already hold, for example to support innovation and new product development. Similarly, the ePrivacy Directive operates as a constraint on website owners' ability to collect valuable information on how their websites are used, in order to improve their services and create innovative new ones. GDPR also imposes significant administrative burdens, for example requiring extensive documentation of decision-making about how data is handled, regardless of the actual level of risk associated with the decision.

The Digital Omnibus would go some way to giving firms the confidence to use data for training, developing and deploying AI models in Europe. But, in doing so, the Omnibus provides a narrow and technology-specific solution for a much larger problem facing innovative European firms. The DFC should go further. In the meantime, the European Commission is proposing, in its Data Union Strategy, new legislative proposals, which risk adding more complexity and overlap to Europe's already-complex regulatory landscape.

²⁹ GDPR art 24.

³⁰ 'GDPR simplification – Nordic position paper', October 2025.

³¹ Mario Draghi, 'The future of European competitiveness', September 2024, Part B, page 319.

³² Digital Omnibus: Commission's proposal definition of personal data, art 4 GDPR.

³³ Digital Omnibus: Commission's proposal, art 9 GDPR.

To unlock a data economy, the DFC should conduct a comprehensive examination of the GDPR and the ePrivacy framework, in order to return to the risk-based approach which was originally intended. This should allow businesses to use data in innovative and responsible ways. Data protection authorities should not adopt a “zero tolerance” approach to risk – but instead ask firms to take measures which are proportionate to the data protection risks and which take into account the economic and social benefits of responsible data sharing and use.

Recommendation 5: Reaffirm and strengthen the risk-based approach in the privacy and data protection framework. The Commission should review the GDPR and ePrivacy framework to ensure that obligations, enforcement and compliance expectations are proportionate to the actual risks posed to individuals. The review should enable the responsible use of data for innovation, research and AI development, particularly where robust safeguards are in place and risks to fundamental rights are low.

Recommendation 6: Reduce GDPR's administrative and compliance costs on businesses in the form of documentation and technical infrastructure requirements. The Commission should simplify the documentation requirements in the GDPR. Administrative burdens and unnecessary paperwork should be reduced, particularly where processing activities present low risks, and compliance obligations should be proportionate and less complex.

Review the proportionality of the AI Act

Concerns about the impact of the AI Act on European competitiveness and innovation have been growing – largely due to its lack of proportionality and approach to risk. The Commission's original proposal took an imprecise approach to risk – treating many AI systems as ‘high risk’ based on factors like the sector in which they are used, rather than on their actual use. The problem became even worse when law-makers added a broad overarching regulation of ‘general purpose AI models’.³⁴ This fails to deliver a genuine risk-based approach: one which facilitates firms creating and using AI models in contexts where there are significant social and economic benefits and the risks to individuals are manageable.

The AI Omnibus will provide some short-term relief by delaying obligations for high-risk AI systems – a welcome recognition that the law's timelines were too quick for industry to feasibly prepare – and by excluding some uses of AI from the AI Act in contexts where comprehensive regulation already applies. However, industry now faces a deluge of secondary instruments. For example, the AI Act includes provision for ten different types of delegated act, and thirteen different types of implementing acts, along with sixteen other types of instruments such as guidelines, codes of practice and recommendations.³⁵ Commission staff have publicly stated that they expect to draft about 70 instruments to properly implement the law.³⁶

³⁴ See Swedish Enterprise, ‘Digital Omnibus on AI’, 3 January 2026; and Zach Meyers, Daniel Schnurr and Pierre Larouche, ‘The AI Act and Technological Neutrality’, CERRE, 25 November 2025.

³⁵ See Pierre Larouche, ‘Legal Framework for an Effective Implementation of the AI Act’, CERRE, February 2025.

³⁶ Kai Zenner, ‘The AI Act: responsibilities of the European Commission (AI Office)’, 10 July 2024.

Many of these documents can significantly affect the scope of the AI Act obligations and the cost of compliance: for example, the Commission's draft guidelines on when AI systems should be treated as 'high-risk' are, in some respects, significantly more onerous on industry than had been expected.³⁷ At the same time, the evolution of the AI market – in particular the growing tendency for models to be refined and repurposed – raises questions about whether the whole approach of the AI Act is future-proofed and fit-for-purpose.

Recommendation 7: The Commission should conduct an overarching review of the AI Act to ensure it represents a genuinely risk-based, proportionate and technically feasible framework – both in its primary text and in its implementation by the Commission's AI Office. The review should also reassess the definition of an AI system to ensure a clear and technically meaningful distinction between AI and conventional software, and address the risk that AI Office guidance expands the concept of AI by conflating autonomy with ordinary automation. As part of this review, the DFC should consider:

- (i) revising the definition of an AI system to ensure that it is sufficiently clear, precise and technologically sound, including by clarifying that "varying levels of autonomy" should not bring conventional software or ordinary algorithmic systems within the AI Act's scope;
- (ii) revising the law so high-risk requirements apply based on genuine risk (not on technological capability or to whole sectors) and impose less administrative cost;³⁸
- (iii) allowing all AI systems (not just those in regulatory sandboxes) to be tested in real-world environments in order to promote more innovation, risk management and adaptation; and
- (iv) removing the requirement for certain AI systems to be registered even if they are proven not to be high-risk systems. This requirement imposes administrative burdens with little benefit to either risk management or transparency.³⁹

4.

Unrealistic timelines and administrative burdens

Excessive administrative burdens and duplication

The overall costs of compliance have also been underestimated. Compliance costs set out in the EU's impact assessments have been dwarfed by the real costs experienced by firms. A recent OECD report highlighted that, in 2023 (the last date when figures

³⁷ For example, under the AI Act, a system is 'high-risk' if the system is intended to be used as a safety component of a product, or is itself a product, regulated by certain EU laws and, under those laws the product requires third-party conformity assessment (AI Act art 6(1)). The Commission's current draft guidelines seem to adopt a wider test that looks not at whether a third-party notified body is involved in the assessment, but also captures cases where third-party conformity assessment can be avoided and harmonised standards can be applied instead. See European Commission, 'Draft Commission guidelines on the classification of high-risk AI systems', 19 May 2026.

³⁸ For example, the Commission's interpretation of the interaction of the AI Act and the Radio Equipment Directive would expand the scope of the high-risk classification into products that may not warrant additional measures. See Business Europe, 'Simplifying the EU Digital Rulebook', July 2025, p 5.

³⁹ AI Act art 49.

were available), 3.9% of employment in Europe was devoted to servicing regulatory compliance and the figure is as high as 5-6% in some parts of Europe, compared to 3.2% in the US.⁴⁰ The EU wide figure is more than double the share of employment devoted to R&D.⁴¹ Mario Draghi showed that the costs of GDPR compliance may reach €500,000 for a small or medium enterprise, and up to €10 million for a larger organisation.⁴² This also has a direct impact on digitisation and innovation. For example, GDPR decreased the data stored by EU firms by 26% and the data processed by EU firms by 15% compared to similar US firms⁴³ - just as the Commission is simultaneously trying to ignite a 'data economy' in Europe.⁴⁴ Importantly, compliance costs tend to hit hardest on smaller firms in the economy, which can often be more innovative.⁴⁵

Duplicative legal requirements are the worst example of driving unnecessary costs onto firms, which are not needed to protect consumers. For example, concepts like 'dark patterns' and 'artificial intelligence', and basic terminology like the term 'product', 'substantial modification' and 'risk', are dealt with in overlapping and unaligned ways across the rulebook. Different terms are used across these laws to identify the same types of technologies. This complicates compliance by firms, enforcement/market surveillance by authorities, and judicial decision-making.⁴⁶ Laws need to be aligned or revised so that the same issue is dealt with once rather than many times – or is at least addressed in a consistent way. In the meantime, a cross-DG taskforce should be set up with industry representation to help ensure consistent implementation and enforcement.

A separate problem is where laws use 'broad brush' approaches when a more narrow intervention would be more effective and efficient. This creates a high risk of unintended consequences and unnecessary compliance cost. The Commission must conduct a comprehensive assessment of existing tech regulation to identify opportunities to cut duplication and unnecessary compliance costs.

Streamline cybersecurity laws

The EU's cybersecurity rules are the worst example of the EU's tendency towards fragmented and overlapping digital laws. Cybersecurity is addressed directly or indirectly in the NIS2 Directive, DORA, GDPR, the Cyber Resilience Act (CRA), the AI Act, product safety and liability legislation, and the GDPR, for example. The Commission has also proposed a revision of the Cybersecurity Act (CSA2) which will also introduce new cybersecurity obligations.

Cybersecurity incident reporting is an area where overlaps are particularly egregious, imposing excessive burden on firms without commensurate benefits. The same attack can trigger reporting under many of the above laws – requiring multiple notifications to different authorities over the same incident. Even worse, the triggers vary depending on the particular obligation.⁴⁷ For instance, while the CRA requires reporting of "actively

⁴⁰ OECD, 'Economic Outlook: Resilient Growth but with Increasing Fragilities', December 2025, p 71.

⁴¹ Ibid.

⁴² Mario Draghi, 'The future of European competitiveness', September 2024, p 319.

⁴³ M Demirer et al, 'Data, Privacy Laws and Firm Production: Evidence from the GDPR', National Bureau of Economic Research, 2024, available at <https://doi.org/10.3386/w32146>.

⁴⁴ European Commission, 'Data Union Strategy', 19 November 2025, COM(2025) 835.

⁴⁵ Mario Draghi, 'The future of European competitiveness', September 2024, Part B, p 318.

⁴⁶ See Business Europe, 'Simplifying the EU Digital Rulebook', July 2025.

⁴⁷ Business Europe, 'Simplifying the EU Digital Rulebook', July 2025, pp 3–4.

exploited vulnerabilities” and “severe incidents”, the NIS2 Directive requires similar reporting of “significant incidents affecting essential and important entities” and the GDPR requires notifications of “significant data breaches” which pose a high risk to individuals. This means the same incident must be rapidly reviewed and assessed against many different standards to determine whether notification is necessary. The timeframes in which notification must be made, the content of the notification, the process of notification, and the authority which must be notified all vary across different cybersecurity instruments. Digital Europe reports that costs of complying with these overlapping requirements amounts to at least €60 billion a year.⁴⁸

The Digital Omnibus seems likely to partially address part of this problem with some common reporting templates. However, it fails to address the most problematic inconsistencies such as setting uniform timelines and triggers for incident reporting and setting up a single point for all incident reports.

Recommendation 8: The DFC must analyse and address the overlaps and inconsistencies between EU cybersecurity laws and adopt a “report once” principle for incident reporting, while ensuring compliance timelines are realistic. This will require harmonising and consolidating incident reporting requirements so there is a single timeline, trigger and reporting point in each country. For example, member-states could be required to designate the same reporting entity for both CRA and NIS2 notifications.

To achieve real burden reduction, this must be accompanied by common templates, definitions, and deadlines and better coordination by supervisory bodies (nationally and at EU level). The goal should be “report once, use many times”, without lowering the level of security. For those EU countries that already have an existing national system for reporting, like Denmark has with the virk.dk portal, the system should be interoperable with the EU platform to ensure “report once only”, minimising duplication and confusion.

More broadly, overlapping cybersecurity laws mean the same company may be subject to several parallel risk management and documentation requirements, often attached to different legal concepts, deadlines, practices, and different supervisory authorities. For example, while NIS2 demands that regulated firms conduct compliance audits on their cybersecurity processes, member-states have imposed different requirements which means an audit in one country will not necessarily be automatically accepted by another country. This means the same process may be subject to multiple audits to meet the requirements of different member-states. This is needlessly costly and complex.

⁴⁸ Digital Europe, ‘Taming the Cyber Storm Whilst Empowering European Businesses To Thrive’, The Download, 2024, available at https://cdn.digitaleurope.org/uploads/2024/11/DIGITALEUROPE-THE-DOWNLOAD-ISSUE-6-FINAL_WEB.pdf.

Unrealistic timelines

EU law-makers have underestimated the demands on regulators to navigate, implement and provide guidance on these laws – and the costs and resources for companies to comply with them. This has led to unrealistic timelines. If laws are not implemented properly because they impose implausible expectations on industry, then the Commission cannot fairly judge if they are successful, which can easily lead to the conclusion that even more rules are required. More emphasis must be given to ensuring proper implementation and enforcement of existing laws before new digital laws are proposed. The Commission should review and be prepared to update timelines which impose unrealistic expectations on industry and supervisory authorities.

The AI Act illustrates that deadlines can often be unrealistic. The Commission did recognise that standards cannot reasonably be finalised by the time the rules for AI deployers take effect. Consequently, the Commission had to propose a delay to implementation of key parts of the law.⁴⁹ But there are many other cases of unrealistic deadlines which have received less attention. These include the Cyber Resilience Act (CRA), which sets cybersecurity standards for internet-connected devices; manufacturers were supposed to be compliant with the Data Act from September 2025 but now need to reassess or redesign their products according to the CRA requirements applicable as of December 2027.⁵⁰ The CRA envisages the development by industry of security standards for a huge number of devices for which no standards currently exist, and relevant standards may only be adopted in October 2027, leaving manufacturers insufficient time to comply. Equivalent laws in the UK and the US are far more modest and realistic in scope.

Another concrete example is the proposed timelines in CADA. A large-scale migration from one hyperscaler to another can take four to five years, yet CADA effectively expects a transition to a European alternative within 12 months. This is neither technically nor operationally realistic and risks disrupting critical services rather than strengthening European cloud capacity.

Review and revise implementation timelines

Industry and regulators are still in the process of implementing and ensuring compliance with the dozens of digital laws enacted by the EU in recent years. While some of the deadlines in these laws would be realistic on their own, the cumulative burden of meeting the compliance deadlines for all these laws is unreasonable. This is true both for public authorities, which must develop guidelines, delegated legislation and supervisory/enforcement functions – and for the private sector.

Recommendation 9: As part of the DFC, the Commission should conduct a systematic review of the 'implementation status' of the EU's digital laws. In doing so, the Commission should identify and address where both individual implementation deadlines, and the cumulative effect of multiple such deadlines, are unrealistic or impose unreasonable demands.

⁴⁹ See proposal for a Digital Omnibus on AI, 2025/0359.

⁵⁰ See Business Europe, 'Simplifying the EU Digital Rulebook', July 2025, p 13.

5. Failure to align with international standards

European firms should be able to compete at a global level – not just to serve the European market. That means European regulation needs to be as harmonised and interoperable as possible with global standards – so that compliance with European laws puts a firm in a strong position to launch in overseas markets.

The EU's digital laws take insufficient account of emerging or already-existing international standards – often because EU law-makers are too concerned with the EU being the 'first mover'. Currently, 59% of EU firms cite compliance with new regulations, standards or certifications as a barrier to international trade (whereas only 42% of US firms do)⁵¹ – which suggests that EU regulation is not well designed to help European firms succeed globally.

The more European laws and standards become idiosyncratic, the bigger the risk that European tech firms fall into the 'Galapagos syndrome': being forced to adopt technological options or business practices that do not fit with demand in the rest of the world. Rather than focus only on being the world's first regulator in emerging policy fields, the Commission should take active part in – and reflect in its own law-making – the efforts of global standardisation bodies. Existing laws should therefore be audited to identify where they create inconsistencies with emerging or existent global standards.

Align with international standards

Misalignment with international standards causes significant problems for European competitiveness – driving up costs for European exporters, making it more difficult for global technologies to be adopted in Europe and complicating Europe's attempts to create global tech champions.

Recommendation 10: As part of the DFC, the Commission should review where and how EU digital laws have diverged from international standards.

The Commission should quantify the costs this divergence imposes on European businesses and consumers and suggest reforms to remove the divergence. It should also ensure that tech laws are designed in a dynamic way, so that firms can adopt relevant international standards as a means of ensuring compliance with EU law.

⁵¹ EIB, 'EIB Investment Survey 2025 – EU Overview', p 12.

How should these problems be addressed?

These problems are no longer ones Europe can afford to ignore. Innovating, and increasing take-up of innovative products, is Europe's key lever to improve its productivity growth and avoid the EU-US economic gap becoming even larger. Fixing these problems does not require Europe to water down regulatory standards. But it does require an honest assessment of why digital regulation has failed to support economic growth or the bloc's position in strategically important sectors – and a determination to address these problems.

The Omnibus packages aim for targeted 'fixes' for specific problems. This is welcome and necessary, even if the AI Omnibus shows that even the Commission's rather modest ambitions are likely to be watered down in the legislative process. However, the overall problem of poor regulatory design – and the problem of the cumulative burden of regulation – requires more than a few targeted fixes. Europe's digital rulebook must be converted from prescriptive rules into modernised and well-designed principles-based laws. And governance structures must be put in place to ensure a coherent and proportionate approach.

Regulatory modernisation is not an end in itself. Its purpose is to help ensure firms, and especially SMEs, feel confident and empowered to adopt new technologies and use them to boost their efficiency and their own capacity to innovate. In this way, improving the digital rulebook is not just about enhancing Europe's tech sector – it is a way to deliver growth across the whole of the European economy and to protect the bloc's economic competitiveness.

To deliver this outcome, we recommend the DFC adopt the following approach to assessing each part of the digital rulebook.

Is a rule still necessary?

When the Commission evaluates an existing digital law or rule as part of the DFC, the first step is to revisit whether the problematic rule is still necessary. Removing a rule does not necessarily mean lowering the EU's standards. Rules may be unnecessary where:

- Dynamics in the sector have changed, so that the market will now deliver the result which was previously thought to require regulatory intervention.
- A lighter-touch approach could deliver the result more efficiently, for example by replacing intrusive rules with a regime for self-regulation or co-regulation.

- A rule has succeeded in its objective and it therefore no longer needs to be kept 'on the books' (i.e. it is now redundant). Some regulatory agencies – such as the UK's Competition and Markets Authority – have undertaken exercises to 'clear out' these types of redundant regulatory obligations.⁵²
- A rule has failed to deliver the intended results. In this case, the rule will impose cost without achieving the benefits law-makers expected.
- Other regulatory rules already require or would result in the same outcome so that the regulatory intervention is duplicative as with important parts of the EU's cyber-security laws, as explained above.

In many cases, these justifications would allow fewer rules – without impacting the EU's regulatory objectives.

If a rule is necessary, can it be modernised?

Where the Commission concludes that regulatory intervention is still required, then a modernised regulatory approach is needed. This approach should be risk-oriented and principles-based to help reduce complexities, inconsistencies and unnecessary costs. This modernised approach should prefer lighter-touch and tightly targeted interventions over onerous broad-brush rules. It should be technology-neutral so the rule is future-proofed. Well-designed regulation should give European businesses freedom to innovate and adapt to – and drive – market and technological changes: allowing firms to experiment as long as they do so responsibly and by mitigating the risks of their business practices. This means modernised regulation should demand outcomes rather than prescribe the detailed way in which firms should achieve those outcomes.

As a positive example, the DSA requires the largest online platforms to identify and mitigate certain systemic risks caused by their services. But it does so without prescribing what those large platforms must do. This is a sensible approach, since tackling problems like disinformation is complex, context-specific, and needs to evolve to make use of new technologies like AI. Similar approaches could be used in other areas like AI regulation and data protection.

The benefit of this approach is three-fold:

- First, this approach **promotes innovation**, because firms are not automatically deemed to be non-compliant simply because a risk has materialised. They are judged on how well they have mitigated risks – rather than on factors that could be outside their control.
- Second, this approach **minimises the risk of inconsistencies or policy tensions** with other laws, since it avoids prescriptive detail.
- Third, because regulators do not need to be engaged in complex technical detail, these laws are **easier to implement** – helping free up regulatory resources which can be used to provide proactive guidance for firms trying to understand their obligations.

Designing laws in this way can enable firms to better experiment and adopt new technologies – since it does not impose unrealistic or unachievable goals like requiring all

⁵² Competition and Markets Authority, 'Reviews of three merger undertakings and one market investigation Order', 21 November 2023.

risks to be fully eliminated when that is not possible. Risk-based regulation could be delivered through tools like more meaningful industry engagement, the wider availability and attractiveness of regulatory sandboxes, the use of digital implementation tools to streamline compliance, and harmonised practical clear guidance.

This approach must also reduce the excessive use and scope of implementing and delegated legislation. Delegated laws have an important role to play in the regulatory framework. But their number has increased dramatically in recent years. They are not subject to the same safeguards or scrutiny as primary legislation. They are increasingly used to expand the scope of laws or to introduce substantive and onerous new requirements – despite EU treaties requiring that the objectives, content, scope and duration of delegated acts are properly defined.⁵³ Excessive use of delegated legislation is a significant cause of complexity and unpredictability. The DFC should also analyse how much compliance detail is set out in secondary legislation, standards, and regulatory documents such as guidelines.

How can new policy tensions be avoided?

The Commission should systematically assess the risk of policy tensions or inconsistent application of a law when proposing new legislative initiatives, and as those proposals make their way through the legislative process. This should firstly be identified through strengthened and more robust impact assessments when an initiative is first proposed. The Commission should conduct updated assessments as the Council and MEPs' positions are made clear – reflecting the recommendation in Enrico Letta's report for a 'dynamic impact assessment' to be introduced into the law-making process.⁵⁴

Where a policy tension or potential for inconsistency is identified, law-makers should either address it up-front, or should include a mechanism to address it quickly in the implementation stage.

Reform governance of the digital rulebook

In a democratic society, it is natural that policy-makers will have multiple policy objectives for the digital sector – and that these different objectives will not always be in perfect alignment. A degree of tension between different objectives in the digital rulebook is therefore inevitable. If these are tackled by policy-makers clearly and efficiently, the problem is tolerable. Today, however, policy trade-offs and tensions are often ignored. Coherence of interpretation is often imposed only by courts following lengthy litigation. This is neither efficient nor desirable given the speed of innovation in technology markets – and the uncertainty can cause immense opportunity costs in the meantime as investments are delayed and innovation does not take place.

Addressing this problem will require the Commission to rethink the governance of the digital rulebook, and the structure of supervision and enforcement. For example, there may be a case for EU bodies rather than national authorities to play a stronger role in order to avoid fragmentation between member-states. At a minimum, laws like the GDPR need to be revised to allow cross-national fragmentation to be addressed rapidly, reflecting the pace of emerging technologies.

⁵³ Treaty on the Functioning of the European Union, article 290.

⁵⁴ Enrico Letta, 'Much More Than a Market', April 2024, p 124.

However, the incoherence of European digital rules also arises from tensions between different EU digital rules, rather than between countries. That may require the DFC to examine how to enable (and require) regulators to better cooperate and develop common policy approaches where regulatory trade-offs arise, particularly at the intersection of competition, data protection, and consumer law.

These arrangements could include structured dialogue between different public authorities to help produce simpler, cross-cutting guidance; the creation of a permanent mechanism to coordinate across Commission Directorates-General to help ensure a more coherent and consistent approach within the Commission; and the adoption of simpler and more principles-based laws which can minimise the risk of inconsistencies between legal regimes. These mechanisms should systematically allow for early industry input to ensure guidance is workable and that policy tensions are resolved before they create unnecessary uncertainty for businesses. The goal would be to stop authorities thinking in 'regulatory silos' and instead ensure they deliver practical guidance which reflects businesses' need for simplicity, predictability and coherence.

Recommendation 11: The DFC should propose reforms to the governance arrangements for the EU's digital acquis so that firms can more easily understand how to comply with the EU's rulebook and to enhance the predictability, coherence and consistency of enforcement.

Many EU digital laws already provide mechanisms for regulatory coordination, such as the European Data Innovation Board under the DGA or the High-Level Group under the DMA. However, these tend to be ad hoc, specific to particular laws, have their own powers, participants and processes, and they are not always comprehensive in the types of authorities that can take part (for example, cybersecurity agencies are not part of the DMA High-Level Group, despite many of the DMA's obligations having implications for cybersecurity). Their ad hoc nature means they can in fact add to the complexity of the regulatory landscape. A more consistent approach – with one body responsible for coordinating all relevant authorities across all relevant digital laws – might be a better approach. We urge the Commission to ensure the ability and incentive for regulatory agencies to cooperate among themselves and with industry. In this context, we welcome the Commission committing to examine *'good practices and challenges in the interplay between the different governance systems for implementing and supervising the rules, including cooperation and consultation mechanisms between authorities and EU-level cooperation through boards and other fora'*.

An alternative or supplementary model would be to empower industry more closely in the process of identifying and suggesting (through self-regulatory or co-regulatory mechanism) how firms should balance competing policy objectives.

Make the DFC-scope sufficiently broad

The Commission has been right to follow a pragmatic approach where it first tackles – through the Omnibus packages – a targeted number of specific and well-identified problems with the rulebook.

However, the problems tackled in the Omnibus packages are only the tip of the iceberg – and the co-legislators' positions show that even the Commission's somewhat modest ambitions with the Omnibus packages are unlikely to be fully achieved. What the Omnibus packages have uncovered is a set of problems which are systematic and run throughout the digital rulebook, requiring “root and branch” reforms to both substance and governance. It is therefore essential that the scope of the DFC is sufficiently broad – and covers both the existing rules and those which are already in development, without prejudging whether ongoing initiatives should continue, be adjusted or reworked.

Review both existing and ongoing legislative initiatives

While the Commission has been working to simplify the digital rulebook, it has also been progressing new initiatives that may introduce additional complexity and constraints on innovation, including CADA, the DNA, CSA2, Chips Act 2.0 and the Digital Fairness Act proposal. In some cases, as explained above, these initiatives risk unintentionally putting European tech firms at a significant disadvantage compared with foreign competitors and creating further regulatory uncertainty. At the same time, ongoing initiatives may provide necessary clarity for specific sectors.

Recommendation 12: Review both existing and ongoing legislative initiatives through the DFC to ensure coherence, proportionality and a reduced overall regulatory burden. Ongoing initiatives, including the DNA and CADA, should be assessed as part of this process. All initiatives should support competitiveness and innovation and contribute to a coherent and streamlined rulebook, without unnecessary duplication, overlaps or uncertainty.

In the medium term, the need for a DFC should give the Commission pause to reflect on how it can adopt processes for better rule-making. These processes could include improving the robustness of impact assessments and being more realistic about administrative and implementation costs of new proposals.⁵⁵ They also call for a change in the governance of the EU's digital laws to enhance coordination by regulators.

Europe's digital firms are burdened by large regulatory compliance costs. But the impacts of the EU's digital rulebook are felt far beyond the tech sector. To boost productivity, firms across the European economy, in every sector, must be encouraged to adopt new technologies, and be able to use them to become more efficient and innovative. Currently, however, the digital rulebook serves as a hindrance to that outcome – in turn, holding back Europe's overall competitiveness. A more competitive and innovative Europe demands a modernised regulatory environment that will encourage entrepreneurs and SMEs to choose Europe – and to stay in Europe as they grow.

⁵⁵ Swedish Enterprise, 'New regulations in Europe's digital economy: design, structure, trade and economic effects', June 2023, p 57.

For further information:

- a) Swedish Enterprise position paper on the [Digital Omnibus](#)⁵⁶
- b) Swedish Enterprise position paper on [AI Omnibus](#)⁵⁷
- c) Swedish Enterprise position paper on [on ePrivacy in the Digital Omnibus](#)
- d) [Nordic position paper](#) on how to simplify the GDPR⁵⁸
- e) [BusinessEurope position paper](#) on simplifying the digital rulebook.⁵⁹
- f) BusinessEurope position paper on [Making the General Data Protection Regulation more effective](#)

⁵⁶ Swedish Enterprise, 'Digital Omnibus on the EU Data Act', 3 February 2026.

⁵⁷ Swedish Enterprise, 'Digital Omnibus on AI', 3 January 2026.

⁵⁸ 'GDPR simplification – Nordic position paper', October 2025.

⁵⁹ Business Europe, 'Simplifying the EU Digital Rulebook', July 2025.

Confederation of Swedish Enterprise

www.svensktnaringsliv.se

Adress: Storgatan 19, 114 82 Stockholm

Phone: +46 (0)8 553 430 00