

## Nordic key recommendations for further improvements to the AI Omnibus and the Digital Omnibus

The Nordic Business Federations welcome the European Commission's Digital Omnibus proposals as important steps towards more coherent, effective, and innovation-friendly digital regulation in Europe. Still, the legislative package does not sufficiently address the need for further simplification, harmonisation, and a meaningful reduction in administrative burdens. Businesses need predictability and legal certainty, avoiding regulatory vacuums or overlaps, as well as clearer, coordinated interplay between digital rules.

The omnibus proposals must not stand alone but should be the first in a series of reforms. We are pleased to see the Commissions commitment to further simplification initiatives via the Digital Fitness Check. Future EU digital regulation must deliver clearer, simpler, more proportional and predictable rules with early clarification of overlaps and better cross-sectoral guidance.

Here follows a set of recommendations from Danish Industry ([DI](#)), Confederation of Finnish Industries ([EK](#)) and Confederation of Swedish Enterprise ([SN](#)) to the co-legislators taking stock of the Commission Digital Omnibus proposals from November 19, 2025.

### Digital Omnibus on AI

*Secure timely adoption before August 2026:* The AI Omnibus must decrease legal uncertainty, not increase it. It is therefore imperative that the omnibus should be adopted before current high-risk AI requirements enter into force. We urge all parties to carefully balance their wish for improvements with the urgent nature of the process.

*Delay obligations for high-risk AI systems:* We strongly support postponing the effective date for high-risk AI requirements under Annex I & III until harmonised standards and practical guidance are available.

*Maintain the transfer of Article 4 AI Literacy from companies to the Member States and the Commission.* The provision is largely declaratory and creates uncertainty for businesses about what level of staff training is sufficient and how compliance should be demonstrated, especially when employees are not engaged in AI-critical roles.

*Improve risk assessment and limit registration and documentation requirements, articles 5 & 6.* Unclear delimitation of high-risk AI creates great uncertainty. Regulation must be based on risks, not technology or entire areas. The removal of registration requirements for non-high-risk in Annex III is positive but should also include documentation requirements as it does not contribute to higher protection or effective supervision.

*Facilitate innovation by real-world testing, Article 2(8), (60) and (60a).* The opportunity is essential for innovation, risk management and adaptation and should therefore cover all AI systems, not only those tested in regulatory sandbox by amendment to Article 2(8).

- *Clarify the interplay between the AI Act and other EU legislation:* The relationship between the AI Act, GDPR, and sector-specific legislation must be clarified, particularly regarding high-risk classifications and AI-based safety components. To ensure coherent implementation, Parts A and B of Annex I should be merged and the more flexible approach of Part B extended to all covered products. High-risk AI requirements should be integrated into sectoral frameworks rather than applied as a separate regime, allowing standards to align with existing compliance systems.

## **Digital Omnibus (Data, Privacy, ePrivacy and Cybersecurity)**

### **EU General Data Protection Regulation (GDPR)**

The GDPR represents a severe hindrance to innovation and technology by setting absolute limitations for the use of data and restricting the use of data for the purposes of developing new products and technology, such as AI models. It also puts an enormous administrative and cost burden in the form of documentation and technical infrastructure cost - affecting the general competitiveness of businesses. *We strongly support all proposed amendments to the GDPR* to accelerate development of AI and reduce administrative burden.

*Further simplification of the documentation requirements,* a real risk-based approach to reduce unnecessary paperwork and limit administrative burdens related to the data subject's rights by making them clear, limited and proportionate.

*Article 4 (definition of personal data):* Alignment with recent CJEU case law (SRB decision) on sufficient levels of pseudonymisation.

*Enable AI-use:* Legitimate interest shall be sufficient for processing personal data in the AI-lifecycle, while special categories of personal data shall be processable for purposes such as bias detection.

*Reduce and harmonise reporting and documentation requirements:* We support the Commission's proposal for common methods and templates for DPIA's and standardization of reporting, as well as the need for clearer guidance and less bureaucracy. Companies face cumulative and overlapping obligations (e.g. DPIAs, breach notifications, pseudonymisation/anonymisation rules).

### **ePrivacy and GDPR**

*Integrate relevant parts of ePrivacy Directive Article 5(3) into the GDPR* - provided the framework is genuinely technology-neutral and risk-based, focusing on processing purposes and real risks rather than specific tools such as cookies.

*Consent should be reserved for high-risk and highly sensitive processing;* broad, undifferentiated consent requirements dilute meaningful choice and exacerbate "cookie fatigue".

*We welcome Article 88a(3)* as a pragmatic step that enables consent-free audience measurement for a provider's own services and improves legal certainty. However, the rigid consent-management constraints

in Article 88a(4), including limitations on re-requesting consent, risk imposing unnecessary technical and operational burdens and should be reconsidered.

*We oppose Article 88b*, which would mandate centralised, automated, machine-readable consent signals, as it risks market concentration, reduced competition, and weakened European digital sovereignty by shifting practical control to a few dominant intermediaries.

*Refrain from introducing further structural mechanisms like Article 88b* until after the real-world impact of Article 88a on consent volumes and user experience has been evaluated.

The Digital Omnibus on data and cyber should proceed swiftly with the targeted adjustments outlined above, delivering immediate simplification and legal clarity. For the remaining elements of the ePrivacy Directive not addressed by this Omnibus, we recommend a holistic review and evidence-based assessment under the Digital Fitness Check, to ensure a coherent, future-proof framework and avoid fragmented regulatory changes.

### **Data Act and streamlining regulation on data mobility**

*Stronger protection for trade secrets*: Data sharing must never compromise the protection of trade secrets or intellectual property. This is an important issue and strongly supported by Nordic businesses given concerns about EU based companies' data being used, for example, to develop competing products in third countries.

*Avoid overlaps on data transfers*: Remove all provisions on international data transfers (personal, mixed, non-personal) in the Data Act and DGA and refer instead to the existing rules in the GDPR to remove complexity and unnecessary compliance work.

*Clarify obligations for "mixed datasets" and exclude certain legacy devices from data sharing*: This will relieve companies of unduly burdensome or technically impractical obligations without compromising the aim of the Data Act.

### **Cybersecurity**

*Harmonise incident reporting*: Nordic businesses support a single entry point across EU legislation and Member States, as proposed by the European Commission. To achieve real burden reduction, this must be accompanied by common templates, definitions, and deadlines across NIS2, GDPR, DORA, CER, and CRA.

*Integrate national platforms with the EU solution*: For those EU countries that already have an existing national system for reporting, like Denmark has virk.dk, it should be interoperable with the EU platform to ensure "report once only", minimising duplication and confusion.

### **About us:**

DI represents 20.000 companies with 650.000 employees, EK represents 15.000 companies (96% SMEs) with 900.000 employees and SN represents 60.000 companies (98% SMEs) with 2.000.000 employees