B9+ recommendations for further improvements to the AI Omnibus and the Digital Omnibus

The B9+ Business Federations[1] welcome the European Commission's Digital and AI Omnibus initiatives as an important first step towards regulatory simplification and improved legal certainty. The proposals rightly recognise Europe's competitiveness challenge, marked by excessive paperwork, overlapping obligations and complex rules.

Our vision is a Europe that can access and safeguard the economic benefits of digital transformation, which requires a strong and effective internal market, openness to international cooperation and trade, and a clear focus on competitiveness and resilience. This means creating strong business conditions and building digital capacities across Europe, enabling companies to connect, innovate and trade.

The Omnibus Package is a necessary and promising start for a continuous simplification effort that promotes competitiveness, removes unnecessary administrative requirements, and streamlines AI, data and cybersecurity rules to support compliance and growth. However, EU policy makers must now deliver on this promise.

We welcome the Commission's commitment to further simplification through the Digital Fitness Check, which will be essential to identify inconsistencies, overlaps, and unintended burdens across EU digital legislation. The interplay between any proposed new laws and existing rules must work with, not against, innovation and the goal of EU competitiveness.

Digital Omnibus

The Data Act should ensure genuine protection of trade secrets and security, including explicit coverage of cybersecurity risks arising from data sharing while ensuring uptake of the use of data. An effective dispute settlement mechanism should be available

[1] The D9+ is a Ministerial forum of likeminded and digitally progressive EU Member States. The B9+ Group is a grass-roots coalition of the main national business confederations of 12 D9+ Member States: CEOE (Spain), VBO-FEB (Belgium), SPCR (Czech Republic), DI (Denmark), EE (Estonia), EK (Finland), Ibec (Ireland), FEDIL (Luxembourg), VNO-NCW (Netherlands), LEWIATAN (Poland), CIP (Portugal) and Confederation of Swedish Enterprise (Sweden).

where refusals are considered unjustified, while voluntary data sharing should be facilitated through clearer and more proportionate rules.

Avoid overlaps on **international data transfers**: Provisions on international transfers in the Data Act and DGA should be removed and aligned with existing GDPR rules to reduce complexity. Clarify obligations for mixed datasets and legacy devices to avoid disproportionate or technically impractical requirements. Clarify that the risk-based approach (Art. 24 & Art.32) applies to measures for data transfers to third countries (Chapter V). Create a positive presumption for recognising intra-company transfers during general business when company has self-certified to appropriate safeguards.

The GDPR must be applied in a genuinely risk-based and proportionate manner, focusing on realistic high risks rather than routine low-risk processing. We strongly support the necessary clarification that low-risk processing of personal data requires a less intensive approach than high-risk processing of personal data. This principle of proportionality is made more explicit in the Digital Omnibus proposal regarding the right of access, information requirements and data breach notifications. This is essential to enable access to data for AI and European innovation, including the use of pseudonymised and other low-risk data for innovation and training. We strongly support alignment of Article 4 (definition of personal data) with CJEU case law on sufficient levels of pseudonymisation, and clarification that **legitimate interest** can serve as a legal basis throughout the AI lifecycle, including for security-related processing notwithstanding the other principles and obligations of the GDPR, such as data minimalization, purpose limitation etc.

We strongly support the clarification of the definition of **scientific research**. The proposal explicitly confirms that scientific research includes research and technology development (innovation) in academic, industry and other settings such as SMEs. This is the interpretation of scientific research as was initially foreseen by the legislators. The clarification does not alter the requirements for scientific research: research needs to be of high quality and meet the conditions of scientific research, such as methodological and systematic approach.

Unnecessary administrative burdens should be reduced, while data subject rights must remain effectively protected and workable in practice. Legal certainty should be strengthened, including through clearer reliance on legitimate interest for innovation and security purposes, and international data transfers should be simplified through greater EU-level responsibility, a risk-based approach and clearer guidance.

Relevant **parts of the ePrivacy** framework, including Article 5(3), should be integrated into the GDPR, provided the approach 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 aligned with the differentiated approach of the GDPR. Broad, undifferentiated consent

requirements dilute meaningful choice and increase “consent fatigue”. A whitelist for low risk essential activities e.g., security monitoring, software updates, anti-fraud and first party analytics (Digital Omnibus, Art. 88a), this is specifically necessary where there is a relationship of authority (such as the employer-employee and government-citizen relationship). Proposed Art 88b introduces economic uncertainty and a new mandatory consent signal on top of existing GDPR rules and should be removed. The proposed browser-level consent mechanism adds complexity without delivering simplification, undermines established publisher-user relationships, and disproportionately harms European SMEs and independent publishers. It risks pushing smaller players behind paywalls, concentrating market power, and restricting low-risk activities such as contextual advertising, fraud prevention, and frequency capping. Co-legislators should instead focus on exempting low-risk activities from consent requirements in line with a risk-based approach.

Other interactions may include between Data Act, DMA, AI Act, DSA and GDPR. Our ask is to identify inconsistencies and overlaps in the Digital rulebook and to ensure these are removed.

Cybersecurity

Deliver a European harmonized secure interoperable technical infrastructure to connect national established Single-Entry Points (SEPs) for reporting that facilitates entities in scope of multiple legal incident reporting obligations to submit one report to be compliant with all applicable rules. See example of Luxembourg and Denmark. We support the setting up of one integrated reporting portal per Member State, covering all statutory reporting obligations, coupled with full EU interoperability through uniform technical and functional standards; and automated and secure transmission where cross-border notifications are required. Companies in all sectors should be allowed to leverage their country of main establishment as the primary interface (single entry point) for cybersecurity incident reporting under relevant EU legislation, provided that this is combined with common templates, definitions and deadlines, and with automated, secure transmission to competent authorities in affected Member States where cross-border notifications are required. ENISA’s role should be supportive and focus on standardisation, interoperability and quality assurance.

Digital Omnibus on AI

High-risk AI obligations should apply **only after relevant harmonised standards, guidelines and key implementation tools are available**, and with sufficient time for adaptation. Also provide sufficient time to ensure that notified bodies[2] can be formally notified on time to perform the required third party conformity assessments.[3] A firm and

[2] With regard to annex I high risk AI systems
[3] Such notification process takes around a year.

realistic application date would be 2 August 2028 to support compliance and avoid fragmented implementation. Similarly, any grace periods on transparency requirements should be realistic and aligned with the delivery of forthcoming Codes of Practice and apply to both providers and deployers.

Regulatory obligations for high-risk AI should be **proportionate and risk-based**, focusing on real risks rather than technology or entire application areas. Unclear delimitation of high-risk AI creates uncertainty and discourages adoption. Reduce administrative requirements for high-risk AI that do not proportionately increase the protection of consumers or society. **Remove or reduce the requirement to register non-high-risk AI systems**[4]. Most systems will not qualify as high risk in practice. This requirement is an administrative burden that impacts innovation/adoption and offers little in terms of risk management or transparency.

Risk assessments and documentation obligations under Articles 5 and 6 should be streamlined. Requirements that do not contribute to effective supervision or risk management should be removed, in line with the objective of reducing administrative burden.

The relationship between the AI Act, the GDPR and sector-specific legislation must be clarified, in particular for high-risk classifications and AI-based safety components. To ensure coherent implementation. High-risk AI requirements should be **integrated into existing sectoral frameworks e.g., Med-Tech**, rather than applied as a parallel regime, allowing standards to align with established compliance systems.

Concluding message

The Digital Omnibus must deliver immediate simplification and legal clarity while laying the foundation for a continuous, evidence-based simplification agenda through the Digital Fitness Check. Only by reducing unnecessary burdens, removing overlaps and ensuring a coherent, risk-based digital rulebook can Europe strengthen its competitiveness, resilience and technological capacity.

***

[4] Article 49 of the EU AI Act requires providers to register AI systems in an EU database, regardless of whether they are ultimately classified as high-risk.