Technology Industries of Finland

24 April 2025

Recommendations for the Digital Package for Simplification

Technology Industries of Finland welcomes the European Commission's initiative to streamline the EU's digital policy framework through the *Digital Package for Simplification*, including a comprehensive *fitness check* of the existing legislative acquis. As Europe strives to strengthen its digital competitiveness, guaranteeing regulatory coherence, predictability, and efficiency is crucial to fostering innovation, investment, and the uptake of data-driven and AI-enhanced technologies. Our recommendations focus on ensuring that the digital regulatory environment and reporting instruments remain fit for purpose by minimising unnecessary compliance costs and enhancing legal clarity for companies operating in the digital ecosystem.

1 Follow up the digital fitness check with meaningful simplification measures

The fitness check needs to assess the effects of EU data and digitalisation legislation on the competitiveness of European companies, identifying the main regulatory challenges and obstacles in developing and introducing AI-driven and other digital technologies and services in Europe. Accordingly, it is necessary to develop an action plan based on the following approach to streamline and simplify regulations:

Trim unclear, unnecessary and overlapping rules by

1. Withdrawing planned proposals, as was the case with the AI Liability Directive.
2. Refraining from introducing new proposals, such as Directive on the AI in the Workplace initiative.
3. Making targeted amendments to key regulatory instruments where revisions have been identified as necessary (see Annex for specific changes to the AI Act, the Data Act, and the General Data Protection Regulation).

2 Ensure legislation is "born digital" and fit for purpose

Every new piece of EU legislation must be "born digital" — meaning that it has to be developed with a consideration for the use of digital tools, technologies, and processes at its core. By designing laws that are inherently suited for machine-readable formats, automated reporting, and real-time compliance checks from the outset, policymakers can ensure new rules are simpler, faster to implement, and remain flexible as technologies evolve.

- **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.

- **Iterate via continuous "fit for purpose" evaluations by making the fitness check a recurring exercise to keep regulations up to date**. Stress-testing legislation and repealing or revising what is not working should be an ongoing effort. Use feedback from industry and regulators to identify provisions that cause excessive burdens or have become obsolete. Regularly update rules or guidance to reflect technological advances so that the regulatory environment stays agile and relevant.

3 Harmonise enforcement through coordination and support

The effective enforcement of AI and data laws hinges on strong coordination, clear guidance, and well-resourced regulators. A harmonised approach across Member States will create a fair and

predictable regulatory environment, fostering trust and compliance. 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 by bolstering the capabilities and coordination among regulators**. 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, akin to how the European Data Protection Board (EDPB) coordinates the GDPR supervision. The European Data Innovation Board should similarly ensure the uniform enforcement of the Data Act and evolve into a credible counterpart to the EDPB, thereby enabling a better balance between data protection and usage.

- **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.

4 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 releases digital tools clarifying the AI Act, the Data Act, and the EHDS Regulation

Public and private parties in Finland and Denmark have come 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 is partly funded by Technology Industries of Finland. These e-tools are provided by Lean Entries through their Entries platform, in English, and will be free for use by all Finnish industrial sectors and the Danish health tech sector throughout 2025.

5 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 (eDelivery, eID, eInvoicing, eSignature) and principles**. Ensure secure and interoperable data sharing, prevent vendor lock-in, and create a truly open digital ecosystem for B2B and B2G interactions.

ANNEX

AI Act

- Clarify that AI-based safety components or functionalities are not to be considered high-risk when harmonised standards under relevant Union harmonisation legislation are available and applied, in line with the original intent of Art. 6(1) (b).

- Merge section A of Annex I with section B and clarify that sectoral frameworks have flexibility to integrate AI Act rules. The NLF legislation (such as machinery, radio equipment or medical devices) would benefit from the more flexible approach of section B. In practice, AI Act requirements would have to be taken into account when the sectoral legislation was amended.

- Delay the entry into application of high-risk requirements until 12 months after relevant harmonised standards are available, based on past examples (e.g., Medical Device Regulation). Once standards become available, companies need time to assess them and integrate them into their development and governance processes.

- Art. 2(6): Clarify that AI used for R&D of commercial products is out of scope.

- Art. 3: Add a legal definition of open-source software (OSS), ensuring clarity on OSS exceptions.

- Art. 3(9): Specify the definition of 'placing on the market' and recognise that for certain categories of products with long development and certification cycles, market placement should be considered at product-model or -type level, rather than for each individual unit.

- Art. 27: Replace the fundamental rights impact assessment with the GDPR data protection impact assessment.

- Art. 41: Delete Art. 41 on common specifications. Common specifications are usually solely driven by the Commission, without much opportunity for the industry to contribute to their development.

- Art. 49(2): Delete Art. 49(2) on registration of AI systems within scope of Annex III but considered not high-risk, as per Article 6(3).

- Art. 57: Require AI Office to provide timeline for listing sandboxes, increasing transparency for SMEs and other businesses.

- Art. 59: Finetune Art. 59 for private companies to permit the lawful re-use of lawfully held personal data for AI testing (e.g., bias correction, new service concepts, privacy/security technologies) under privacy safeguards, thereby easing innovation and reducing resource burdens—particularly for SMEs.

- Art. 72(3): Delete Art. 72(3) which requires providers to follow a specific post-market monitoring plan, whose framework will be designed by the Commission in an implementing act, giving providers flexibility in developing their own post-market monitoring plan and activities.

- Art. 74(13) and Art 92(3): Delete the possibility for market surveillance authorities to access the source code of an AI system or a GPAI model. Authorities requesting source code access may not have the technical means and sufficient resources to avoid data breaches and have the code accessed by malicious actors.

- Art. 82: Delete Art. 82 on compliant AI systems which present a risk, as compliance with the AI Act should be sufficient for an AI system to be allowed on the market.

- Art. 83: Amend Art. 83 on formal non-compliance so that the restrictions or withdrawal measures would only apply if the provider refuses to comply.

- Art. 91: Add protection for trade secrets, ensuring confidentiality of information obtained from GPAI model providers by the Commission under Art. 78.

- Art. 111: Apply the legacy clause (Art. 111) to all AI already on the market, including GPAI models.

- Art. 111(2): Change 'significant changes' to 'substantial modifications' to ensure alignment with NLF definitions (e.g., Machinery Regulation).

Data Act

- Art. 2(22): Specify the definition of 'placing on the market' recognising that for certain categories of products with long development and certification cycles, market placement should be considered at product-model or -type level, rather than for each individual unit.

- Art. 4: Grant data holders the right to use the data, at a minimum, for purposes including diagnostics, research and development, quality control, and safety.

- Amend Chapter IX of the Data Act to establish a "One-Stop-Shop" at EU level, that is a competent authority that companies can voluntarily opt in to under a 28th regime.

- Art. 15: Limit mandatory data sharing requests to public emergencies only; delete para. (1)(b) to avoid broad, non-essential data requests.

- Chapter V: Set a single reporting point for the data access request framework that is compatible with similar government access request provisions in other legislation, including the revised European Statistics Regulation.

- Arts 37 (10)–(13): Amend to align with the GDPR, thereby reducing administrative overlap and easing the compliance burden for companies.

- Art. 41: Limit model contractual terms / standard contractual clauses only to Data Act provisions to prevent complexity and ensure wider adoption.

- Remove Articles 32 and 28(1)(b) of the Data Act due to overlaps with Chapter V GDPR, as their purpose is unclear and they add unnecessary complexity. Introduce provisions to increase free flow of data with like-minded partners instead.

- Ensure a practical interpretation of GDPR rules on data minimisation, anonymisation, and pseudonymisation to facilitate data processing in an AI and data space context.

GDPR – Towards automatic compliance by design

Strong data protection is an objective that the EU cannot afford to lose during times of geopolitical turmoil. At the same time, we cannot afford to burden companies with overly complicated compliance or slowing down the emergence of innovation due to legal uncertainty.

The current one-size-fits-all model of the GDPR imposes excessive compliance burden on companies, while failing to effectively regulate large platforms which pose the most significant potential privacy risks.

If the GDPR is revised, the focus should be on streamlining it to enable companies to integrate compliance seamlessly into their processes, tools, and services and even automate parts of compliance using standardised approaches.

Key challenges

From the companies' perspective, GDPR-related challenges fall into two main categories:

1. The first and most significant issue is the lack of clarity and legal certainty on how the GDPR interacts with new and existing data-related laws. This complexity is made worse by varying national implementations and interpretations across EU member states.

2. The second category of challenges is related to specific GDPR provisions, particularly strict purpose limitation rules and the restrictive approach to pseudonymisation. These restrictions make it difficult to reuse or share personal data, even in cases where the risk to privacy is minimal.

Proposed scope of the GDPR revision

- **SME exemptions alone do not suffice**: Looking at the challenges presented above, exempting SMEs from some GDPR requirements alone does not meaningfully improve EU competitiveness or strengthen the internal market.

- **Targeted amendments**: We advocate for clarifying some key provisions of the GDPR without altering or destabilising its core structure. Clarifying key GDPR provisions at the article level is crucial, as lengthy and non-binding guidance documents cannot resolve fundamental differences in interpretation.

- **Improve the regulatory interplay**: The different legislative initiatives adopted since the GDPR entered into force (e.g., DGA, DSA, DMA, DA, AIA) should form a coherently interoperable system that helps organisations innovate and scale in the Single Market. The newer regulations heavily rely on the GDPR, but their interplay is far from optimal. The Commission should conduct the GDPR revision in a larger context, considering at least the Data Act and AI Act at the same time. Data processing for AI should follow harmonised rules under both the GDPR and the AI Act to prevent companies from facing overlapping regulatory requirements.

- **Consider ePrivacy while updating the GDPR**: The existing ePrivacy Directive is outdated and the attempt to replace it with an ePrivacy regulation failed. If the GDPR undergoes simplification and revision, electronic communications privacy must be

addressed simultaneously. This approach will lead to a more integrated approach to data protection that enhances user privacy while supporting digital innovation.

- **Keep Procedural Regulation separate**: The GDPR Procedural Regulation is a separate piece of legislation designed to harmonise enforcement procedures for cross-border cases, maintaining the GDPR's core principles intact while addressing procedural shortcomings. Keeping them separate allows for targeted updates to procedural rules without reopening the politically sensitive GDPR text, ensuring flexibility and stability in data protection enforcement.

Suggested improvements

Centrally conducted assessments and adequacy decisions regarding data transfers: To reduce burdens on individual companies, the European Commission could conduct assessments and make more adequacy decisions regarding data transfers with third countries (evaluating third-country legal systems and practices) and data transfers involving significant players (e.g., Microsoft, Amazon, Google). By centralising this process, the Commission can eliminate the redundant efforts organisations currently undertake. The impact assessment related to standard contractual clauses for data transfers is administratively burdensome for companies. This assessment should be partially transferred to the responsibility of the authorities.

A comprehensive framework for applying the GDPR to the training of AI models: The application of the GDPR to AI training and usage should be clarified to ensure that the development of European general-purpose AI models (GPAI models) is not hindered. The current uncertainty around lawful bases for processing, the interpretation of purpose limitation, and the thresholds for anonymisation and pseudonymisation creates legal ambiguity and compliance challenges for developers. It is important to start developing such a framework now, even if the preparation takes a longer time.

Non-personal use of personal data: Cases when the purpose of processing is unrelated to the data subject should be scoped out from the GDPR. This would allow processing as non-personal data if the processor has no means, interest, or intention to engage with the personal data aspect of the dataset and if the dissemination of the data is prevented through technical and organisational measures (e.g., industrial measurement data where the operator has no interest in possible traces of human activity).

Strengthen and clarify legitimate interest and contract: Legitimate interest and contract are the most important and widely used legal bases for companies' data processing. The application and interpretation of these should be straightforward in ordinary, low-risk day-to-day cases. The balance test required to rely on legitimate interest poses significant challenges for SMEs. Conducting a balance test is unnecessary in most clear cases of legitimate interest processing, and this should also be stated explicitly.

Loosening the interpretation of pseudonymisation: It is difficult for companies to know when anonymisation and pseudonymisation are sufficient from the GDPR perspective. If pseudonymised data is transferred to a third party with no identifiers, then the third party should be able to process the pseudonymised data as non-personal data.

Facilitate the development of Codes of Conduct for low-risk use cases: Data will only be fully utilised if the application and interaction of the GDPR, the Data Act, and the AI Act are transferable to operational activities. To fully leverage the Data Act, SMEs must be able to place their trust in third-party digital product companies to process data, including personal data, on

their behalf to facilitate service provision. The industry needs scalable solutions for typical low-risk personal data use cases. Before the GDPR, this was efficiently managed using sector-specific Codes of Conduct, but creating such instruments has become too cumbersome (2–3-year project) under the GDPR Article 40.

The concept of a quasi-controller: The concept of a quasi-controller should be introduced to better reflect the role and responsibilities of platform providers, especially large cloud service providers. A quasi-controller would have responsibilities similar to those of a data controller, recognising that these providers often determine how personal data is processed through the design of their products or services, without leaving meaningful room for the actual controller to give instructions. For example, in services like Microsoft 365, the customer acting as the controller may have little to no ability to influence how the provider delivers the service. A quasi-controller also has its own commercial interest in the data processing, such as using the data to improve or develop services.

Remove the cookie consent article from the ePrivacy directive: Article 5(3) of the ePrivacy directive requires website operators to obtain user consent before storing or accessing information on the user's device through cookies or similar technologies. This should be removed, and the GDPR should be used instead.

Clarify the interplay between the restrictions regarding profiling from the GDPR and AI Act: There is a growing need to align and clarify the relationship between the GDPR's restrictions on profiling (Article 22) related the obligations introduced under the AI Act. As AI systems increasingly power automated decision-making processes across sectors, overlapping and sometimes ambiguous requirements from both regulations create legal uncertainty for developers and deployers of AI.

Establish a mechanism for the Data Protection Authorities to provide official certifications as part of the prior consultation for potential high-risk cases: The prior consultation procedure with the supervisory authorities should lead to official certification confirming that the proposed activity meets data protection standards, when that is the case Authorities would be required to evaluate such consultations and issue certifications where appropriate based on the information provided. This would not restrict DPA's ability to act in other situations, but create a more predictable path for organisations to demonstrate compliance in advance.

Inquiries:

Jussi Mäkinen, Director, EU Regulation, jussi.makinen@techind.fi, +358 40 900 3066
Joonas Mikkilä, Senior Advisor, joonas.mikkila@techind.fi, +358 45 129 6791
Antti Poikola, Data Economy Lead, antti.poikola@techind.fi, +358 44 337 5439