Technology Industries of Finland

30 January 2026

Recommendations on the Digital Omnibus proposals

Technology Industries of Finland (TIF) welcomes the European Commission's intention to simplify EU digital legislation through the Digital Omnibus proposals on AI as well as data and cyber. European digital investments need better regulation. While the proposals contain some useful adjustments, they do not yet amount to the step change in simplification that technology-intensive industries need to innovate, deploy new solutions and scale across Europe.

TIF remains concerned that the cumulative and sometimes overlapping obligations stemming from the AI Act, the Data Act and the GDPR as well as sector specific regulation risk maintaining high compliance costs and legal uncertainty. We also see a clear need to address cybersecurity legislation in a more coordinated and timely manner. In this respect, we acknowledge positive indications on streamlining incident reporting and encourage further work through a dedicated cybersecurity omnibus, including targeted revisions to NIS2 and the Cyber Resilience Act.

Looking ahead, TIF is ready to work pragmatically with the Commission and EU co-legislators to improve the coherence and effectiveness of the EU digital framework. A more proportionate and predictable regulatory environment is essential to reinforce Europe's competitiveness, attract investment, and ensure that digital legislation delivers real-world value. Our detailed recommendations for targeted improvements are set out below.

AI Act

Summary of key recommendations:

- **Fast-track stop-the-clock measures**: Separate and urgently adopt the timeline postponements in a standalone proposal to ensure legal certainty before August 2026.
- **Set firm high-risk AI deadlines**: Fix application dates at December 2027 (Annex III) and August 2028 (Annex I) to ensure predictability for compliance planning. If fixed dates are not maintained, allow acceleration only with advance notice, consultation, and clear criteria.
- **Extend transparency grace periods:** Extend the Article 50 grace period to 12 months and apply it consistently to both providers and deployers, covering obligations under Article 50 (1–4).
- **Integrate high-risk requirements into sectoral frameworks**: Merge Annex I Sections A and B to embed high-risk AI requirements into sectoral legislation, with Annex I acting as *lex specialis* under a maximum-harmonisation AI Act.

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

- **Preserve and expand targeted simplification measures**: Maintain and expand the administrative simplifications and innovation enablers to ensure a proportionate, predictable and competitiveness-friendly AI framework.

Fast-track stop-the-clock measures in a separate proposal

To ensure that the proposed "stop-the-clock" measures can be adopted ahead of the 2026 deadline, the timeline-related amendments should be fast-tracked and separated from the broader AI Omnibus package. In practical terms, a standalone proposal could be limited to points 30 and 31 of the current AI Omnibus draft, together with the related recitals. The remaining elements of the Omnibus could then proceed through the ordinary legislative process, with the agreed timeline adjustment providing the necessary space to conclude discussions on the other provisions in a more considered manner.

Postpone the application of high-risk requirements

The next major milestone under the AI Act is 2 August 2026, when key requirements for high-risk AI systems under Annex III and Annex I and certain transparency obligations are set to apply. Effective implementation of these rules depends critically on the availability of harmonised standards, which translate legal requirements into practical, usable guidance for providers and deployers.

At present, the timelines for developing these standards are slipping well beyond what was originally envisaged, with several expected only after the requirements formally enter into force. This creates a risk of significant legal uncertainty and implementation bottlenecks, particularly for SMEs and startups with limited compliance resources. Against this background, the targeted postponements proposed in the AI Omnibus are justified and necessary to ensure realistic implementation timelines and to avoid undermining AI deployment and competitiveness in Europe.

The AI Omnibus introduces a two-step enforcement delay for high-risk AI systems, with default extensions of the compliance deadlines (16 months for Annex III systems, 12 months for Annex I systems) and the possibility for the Commission to accelerate their application (6 months for Annex III, 12 months for Annex I) once it considers sufficient compliance support measures to be in place.

Replace moving targets with fixed high-risk timelines

While the delay itself is necessary and welcome, this dual-trigger mechanism is complex and risks creating a moving target for compliance, undermining the predictability that both industry and public authorities need for planning, budgeting, and implementation. To ensure legal certainty, the Omnibus should establish firm application dates for high-risk systems—December 2027 for Annex III and August 2028 for Annex I—rather than leaving the timeline dependent on future administrative decisions.

If fixed dates are not maintained in the final text, the Omnibus should instead tightly define and constrain the Commission's ability to trigger earlier application: the Commission should be required to provide advance notice, consult stakeholders (including industry and the co-

legislators), and apply clear, objective criteria for what constitutes "adequate measures in support of compliance", explicitly linked to the availability of harmonised standards and key guidance documents. This would help ensure that any decision to shorten timelines is transparent, evidence-based, and workable in practice.

Extend the transparency grace periods

The AI Omnibus introduces a 6-month enforcement delay for certain transparency obligations, notably for AI providers required under Article 50(2) to mark AI-generated outputs for legacy generative AI systems placed on the market before 2 August 2026. This adjustment is justified, as the relevant code of practice and guidelines are expected only shortly before the rules apply.

However, no corresponding grace period is foreseen for AI deployers, even though their obligation to disclose AI-generated content depends on the availability of such marking and guidance. For consistency and legal certainty, the grace period should also cover deployer obligations under Article 50(4) and be extended to 12 months, allowing sufficient time to analyse and implement the code of practice.

In addition, the grace period should also cover the transparency obligations under Article 50(1) and (3), which are expected to be clarified only through guidelines in mid-2026. A minimum 12-month grace period should apply to both providers and deployers to allow for meaningful implementation.

Integrate high-risk requirements into sectoral frameworks

Early implementation work highlights growing misalignment between the AI Act's horizontal requirements and existing sectoral legislation, in particular for products covered by Annex I, Section A. Delays in developing harmonised AI standards and uncertainty over their interaction with sector-specific product obligations risk disrupting established conformity assessment pathways and overburdening notified bodies.

While the AI Omnibus introduces procedural improvements for notified bodies, these do not resolve the structural issue of applying high-risk AI requirements in parallel to sectoral rules. This concern is further underscored by the fact that the Medical Devices Regulation (MDR) has recently been proposed to be moved from Section A to Section B, highlighting the need to revisit the structure of Annex I in a comprehensive manner.

To ensure coherent implementation, Annex I should be streamlined by merging Sections A and B and extending the more flexible Section B approach to all Annex I products. This would allow high-risk AI requirements to be integrated into sectoral regulatory frameworks, rather than applied separately, while enabling harmonised AI standards to be translated into sector-specific contexts without undermining existing conformity procedures. The Omnibus should also clarify that Annex I legislation acts as *lex specialis* and confirm the AI Act as a maximum harmonisation instrument, to prevent fragmentation and ensure legal certainty across sectors.

Preserve and expand targeted simplification measures

Many elements of the AI Omnibus proposal move in a positive direction, particularly those aimed at reducing unnecessary administrative burdens and supporting innovation. Notable examples include removing the registration requirement for non-high-risk AI systems, extending SME relief measures to small mid-cap companies, replacing mandatory post-market monitoring templates with guidance, introducing a legal basis for real-world testing under Annex I, Section B, and making AI literacy obligations voluntary for companies. A new legal basis for data processing to mitigate bias in AI systems and the centralisation of oversight for certain GPAI-model-based systems and enabling the creation of EU-level regulatory sandboxes at EU level also improve coherence. These changes should be preserved and, where possible, expanded to ensure the AI framework remains proportionate, predictable and supportive of innovation.

Data Act

Summary of key recommendations:

- **Give manufacturers the right to reuse data**: Recognise manufacturers' right to use and share data generated by connected products they have placed on the market at least for core operational, safety and innovation purposes to encourage the use of readily available data in European industries and to drive demand for new data-driven offerings.

- **Clarify "placing on the market" for legacy products**: Specify that for certain products with long development and certification cycles, market placement should be considered at product-model or -type level, rather than for each individual unit.

Consolidate and streamline Europe's data rules framework

The proposal to bring together key elements of Europe's data legislation within the Data Act represents a constructive step towards greater coherence and legal clarity, even if its direct impact on reducing company-level compliance burdens is likely to be limited. Integrating the Open Data Directive, the Data Governance Act and the Free Flow of Non-Personal Data Regulation under a single framework simplifies the overall architecture and offers public authorities a clearer basis for handling data access and reuse.

The Omnibus also makes a welcome improvement in the business-to-government data sharing obligation by replacing the open-ended notion of "exceptional need" with a more narrowly defined "public emergency" threshold. This refinement strengthens legal certainty and helps ensure that data requests remain proportionate and predictable, while preserving the ability of authorities to act where genuinely necessary.

Give manufacturers the right to reuse data

We propose amending Article 4(13) and (14) of the Data Act to clearly recognise manufacturers' right to use and share data generated by connected products they have placed on the market, even in the absence of a contract, at least for core operational and

innovation purposes such as diagnostics, research and development, quality assurance and control, and safety. Such use would be without prejudice to the manufacturers' obligations under the GDPR. Establishing an explicit legal basis in Article 4 would support innovation and product development across the EU, while ensuring that such use fully respects users' rights and complies with applicable EU and national rules on data protection, trade secrets and intellectual property.

Clarify "placing on the market" for legacy product types

We ask adjusting Article 2(22) of the Data Act to clarify the definition of "placing on the market" by recognising that, for products with long development, certification and delivery cycles, market placement should be assessed at the level of the product type or model rather than for each individual unit. This clarification should be set out in a substantive provision, ensuring legal certainty for legacy product types that continue to be placed on the market over extended periods.

GDPR

Summary of key recommendations:

- **Clarify the definition of personal data:** Streamline, on the basis of the CJEU case law, the treatment of properly pseudonymised data as anonymous where there is no access to additional data enabling re-identification.

- **Simplify rules to support AI model development:** Simplifications are welcome, but they may be best delivered in a more technology-neutral manner.

Clarify the definition of personal data

We support the Commission's proposal to amend the definition of personal data in order to codify the relevant CJEU case law. This should provide the missing link to the Data Act and bring welcome simplification, especially for the processing of industrial data. As a rule, most datasets contain small elements of personal data that are not relevant for the further use of data, for example in analytics. This may be the most significant proposal for industrial data in the overall package. However, as the rule is now disconnected from the context of the case, the clarity of the provision will need special care to create a predictable and future-proof basis for businesses.

We support the proposed new Article 41a of the GDPR, which would provide a legal basis for the Commission to adopt implementing acts on pseudonymisation. Development of systematic and more unified approach—simultaneously strengthening risk-based approach—on privacy-enhancing technologies would be highly beneficial for the European data economy.

Example:

> *A complex machine with thousands of sensors and data points generates an extensive dataset on its operation. An operator changes certain settings, causing the*

dataset to include personal data. For the value of the dataset, the link to a specific person is irrelevant; only the changes made matter. The proposed change would clarify the further use of this dataset, provided that any personal data is properly pseudonymised in the original dataset, for example by using a non-identifying string of numbers instead of personal identifiers.

Simplify rules to facilitate AI model development

We support the Commission's proposals to the GDPR to encourage and facilitate AI model development in Europe. However, it may be wise to keep the framework as technology-agnostic as possible and to provide the necessary flexibility by relying on legitimate interests in a technology-neutral manner. The resulting framework should enhance uniform application and predictability.

We do not consider it well founded to suggest that data may be retained in the AI system, as stated in Recital 33.

Cyber

Summary of key recommendations:

- **Establish a truly single-entry point**: Extend its scope to all relevant regimes, including the AI Act, and rely on the CRA reporting platform already being developed by ENISA rather than creating parallel systems.

- **Mandate one harmonised incident-reporting template and harmonised timelines**: Require a single core template, with limited sector-specific additions, so that one notification can satisfy reporting obligations across the GDPR, NIS2, DORA, CER, CRA and related frameworks.

- **Streamline ENISA's statutory tasks:** Reduce ENISA's existing statutory tasks (currently at least 140) as part of the simultaneous revision of the Cybersecurity Act (CSA).

On cyber, the Omnibus mainly addresses how incidents are reported, not what must be reported or when. By contrast, there is a proposal to further complicate reporting by changing the GDPR reporting timelines and, consequently, further de-harmonising reporting deadlines. Timelines should be maximally harmonised to simplify the collection, analysis and synthesis of data for reporting.

Assigning ENISA to develop a single-entry point for notifications under the GDPR, NIS2, DORA, eIDAS and CER is a welcome step, but it remains limited in scope and ambition. The current layering of reporting timelines—built *de facto* on the GDPR's 72-hour rule and supplemented by multiple early warnings and follow-ups under other acts—risks entrenching a fragmented model that diverts resources from incident response to compliance.

Greater simplification would require a genuinely single entry point covering all relevant regimes (including the AI Act and the CRA platform), and a harmonised incident-reporting template.

In exchange for adopting a wholly new operational area (including governance of the reporting platform), ENISA's existing statutory tasks (at least 140) should be reduced as part of the simultaneous revision of the Cybersecurity Act (CSA).

--

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