Technology Industries of Finland

06 March 2026

Recommendations for the Digital Fitness Check

Technology Industries of Finland sets out these recommendations to contribute to the Digital Fitness Check and to support a regulatory approach that strengthens Europe's competitiveness in the digital domain. Europe should restore the link between regulation and the Single Market. Instead of rushed volume and omnibus-scale mistakes, regulation should be guided by necessity, consistency, and—above all—quality.

The Digital Fitness Check should urgently address inconsistencies—different definitions and interpretations—across the whole acquis of EU data and digitalisation legislation and assess their cumulative impact on the European market.

Europe's main digital regulatory challenge is inconsistency and lack of scale. Much of this stems from the GDPR being interpreted and implemented in divergent ways across Member States. Another key problem is the weak application of a risk-based approach, which creates disproportionate friction even where risks are low.

The Commission should strengthen the digital Single Market by enabling uniform, standardised and risk-based compliance. This is essential to spur service development and unlock digital investment. Without it, the European data economy will not reach its potential. Europe should also prioritise the development of enabling data infrastructure—most notably through Data Spaces—where industry should lead the way to accelerate investment and uptake.

At the same time, the Digital Fitness Check should be treated as a strategic opportunity to rethink the regulatory approach. Regulation should focus on durable principles that underpin the market and, in carefully selected areas, on targeted initiatives of "surgical precision" that can trigger momentum.

Our key recommendations are:

1. Put quality and consistency first, and restore the link to the Single Market
2. Ensure standardised, automated, and scalable compliance
3. Harness digital to complete the Single Market
4. Decrease the role of EU and Member State public sector actors in cybersecurity

Put quality and consistency first, and restore the link to the Single Market

The EU digital acquis must prioritise quality, consistency, and legal certainty over regulatory expansion. The Digital Fitness Check should focus on fixing the existing framework by aligning core definitions and concepts. Future legislation should be strongly linked to the development of the Single Market. In practice, initiatives must either remove bottlenecks or resolve inconsistencies that hold back progress. A vibrant digital Single Market with competing providers is the best guarantee of European values.

Technology Industries of Finland

Eteläranta 10, P.O.Box 10, FI-00131 Helsinki
Telephone +358 9 192 31
www.techind.fi
Business ID: 0215289-2

- **As a rule, refrain from introducing new legislative proposals** in the digital space during the ongoing European term, to allow companies, organisations and public authorities to adopt the legislative frameworks that have recently entered into application. New regulatory initiatives should be limited to building and enhancing the Single Market and facilitating data flows with third countries.

- **Harmonise definitions and concepts across the EU digital acquis**, to reduce legal uncertainty, overlapping obligations, and compliance costs for companies operating across the Single Market.

- **Use regulations rather than directives as the legislative instrument for EU digital legislation**, to ensure uniform application across the Single Market and avoid fragmentation arising from divergent national transposition.

- **Design regulation for standardised implementation**. The Single Market cannot develop if every actor interprets the rules differently.

- **Move to genuinely risk-based requirements—now**. The EU urgently needs approaches that adjust requirements to the risks posed to data subjects and society.

- **Provide sufficiently long grace periods between entry into force and application**. Where compliance relies on harmonised standards, application should, as a rule, begin no earlier than 12 months after the relevant harmonised standards are made available, to ensure predictable and workable implementation.

- **Ensure prospective application and non-retroactivity of EU digital legislation.** New requirements should apply only to products and services placed on the market after the date of application, avoiding disproportionate compliance burdens for existing deployments. Legislation should reflect market realities at the time of application and allow sufficient time for harmonised standards and contracts to develop.

- **Require the systematic use of dynamic and collaborative ex ante impact-assessment mechanisms**—such as testing regulatory options and preparing supportive structures for application (e.g. standards and contracts)—when developing new regulation for digital markets and technologies. This will help ensure legislation is fit for purpose, innovation-friendly, and future-proof.

- **Develop machine-readable regulations with open APIs** to enable real-time compliance checks and automated reporting and to streamline interactions between businesses and regulatory authorities. Digital reporting solutions must be in place before introducing new obligations for companies. Review existing legislation to identify reporting requirements that can be met digitally and automated, reducing administrative burdens.

Harmonise enforcement to build the Single Market

The effective and uniform enforcement of AI and data laws hinges on strong coordination, clear guidance, and well-resourced regulators. A harmonised approach across Member States is a sine qua non requirement for a Digital Single Market where solutions can scale. Cross-sector cooperation and the continuous upskilling of authorities are essential to keep pace with technological advancements and ensure robust oversight.

- **Build a strong and cohesive enforcement mechanism for AI and data laws to ensure uniform application of the acquis**. As regards the AI Act, the EU's new AI Office should take a lead role in harmonising the Regulation's enforcement across Member States, drawing lessons from the GDPR's fragmented implementation. The European Data Innovation Board should similarly ensure the uniform enforcement of the Data Act and evolve into a credible counterpart to the EDPB, helping to strike a better balance between data protection and data use.

- **Establish formal cooperation channels** between data authorities, competition authorities, consumer protection agencies, and the new AI regulators. Many issues span multiple domains, so joint investigations and info-sharing will lead to more effective enforcement. National authorities should be provided clearer guidance and expert assistance to oversee compliance. To this end, thematic subgroups for national Data Act regulators should be created under the EDIB. Additionally, invest in joint training programmes to equip regulators with required knowledge, allowing them to keep up with fast-evolving technologies.

Promote regulatory technology to reduce administrative burdens

The European Commission should launch a programme dedicated to promoting the development and deployment of regulatory technology (RegTech). The effective use of RegTech solutions is a key enabler in reducing administrative and reporting burdens, as this technology can help in navigating regulations, automating compliance processes, enhancing data interoperability, and improving regulatory oversight without adding complexity for businesses. The programme should perform at least the following functions.

- **Support the development of RegTech tools and services** to simplify compliance with digital and other EU regulations. Prioritise funding for companies innovating in this space, especially SMEs and startups using AI-powered systems, to enhance automation in compliance checks, data privacy, and conformity assessments.

- **Create a RegTech Innovation Platform** to unite users, regulators, and RegTech companies in developing advanced RegTech tools. This platform would enable the sharing of best practices, host innovation challenges, and support collaboration across Member States to ensure that tools remain aligned with regulatory changes.

- **Ensure that RegTech solutions are accessible** to companies and authorities through European Digital Innovation Hubs, trade associations, regulatory sandboxes, official digital and data coordinators, and other relevant networks and channels.

Example: A joint Finnish–Danish initiative released digital tools to clarify the AI Act, the Data Act, and the EHDS Regulation

Public and private parties in Finland and Denmark came together in a joint action to produce a catalogue of e-tools to explain and educate industrial actors on the AI Act, Data Act, and European Health Data Space regulation. The pilot was partly funded by Technology Industries of Finland. These e-tools were provided by Lean Entries through their Entries platform, in English, and were free to use for all Finnish industrial sectors and the Danish health tech sector by the end of 2025.

Construct the building blocks of the European real-time economy

The European Commission should expand and solidify the underlying "soft infrastructure" of the Digital Single Market by launching a comprehensive programme on the interoperable building blocks of the real-time European economy, including the European Business Wallet, with the aim of easing and automating B2B transactions and B2G reporting (e.g. in taxation and sustainability) across Member States. The programme should include at the least the following measures.

- **Make digital identity infrastructure widely available for companies through the European Business Wallet**. The technical framework should guarantee a high level of security and interoperability across the EU while allowing private sector providers to develop wallets that serve specific use cases. This flexibility will ensure that identity control instruments can adapt to diverse business needs, such as data sharing between multiple parties, while maintaining a harmonised and secure digital identity ecosystem.

- **Define common standards for digital reporting formats and input data to ensure technical and semantic interoperability**. Leverage existing frameworks such as the eXtensible Business Reporting Language (XBRL) and Connecting Europe Facility (CEF) building blocks to avoid fragmentation and promote consistency across Member States.

- **Establish a common European open data exchange infrastructure by incentivising the use of standardised digital transaction documents (e.g. eDelivery, eInvoicing, eSignature, as well as European Digital Identity and the European Business Wallet attributes) and principles**. Ensure secure and interoperable data sharing, prevent vendor lock-in, and create a truly open digital ecosystem for B2B and B2G interactions.

Rethink and decrease the role of public sector actors in cybersecurity

In the context of the Single Market, cybersecurity is primarily implemented by organisations that own and operate information and communications technology (ICT) systems and control the data they hold. For enterprises, cybersecurity is fundamentally about protecting private assets. Accordingly, while EU and Member State authorities set requirements, provide guidance and oversee compliance, day-to-day cybersecurity governance ultimately

rests with data and system owners. Operational resilience and cybersecurity are therefore integral to every organisation's risk management.

The EU can best contribute by collecting and analysing cybersecurity-related information to support the prevention and detection of cyber threats, as well as the countermeasures taken by data owners. At the same time, it should be recognised that, while information exchange between Member States is necessary for preventing, investigating and, to some extent, mitigating cybersecurity incidents, the most essential work is carried out by the data and system owners themselves. The EU can provide complementary public services to strengthen the capabilities of these owners. Most importantly, the EU should move beyond a purely compliance-driven approach and focus on reinforcing the Single Market for cybersecurity capabilities.

It is critical to note that enterprises are being compelled to operate in a fundamentally new environment. EU policy must therefore safeguard companies' viability and economic security. While cybersecurity products and services help address confidentiality and integrity risks, supply-chain risk management must also cover availability risks arising from third-country suppliers, as well as dependencies on energy inputs. These external risks should be reduced by enhancing the EU's global competitiveness in the digital transition and by strengthening societal resilience. Regulation should provide clarity and predictability and reduce the cost of entering the Single Market through effective supervision, certification and proportionate management of supply-chain risks.

- **Sharpen ENISA's mandate** and direct its resources towards operational cooperation and the development of European situational awareness for the benefit of Member States and the Single Market. Harness ENISA's capabilities—and the information it gathers through its operational tasks—to strengthen data holders' ability to prevent and detect cyber threats and to support effective countermeasures.

- **Establish an EU mechanism to manage ICT supply-chain security,** as it would enable the identification of non-technical critical risks posed by third countries in relation to ICT components and suppliers. This, in turn, would make it possible to restrict high-risk suppliers from participating in critical infrastructure, public procurement and EU funding programmes.

- **Scale back EU cybersecurity training, skills development and awareness-raising activities** (e.g. the Cyber Skills Academy), as these functions are better led by Member States and delivered by the market. Channel EU funding measures related to cybersecurity expertise through the European Cybersecurity Competence Centre (ECCC), so that resources can be directed towards strengthening Member States' cybersecurity capabilities.

- **Consider converting the NIS2 Directive into a NIS3 Regulation** (including the recently proposed amendments), depending on the success of Cyber Posture Certification under the CSA2 in covering NIS2 requirements and ensuring that authorities cannot impose overlapping additional obligations.

- **Provide EU financial support for the adoption of cybersecurity risk-management measures by data owners in NIS2 sectors**, rather than pursuing direct actions that create inefficiencies and overlap with Member State competences. Scale up existing frameworks for providing financial support to third parties through the European Cybersecurity Competence Centre (ECCC) and its Network of National Coordination Centres (NCCs) to accelerate the uptake of modern cybersecurity solutions.

Inquiries:

- Jussi Mäkinen, Deputy Director, EU and Public Affairs, jussi.makinen@techind.fi, +358 40 900 3066
- Joonas Mikkilä, Senior Advisor, joonas.mikkila@techind.fi, +358 45 129 6791
- Peter Sund, CEO, Finnish Information Security Cluster (FISC) at Technology Industries of Finland, peter.sund@techind.fi, +358 50 565 0621