SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

RESPONSE TO

European Commission's Digital Fitness Check Call for Evidence

MARCH 2026

Contents

Contact information:

Carola Ekblad carola.ekblad@svensktnaringsliv.se
Carolina Brånby carolina.branby@svensktnaringsliv.se

Introduction and executive summary

Europe's share of the global ICT market nearly halved over the period 2013-22.[1] It is lagging the US and China in seven of the eight most strategic technologies.[2]

The volume, quality and cumulative burden of regulation is an important barrier to the success of the bloc's technology sector – and to the take-up of new technologies by European businesses across all sectors of the economy to improve their productivity. In this context, the Digital Fitness Check (DFC) is a unique opportunity to restore 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.

Swedish Enterprise has already contributed to the discussion of how to improve regulation in 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] This response 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.

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

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

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.

We see the key problems being the following:

1. Regulatory fragmentation

The economic value of a genuine digital single market would be immense.[8] 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

2. Overlapping and incoherent obligations

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

Read more

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

4. Unrealistic timelines and administrative burdens

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

Read more

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

8 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.

As an overarching recommendation, the Commission must review and address where member-states have diverged from a consistent set of single market rules. It must also provide clear, cross-instrument guidance on how different obligations interact in practice. And it should identify where rules are disproportionate or misaligned with global standards. In relation to specific files, we ask the Commission to focus on the following concrete solutions:

- **Data Act:** strengthen protection of trade secrets and remove article 32X so firms do not have to comply with two parallel regimes for data transfers: one for personal/mixed datasets and one for other non-personal/industrial data.
- **GDPR and ePrivacy:** return to the risk-based approach that was originally intended, rather than precluding the use of data for innovative purposes. Reduce the enormous administrative and compliance costs on businesses in the form of documentation and technical infrastructure requirements. Conduct a holistic review of the ePrivacy Directive and GDPR to avoid fragmentation and ensure a future-proofed regime.
- **Cybersecurity:** review how the EU's cybersecurity rules as a whole effect European competitiveness. Analyse how the rules affect the time to market of products, global supply chains and the ability of tech companies to scale internationally. Increase coordination, clarify responsibilities, reduce overlaps and tighten the relationship between risk and regulatory burden.
- **DSA and DMA:** implement and enforce these laws in ways which are harmonised across the EU, while ensuring a fair and even regulatory playing field for businesses in the European market.
- **AI Act:** even if the AI Omnibus is enacted quickly, the Act still needs significant additional improvement to be proportionate and risk-based. This includes:
  - » 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.
  - » Allowing all AI systems (not just those in regulatory sandboxes) to be tested in real-world environments for innovation, risk management, and adaptation.
- **Copyright:** develop an EU-level policy response to the questions of how IP laws apply to new technologies to protect technological innovation and artistic expression, while avoiding a proliferation of inconsistent national solutions.

The Commission must aim higher than applying narrow fixes to the worst problems with the rulebook today, as in the Omnibus proposals. This is an opportunity to conduct a 'root and branch' review – fixing laws which are inflexible, incoherent, and idiosyncratic in a global context, and cutting barriers to businesses growing within Europe. The Commission needs a modernised approach: with simpler, more flexible, proportionate laws, which draw on principles-based regulation. Reforms should foster responsible innovation, and the diffusion of technology across all sectors of the European economy - rather than rigid and prescriptive rules which hold back the EU's potential.

Problems with the EU's digital rulebook and their impact

It is widely recognised that the EU's GDP is falling further behind that of the US, and that a large part of the gap is down to Europe's weakness in both innovating and incorporating digital technologies into firms' working practices to boost efficiency.[9]

Regulation is undoubtedly a significant barrier to the tech sector's growth. Approximately 69% of businesses across Europe cite regulation as a barrier to investment and growth:[10] a figure which has grown significantly in recent years.[11] Regulation is often cited as among the most important of all the obstacles to growth.[12] For example, 40% of Swedish companies state that regulatory burden and bureaucracy are among the top two significant obstacles to growth.[13] And European businesses are more likely than US firms to cite regulation as a major obstacle to doing business.[14]

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.[15] 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.

1. 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.[16] Divergences emerge through national 'gold plating', where law-makers add new or additional requirements (or retaining 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.[17]

---

9 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.

10 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.

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

12 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.

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

14 EIB, 'EIB Investment Survey 2025 — EU Overview', p 29.

15 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.

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

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

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.

The following are examples of fragmented EU regulation:

- **DSA and DMA:** there are numerous examples of EU member-states supplementing the EU's Digital Markets Act and Digital Services Act with national laws covering similar topic, such as digital competition[18] or online content regulation.[19] There is also intra-EU divergence on whether business practices like imposing 'narrow MFN clauses' are permissible. The Commission needs to implement and apply the DMA and DSA in ways that set a uniform set of standards across the EU. This is essential so EU firms can benefit from having a uniform approach to dealing with the same large digital platform across Europe, and so that tech platforms can adopt a single approach to compliance. At the same time, simplification reforms must maintain a fair and even playing field for EU businesses in the European market.
- **GDPR and ePrivacy Directive:** these laws are renowned for their inconsistent interpretation and application by different national (and in some cases sub-national) data protection authorities. In addition to inconsistent interpretation of GDPR itself, GDPR allows member-states to define their own aspects of privacy rules in at least 15 different areas.[20] The Commission should conduct a holistic review of the ePrivacy Directive and GDPR to avoid fragmentation and ensure a future-proof regime.
- **Lack of coherent policy on AI and copyright:** emerging technologies are challenging for copyright legislation and practices. This is true for several emerging technologies, but especially the use of AI. Currently, there is no EU-level policy response to how IP laws should deal with these challenges, which creates uncertainty and risks proliferation of inconsistent national solutions. The Commission must urgently develop a position in order to find the right balance between promoting technological innovation and protecting IP holders and artistic expression. It is not an either-or situation. Regulation must clearly distinguish between harmful misuse, on the one hand, and lawful applications on the other.

18 For example, the Digital Markets Act — despite purporting to be a law aimed at addressing the risk of legislative divergence across member-states — co-exists with art 19a of the German competition law, which covers similar market problems in a different way.

19 Laura Aade & Catalina Goanta, 'Ban-It-Harderism in European Consumer Law: The Case of the French Influencer Law', Journal of Consumer Policy, vol 48, 2025, p 523. The Commission has set up a database for member-states to record where they had engaged in 'gold-plating'. However, this database has very rarely been used: member-states are reluctant to admit when they engage in 'gold-plating' and to subject these decisions to Commission scrutiny.

20 Mario Draghi, 'The future of European competitiveness', September 2024, part B, p 319. Third, the Commission not pursuing member-states that fail to properly adopt EU law (or, as with NIS2, adopting it on different timescales). The number of new proceedings has been in continuous decline since 2020. In 2023, the last year for which figures are available, the Commission opened the fewest number of cases against member-states for failure to implement EU laws than in any of the preceding five years. This contributes to an atmosphere of unaccountability by member-states.

2. 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 DSA interacts with 54 other EU laws, for example.[21] 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 enacted[22] involving a vast number of different policy objectives.[23] Proposals were progressed in silos by legislators. Conflicting goals between laws were not identified or resolved by lawmakers, 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.

The following are examples of policy tensions and overlaps between laws:

- **Data laws, intellectual property and trade secrets:** there is a policy tension between laws that aim to promote data portability or a 'data economy' (like the Data Act and DMA) and those that focus on data protection or protection of IP (such as GDPR, which imposes strict constraints on the commercialisation of personal data).[24] The rulebook needs to better tackle the policy trade-offs, for example the Data Act should respect the need for EU firms to protect their trade secrets since these are key to ensuring economic security and global competitiveness.[25] The revision of the Trade Secrets Directive, announced in the 2020 data strategy, must be completed to further strengthen the protection of trade secrets.
- **Data Act and cross-border data transfers:** 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 32X) introduced an entirely new regime for offshore transfers of industrial data. This requires firms to comply with two

21 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.

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

23 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).

24 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.

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

parallel regimes which use different thresholds and rules, introducing unnecessary complexity and cost burdens. The Commission should ideally remove the Data Act regime but at a minimum, to reduce complexity, it should clarify that countries which provide adequate protection under the GDPR are also suitable destinations for non-personal data transfers.

- **DMA, privacy and cybersecurity:** The DMA demands more openness from digital platforms like operating systems. However, when implemented without sufficient safeguards, openness can pose privacy and security risks. This, in turn, is in tension with cybersecurity laws, which imposes security standards on operating system providers. While the DMA has privacy and security safeguards these are only partial and their operation is untested. A more holistic approach to resolving this policy tension is essential.
- **Cybersecurity:** The EU's cybersecurity laws are fragmented, overlapping and the same company may be subject to several parallel risk management, reporting and documentation requirements, often with different concepts, different deadlines and different supervisory authorities. The fitness check should especially analyse the interaction between the NIS2 Directive; the Cyber Resilience Act (CRA); DORA; the AI Act; product safety and liability legislation; and the GDPR. These rules collectively impose significant unnecessary administrative complexity and burden.

3. Lack of proportionality and risk-based approaches

The pace of new law-making has meant that lawmakers 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, particularly for SMEs. 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.

The following are examples of a lack of proportionality in EU laws:

- **AI Act:** 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 is become even worse given law-makers added a broad overarching regulation of 'general purpose AI models'.[26] To make the AI Act more risk-based, the Commission should:

  (i) Amend the AI Act so that all AI systems (not just those in regulatory sandboxes)

26 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.

can be tested in real-world environments in order to encourage innovation, risk management and adaptation.

(ii) Revise the law so high-risk requirements apply based on a system's genuine level of risk (not on technological capability or the sector it is deployed in) and impose less administrative cost.[27]

(iii) Remove the requirement for certain AI systems to be registered even if they are proven not to be high risk systems.[28] This requirement imposes administrative burdens with little benefit to either risk management or transparency.

- **GDPR:** 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]). However, over time the GDPR has been interpreted to set absolute limits on the use of data, and data protection authorities emphasise protection where there is little practical risk and without regard to economic and innovation costs.[30] The Omnibus proposals leave problems unaddressed. To reduce administrative burdens and unlock a data economy, the Commission should:

  (i) provide guidance on how firms can mitigate risks while using data to train and adapt AI systems and models;

  (ii) delimit the obligations for pseudonymised data;[31] and

  (iii) amend GDPR so data processors can process special categories of personal data where necessary and justified (e.g. for bias mitigation in AI models).

  GDPR also imposes disproportionate costs by making it difficult and onerous to conduct cross-border data transfers (for example, because 'transfer impact assessments' need to be produced) even in cases where the risk of a breach is only theoretical.[32]

- **The Data Act** provides an illustration of a law which is not well targeted. The law forces firms which produce smart data-generating devices to share that data with other firms. The stated purpose of the Act is to increase competition, and indeed the Act may help in cases where dominant firms are 'hoarding' data. But most connected devices are sold in highly competitive markets. By applying the same rules to all manufacturers — even markets where there is no evidence of any competition problem — the Data Act reduces firms' incentives to collect valuable data in the first place, and burdens many firms with unnecessary costs. As noted above, at a minimum the Commission should increase protection of trade secrets to minimise the law's impact on innovation.

27 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.

28 AI Act art 49.

29 GDPR art 24.

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

31 De-identified or pseudonymised data is often sufficient for innovation and can have minimal risk to individuals. See Zach Meyers, 'Helping Europe's digital economy take off: An agenda for the next Commission', CER, February 2024; and article 4 in 'GDPR simplification — Nordic position paper', October 2025.

32 The Swedish National Board of Trade report estimates that, after the introduction of the GDPR, the profit margins of data-intensive firms in the EU increased by 1.7 to 3.4 percentage points less than the profit margins of US counterparts. Cited in https://www.cer.eu/insights/making-eus-digital-regulatory-reset-count-four-recommendations. See also 'GDPR simplification — Nordic position paper', October 2025.

- **Cybersecurity:** High cybersecurity standards can be a competitive advantage for Europe. However, the DFC should assess how the laws as a whole affect European competitiveness – including the time to market of products, global supply chains and the ability of tech companies to scale internationally. The DFC should clearly test whether the cybersecurity requirements are risk-based, technology-neutral and proportionate to the actual threat. Requirements for e.g. incident reporting, vulnerability management and third-party management must be reasonable in relation to the importance and exposure of the business, to avoid undermining the focus on truly critical risks. To ensure proportionality, the DFC should also examine whether key concepts ("material incident", "sufficient measures", "state of the art") are sufficiently precise for companies to be able to predict in practice what is required for regulatory compliance. A risk-based approach also requires cybersecurity laws to be adaptable to how value chains work. Cybersecurity is increasingly regulated upstream, e.g. through the CRA's requirements for products with digital elements. This risks creating uncertainty about the division of responsibilities (e.g. between manufacturers, integrators, distributors and users). It also risks regulatory responsibility no longer lying with the entity which is best placed to manage it.

4. Unrealistic timelines and administrative burdens

Unrealistic timelines

EU lawmakers 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 has recognised that standards cannot reasonably be finalised by the time the rules for AI deployers take effect. Consequently, the Commission has had to propose a delay to implementation of key parts of the law.[33] 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.[34] 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.

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

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

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 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.[35] The EU wide figure is more than double the amount the share of employment devoted to R&D.[36] Mario Draghi showed that the costs of General Data Protection Regulation (GDPR) compliance may reach €500,000 for a small or medium enterprise, and up to €10 million for a larger organisation.[37] 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 firms[38] - just as the Commission is simultaneously trying to ignite a 'data economy' in Europe.[39] Importantly, compliance costs tend to hit hardest on smaller firms in the economy, which can often be more innovative.[40]

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.[41] 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.

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

36 Ibid.

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

38 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.

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

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

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

Cybersecurity incident reporting provides a significant example of excessive burden – the same attack can trigger reporting under many different laws (NIS2, DORA, GDPR, CRA, etc.) but the triggers, timeframes, processes and national authority vary depending on the particular obligation.[42] Digital Europe reports that costs of complying with these overlapping requirements amounts to at least €60 billion a year.[43]

Nordic businesses support a central reporting entry point across EU legislation and Member States, as proposed by the European Commission. If this is not achieved in the digital Omnibus, it should be addressed in the DFC. 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 Demark has virk.dk, it should be interoperable with the EU platform to ensure "report once only", minimising duplication and confusion.

Other overlaps include reporting of unsafe and illegal products under the GPSR, DSA and the Market Surveillance Regulation.[44]

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 lawmakers 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)[45] – 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.

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

43 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.

44 Business Europe, 'Simplifying the EU Digital Rulebook', July 2025, p 4.

45 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 a key lever for productivity. 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. Europe's standards must be converted from prescriptive rules into modernised and well-designed principles-based laws. Regulatory modernisation can enhance the EU's innovative capacity and its competitiveness.

The digital Omnibus approach aims for targeted 'fixes' for specific problems. This is welcome and necessary. However, the overall problem of poor regulatory design – and tackling the problem of the cumulative burden of regulation – requires more than a few targeted fixes.

Is a rule still necessary?

When the Commission recognises a digital law requires reform, 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.[46]
- A rule has failed to deliver the intended results. In this case, the rule will impose cost without achieving the benefits lawmakers 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 cybersecurity laws, as explained above.

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

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

If it is necessary, can a rule 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 rules are 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.

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.

Similar approaches could be used in other areas like AI regulation and data protection. 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 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.[47] 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.

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

Finally, EU laws need mechanisms to ensure timely implementation and coherent interpretation of EU law across the EU – and its consistency with global standards.

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.[48]

Where a policy tension or potential for inconsistency is identified, lawmakers should either address it up-front or should include a mechanism to address it quickly in the implementation stage. Today, coherence of interpretation is eventually imposed by courts, but this is neither efficient nor desirable given the speed of innovation in technology markets – and lack of harmonisation can cause immense costs in the meantime.

Addressing this problem may require the Commission to rethink the structure of supervision and enforcement – so that EU bodies rather than national authorities play a stronger role. Alternatively, it may mean better enabling (and requiring) national regulators to develop common policy approaches where regulatory trade-offs arise, particularly at the intersection of competition, data protection, and consumer law. This should be applied not only to new laws but – within the context of the DFC – to the existing acquis.

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, 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.

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

Conclusion

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. This DFC is an essential next step. We urge the Commission to be ambitious. 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.**

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 such as improving the robustness of impact assessments and being more realistic about administrative and implementation costs of new proposals.[49]

Europe's digital firms are burdened by large regulatory compliance costs. But the biggest cost to Europe is for the missed opportunities – entrepreneurs which never saw their ideas succeed, or which moved to other parts of the world to launch innovative products and services and therefore are not present to highlight the cost and burden of poorly designed regulation. 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.

For further information:

a. Swedish Enterprise position paper on the Digital Omnibus
b. Swedish Enterprise position paper on AI Omnibus
c. Swedish Enterprise position paper on ePrivacy in the Digital Omnibus
d. Nordic position paper on how to simplify the GDPR
e. BusinessEurope position paper on simplifying the digital rulebook.
f. BusinessEurope position paper on Making the General Data Protection Regulation more effective

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

Confederation of Swedish Enterprise
www.svensktnaringsliv.se

Adress: Storgatan 19, 114 82 Stockholm
Phone: +46 (0)8 553 430 00