ERT

EXPERT PAPER

ERT Position on the EU's Digital Omnibus Package

TECH, AI & DATA

MARCH 2026

Executive Summary

- A unified regulatory environment is key to boosting Europe's competitiveness, innovation, and digital infrastructure. The Digital Omnibus proposals offer a timely opportunity to simplify EU digital legislation by reducing fragmentation and ensuring greater consistency across the framework. ERT supports the Commission's *intention*, especially efforts to lower administrative burdens and create a more predictable, innovation-friendly regulatory environment.
- However, the current scope of the Omnibus remains limited and does not yet fully address several persistent challenges that continue to undermine Europe's digital competitiveness and the ability of its technology sector to innovate and scale. In particular, existing inconsistencies and disproportionate obligations across the Data Act, AI Act, and Cyber Resilience Act (CRA) risk creating legal uncertainty and placing European companies at a disadvantage compared to global competitors.
- To ensure the Omnibus delivers meaningful simplification, it should close remaining gaps and resolve contradictions between horizontal digital legislation and sector-specific frameworks across Member States. The Omnibus should provide clear guidance on definitions, reporting processes, and compliance pathways to reduce uncertainty for businesses and national authorities alike.
- Regulatory requirements should be risk-based, proportionate, and responsive to the pace of technological change, and designed to support rather than impede innovation and growth. Provisions that risk undermining the global competitiveness of Europe's technology leaders or creating excessive regulatory burdens should be withdrawn or substantially revised. The expansion of EU-level regulatory sandboxes and real-world testing mechanisms will be critical to accelerating innovation and lowering barriers to market entry for European companies.
- ERT calls on the co-legislators to use the Digital Omnibus as an opportunity to build a more coherent, proportionate, and globally competitive digital regulatory environment. This will enable the EU to unlock the full potential of European companies to shape the future of digital technologies, strengthen the Single Market, and advance Europe's digital sovereignty.

Introduction

A streamlined and harmonised digital regulatory environment is essential to strengthen Europe's global competitiveness, support innovation, and enable the development of high-quality digital infrastructure. The current regulatory landscape – shaped by the AI Act, Data Act, ePrivacy Directive, GDPR, Cyber Resilience Act (CRA), NIS2, DORA and various sectoral frameworks – remains complex, fragmented and difficult to implement consistently across the Single Market.

The Digital Omnibus presents a unique opportunity to address these challenges. By reducing fragmentation and improving coherence across the EU's digital rulebook, the Omnibus can create a more predictable and innovation-friendly environment while ensuring that regulatory burdens remain proportionate to the pace of technological development. The Digital Omnibus must reflect long-standing industry calls for simplification, alignment of definitions and reporting processes, and more coherent implementation pathways.

Several shortcomings in the proposal risk introducing new uncertainties or leaving existing inconsistencies unaddressed. In their current form, the Data Act, AI Act and CRA include provisions that negatively affect the global competitiveness of Europe's technology leaders and risk constraining the ability of European companies to innovate and scale. Many Member States have already signalled strong support for swift action and targeted regulatory relief for their local industries.

The Commission must now drive the Digital Omnibus negotiations in close partnership with Member States and the European Parliament to ensure that all critical shortcomings are addressed and that harmful provisions are withdrawn. By refining the proposal during the legislative process, the EU can unlock the full potential of European companies to contribute to Europe's digital and cloud infrastructure and advance the Union's broader competitiveness and digital sovereignty objectives.

In the following pages, ERT outlines its positioning on the key elements of the Digital Omnibus proposals – focusing on Artificial Intelligence, Data, and Cybersecurity – and sets out concrete recommendations to ensure a coherent, innovation-friendly and globally competitive digital framework for Europe.

Artificial Intelligence

The Digital Omnibus on AI Regulation Proposal[1] introduces amendments to the AI Act aimed at facilitating implementation, reducing administrative burdens, and enhancing legal certainty. This includes the provision of additional time for compliance, encouraging the use of innovation-friendly instruments, mitigating certain structural inconsistencies within the broader regulatory landscape, as well as the expansion of real-world testing mechanisms and the establishment of EU-level regulatory sandboxes, which are expected to accelerate innovation and lower barriers to market entry. ERT welcomes this direction.

However, several gaps and risks remain which will need to be addressed to ensure that the Omnibus delivers a more pragmatic and proportionate implementation of the AI Act:

- While the proposed delay of key high-risk AI obligations is a constructive step intended to allow for the development of harmonised standards and to give both businesses and regulators additional time to adapt, ERT considers that further ambition is required to ensure effective implementation.
- Progress on standardisation remains slower than anticipated and continues to show limited alignment with international standards (ISO, IEC, NIST), which could

1 https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

have implications for global competitiveness if not addressed in a timely manner. This poses a significant risk to global competitiveness.

- The interplay between the AI Act and other horizontal and sector-specific frameworks, including GDPR, the Data Act, CRA, DSA, DMA, and existing sectoral legislation remains complex, particularly for systems already subject to established safety regimes. In its current form, the proposal may not yet deliver the level of legislative coherence needed to facilitate compliance and meaningfully reduce administrative burdens.

Building on these considerations, ERT presents the following recommendations:

- **Introduce a 24-month postponement of the application of the remaining provisions of the AI Act to conduct a comprehensive review.** This period should pave the way for a revised European AI framework that strikes an appropriate balance between trust, innovation, and investment, ultimately supporting a competitive and resilient digital economy in Europe.
- **Ensure that harmonised standards for high-risk AI systems are adopted at least 12 months before the provisions are implemented.** The current proposal, which provides only a 6-month transition period for Annex III systems, would not offer sufficient preparation time for businesses. Implementation should therefore be delayed until one year after standards are in place, in line with earlier Commission considerations and calls from a broad range of stakeholders.
- **Promote consensus-based standardisation processes** that incorporate best practices in AI design, development, testing, deployment and cybersecurity.
- **Ensure that European harmonised standards are aligned with internationally recognised frameworks (ISO, IEC, NIST)** to avoid regulatory fragmentation and duplicative compliance obligations.
- **Create a central EU repository of GPAI models deemed compliant with the AI Act.** This would avoid the need for duplicative assessments by companies and authorities across individual Member States.
- **Provide clear and timely guidance on key concepts, including the definition of "safety components"**, the treatment of open-source models, and the criteria for classifying systems as high-risk.
- **Ensure a streamlined interaction between the AI Act and existing legislation**, particularly for AI systems already subject to sector-specific safety and security frameworks and listed in Annex I A (e.g. medical devices, machinery).
- **Clarify the interaction between the AI Act, the GDPR, and the ePrivacy Directive (Article 6)**, notably regarding transparency, fairness, profiling, and the processing of personal data for bias monitoring and risk mitigation.
- **Work closely with regulators to ensure that regulatory sandboxes are accessible**, well-coordinated across authorities, and adequately resourced to support innovative AI development.

Data

The Digital Omnibus Regulation[2] proposal seeks to merge and amend several existing instruments in order to establish a more cohesive and simplified framework for data access, sharing, protection, and reuse. ERT welcomes the effort to consolidate the Data Act, Data Governance Act and Open Data Directive into a more coherent and integrated EU data framework. The proposal has the potential to enhance predictability and streamline compliance obligations. By clarifying regulatory expectations and timelines, it could help reduce unnecessary administrative uncertainty for businesses.

2 https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

However, significant gaps remain that risk undermining operational certainty for businesses:

- The Omnibus does not address concerns regarding mandatory B2B data-sharing obligations. It does not consider the impact on flexibility models, where the Data Act requires access to real-time data by customers and third parties, affecting local market operations and coordination with system operators. In addition, cybersecurity risks arising from the opening of APIs for critical grid data are not sufficiently addressed.
- Key concepts relevant to the energy sector remain insufficiently defined under the Data Act, including 'connected device' or 'related service'. It remains unclear whether assets such as smart meters, SCADA systems, smart chargers, or grid sensors fall within scope, or whether grid flexibility management qualifies as a related service.
- The proposal does not clearly establish the interaction, interoperability, and legal hierarchy between the consolidated data framework and sector-specific legislation. Nor does it clarify liability allocation in cases where shared data is used by third parties and leads to incidents or damages.
- There is no assessment of the economic impact on electricity distribution operators, including costs related to technological adaptation (APIs, data portals), enhanced cybersecurity requirements, and interoperability obligations. Regulatory incentives to offset these investments, such as tariff-based compensation mechanisms, should be considered.
- Contract renegotiation obligations remain disproportionate and impractical, particularly in complex industrial and long-term contractual relationships. When it comes to mandatory data sharing, a contractual obligation imposing on data holders the renegotiation of existing complex contracts represents considerable administrative burden, disproportionate costs and introduces legal ambiguity.
- Trade-secret protections under the Data Act remain insufficient to safeguard high-value industrial data. While the "trade secrets handbrake" exists, data holders may still be compelled to disclose sensitive information once security arrangements are agreed – at which point any misuse or leakage may already have caused irreparable harm. Obtaining protection or judicial compensation for trade secrets once they have been unlawfully disclosed is practically impossible. This fundamentally erodes the principles of fair competition by mandating disclosure of essential competitive elements, including trade secrets, through legally imposed sharing obligations.
- Under EU law (Trade Secrets Directive), trade secrets are protected and derive their commercial value, because they are secret. The general obligation to disclose trade secrets under the Data Act fundamentally undermines this right.
- While the Omnibus proposal introduces the possibility to deny disclosure on cybersecurity grounds, it still requires exceptional circumstances and the demonstration of a high risk exposure, which is effectively unachievable.
- Further, the case-by-case notification to authorities remains burdensome.
- Although the partial integration of certain ePrivacy elements (e.g. cookie provisions) into the GDPR is noted, the Omnibus does not resolve long-standing issues related to ePrivacy metadata rules, which continue to impose unnecessary compliance burdens.
- Further clarification is needed on the interplay between the Data Act and the GDPR to ensure legal coherence and reduce compliance uncertainty.
- "Data processing service" is very loosely defined, leading (1) to legal risks due to interpretation, (2) to extensive technical and contractual measures if interpreted

broadly even for digital services not intended to be covered, and (3) to compliance violations and economic risks if interpreted narrowly. In the worst case, the entire SaaS portfolio might be impacted, even though not intended to be covered by the Data Act.

Building on these considerations, ERT presents the following recommendations:

- **Extend the Data Act's transition period from 12 to 36 months**, followed by a gradual application of additional requirements (design for direct access, switching, contracts) to reflect the scale of technical and organisational changes required for compliance.
- **Make B2B data sharing voluntary by default, based on industry-developed codes of conduct recognised by the Commission.** In industrial B2B markets, contractual balance already exists, allowing parties to negotiate data rights on an equal footing (e.g. through tenders). Additional mandatory rules risk undermining contractual freedom, legal certainty, and investment incentives.
- **In the absence of a voluntary framework:**
  - **Strengthen trade secret protections to ensure that sensitive industrial information and proprietary know-how are not exposed**, which is essential for maintaining European competitiveness. This includes avoiding the disclosure of confidential supplier information through data-sharing rules, as large-scale data sharing may unintentionally reveal sensitive supplier processes or designs.
  - **Treat trade secrets and cybersecurity risks as fully recognised grounds for refusing access to data without mandatory notification, since they are clearly defined under EU law.** Where users believe a refusal is unjustified, they should be able to contest it before independent dispute-settlement bodies or, ultimately, before the courts.
  - **Remove or significantly reduce contract-renegotiation obligations on data holders under the Data Act's data sharing rules**, which generate disproportionate administrative costs and legal uncertainty.
  - **Clarify the "products" and "related services" in scope**, including practical examples distinguishing them from data processing services. Limit the scope of the Data Act to connected products and explicitly listing excluded devices to enhance legal certainty.
  - **Clarify definitions, including raw versus derived data, and improve legal certainty for data processing services.** ERT proposes:
    i. Raw data: the first, unprocessed data captured from a single sensor in its native form.
    ii. Derived data: data that has undergone processing, transformation, aggregation, or analysis, including data generated through additional investment such as algorithms, analytics, or domain expertise.
    iii. Limit mandatory data sharing to raw data only, together with the minimum adaptations required to ensure usability and readability. Processed, inferred, or value-added data should be excluded to protect trade secrets and intellectual property.
- **Exclude SaaS & PaaS services from Chapter VI and clarify that switching provisions for data processing services not unintentionally capture B2B solutions** (e.g. ERP systems embedded in enterprise environments), as doing so would create revenue uncertainty, impair cost recovery, and discourage innovation.
- **Extend the exemption for custom-made services from switching rules under Chapter VI to all such contracts, regardless of their signing date, to ensure**

consistency and fairness. Additionally, remove differential treatment between SMEs and larger companies to avoid legal uncertainty and unjustified regulatory disparities.

- **Clarify that Chapter VI does not apply where contracts are provided by the customer** (e.g. public tenders) or are individually negotiated.
- **Strengthen interoperability and cross-sector data availability through Common European Data Spaces**, building on successful industry-driven initiatives such as Manufacturing-X and Catena-X.
- **Simplify notification procedures**, as current requirements could lead to excessive daily notifications, creating unnecessary administrative burdens for both companies and authorities.
- **Address unresolved ePrivacy issues:** many provisions of the ePrivacy Directive have been incorporated into the Digital Omnibus, with several others included in the DNA proposal. Only a small number of articles remain unresolved. The outstanding provisions – most notably the outdated Article 6 – should be repealed, with the principle of the confidentiality of communications into existing and/or future EU law.
- **Clarify the interaction between the Data Act and the GDPR**, particularly where the Data Act may restrict data uses that would otherwise be lawful under GDPR provisions.

GDPR:

- **Make the Record of Processing Activities (RoPA) optional for low-risk processing and mandatory only for high-risk activities (e.g. Privacy Impact Assessment criteria).** This reduces undue administrative burden on organisations and aligns documentation efforts with actual risk exposure, focusing compliance where it matters most.
- **Limit data processing agreements (Art. 28) to critical operational details**, such as security, transfers, and sub-processors. This approach shortens negotiation cycles, and accelerates deployment of new technologies and replaces "contractual complexity" with contractual agility, ensuring compliance while removing unnecessary administrative barriers.
- **Harmonise international data transfers assessment by replacing** Transfer Impact Assessments (TIAs) with a set of pre-approved, country-specific supplementary measures. Responsibility for compliance should shift to the service provider in the importing country, who is best positioned to implement supplementary measures. This change restores predictability, reduces costly subjective assessments and strengthens the competitiveness of EU businesses by streamlining access to global services.
- **Strengthen protections against "excessive" Data Subject Access Requests (DSARs)**, particularly in HR and pre-litigation contexts. The definition of "excessive" should include harassment and "fishing expeditions" used for legal leverage, balancing individual's right with the controller's need to prevent procedural abuse and ensuring DSARs are not misused for litigation pressure.
- **Maintain the proposal's approach** of incorporating the CJEU's recent case law on personal data and pseudonymisation. This brings the much-needed clarity and harmonisation for data-driven research and innovation.

Cybersecurity

The Digital Omnibus Regulation[3] proposal introduces adjustments to the EU's cybersecurity framework, with the objective of simplifying compliance, reducing fragmentation, and improving coherence across the Cyber Resilience Act, NIS2 and DORA regimes. The subsequent Cybersecurity Package, released in January 2026, includes further initiatives towards standardisation and simplification.

ERT supports the establishment of a single-entry point for incident reporting at Member State level, enabling one-time submission of information that is automatically disseminated to all relevant authorities. This could be achieved by building on the single-entry platform envisaged under the Cyber Resilience Act, whereby national CSIRTs simultaneously notify the EU-level reporting mechanism.

For cross-border incidents or those affecting multiple entities within a corporate group, legal clarity is essential. The entity responsible for incident reporting should be clearly and consistently defined across all relevant legislation, following the approach already set out in NIS2. Where multiple entities within a group are concerned, reporting should be carried out by a single designated entity located in the most relevant jurisdiction – namely, the Member State where the group has its main establishment in the Union.

Despite this progress, several important challenges remain:

- Simplification measures under the CRA remain insufficient. The regulation continues to impose disproportionate burdens, particularly in light of the requirement to develop more than 40 harmonised standards within unrealistic timelines, the need to designate Notified Bodies, and the lack of clarity on core concepts such as "placing software on the market" and the treatment of remote data-processing solutions.
- The interaction between reporting mechanisms under NIS2, DORA, GDPR, CRA and other relevant frameworks remains unclear, including how the single-entry point for incident reporting will relate to the single reporting platform to be established under Article 16 CRA for notifications of actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements.
- Reporting obligations under the CRA come into effect on 11 September 2026, meaning the single reporting platform (Art. 16 CRA) must be operational by that date. If the single-entry point is only available 18 months after the regulation enters into force, this could create uncertainty for companies and authorities.
- It is currently unclear whether actively exploited vulnerabilities under the CRA are to be reported via the single reporting platform (Art. 16 CRA) or the single-entry point, which may affect legal clarity and operational planning.
- The Omnibus does not address requests for sector-based exemptions under the CRA, including for products already regulated under frameworks such as the Machinery Regulation or other sectoral legislation that demonstrably meet equivalent cybersecurity objectives.
- Retroactive obligations under Articles 69(2) and 69(3) of the CRA remain unchanged, despite the significant technical and operational challenges of developing patches or fulfilling reporting obligations for legacy products no longer in active support.
- Overlaps between the CRA, Machinery Regulation, NIS2, Radio Equipment Directive, and DORA – covering definitions, thresholds, reporting timelines, and conformity assessment requirements – continue to create substantial

3 https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

administrative burden and risk divergent national implementation.

- Delays in the development of timely, consensus-based, and internationally aligned harmonised standards risk undermining legal certainty and the effective implementation of the entire cybersecurity framework.

Building on these considerations, ERT proposes the following recommendations:

- **Ensure that harmonised standards are available at least 18 months before the application** of any New Legislative Framework legislation, including the CRA, and postpone the CRA's application accordingly. A minimum of 18 months should elapse between the citation of CRA standards in the Official Journal and the end of the CRA transition period.
- **Promote the use of recognised European and international standards**, including ISO/IEC 2700X, ISA/IEC 62443, and the NIST Cybersecurity Framework, to support predictable compliance and international alignment.
- **Accelerate the citation of CRA harmonised standards** to consolidate the Single Market, reduce fragmentation, and enhance legal certainty.
- **Introduce risk-based and sector-based exemptions** under the CRA for products already subject to robust cybersecurity or safety requirements under other EU legislation (e.g. Machinery Regulation, Radio Equipment Directive).
- **Remove Articles 69(2) and 69(3)** to eliminate disproportionate retroactive obligations and ensure that the CRA applies only to products placed on the market after its full entry into force.
- **Exclude from the CRA major infrastructure projects, such as rail or grid systems, that started before the CRA entered into force** but will only be placed on the market after the end of the transition period. Moreover, extensions to existing major infrastructure projects, such as rail or grid systems, should be feasible without the need of a complete replacement or upgrade of the current infrastructure. To maintain security and operational continuity, the CRA should recognise compensating security measures (as described in standards such as EN IEC 62443) as compliant alternatives. Manufacturers should be allowed to reference such measures to demonstrate equivalent protection.
- **Introduce mutual recognition of audits and conformity assessments across Member States.** Compliance with CRA requirements should also demonstrate compliance with parallel cybersecurity obligations under sectoral legislation, and NIS2 audits conducted in one Member State should be recognised across national transpositions.
- **Streamline and harmonise reporting and registration obligations across CRA, NIS2, GDPR, eIDAS, CER and DORA** through:
  - Common definitions, thresholds, and reporting timelines
  - A single national reporting authority
  - A standardised European reporting template
- **Provide practical guidance on reporting obligations** applicable from 11 September 2026, along with the required ENISA reporting tool, at least **6 months** in advance to ensure sufficient time for companies and authorities to prepare.
- **Provide clear, sector-specific guidance on key concepts such as "substantial modification"**, ensuring that risk assessments reflect the diversity of operational contexts across industries.
- **Simplify and harmonise NIS2 transposition**, including consistent designation of critical and important entities, avoidance of national gold-plating, centralised registration for multinational companies, harmonised reporting processes, and

mutual recognition of security audits. Cloud services already covered by NIS2 should be excluded from, or subject to tailored treatment under, the CRA to avoid duplicative obligations.

Digital Infrastructure

Europe's AI leadership, digital transformation as well as overall economic resilience and competitiveness depend on efficient network deployment, reliable compute capacity, and the strategic development of data centres. To boost these critical enablers, Europe requires a modern, investment-friendly and coherent regulatory framework for digital infrastructure. The Digital Omnibus represents a welcome first step by addressing selected procedural inefficiencies and administrative burdens. However, the Omnibus is only one element of a much broader reform agenda.

The deployment of reliable, ultra-fast 5G and fibre infrastructure continues to be constrained by regulatory barriers and a persistent investment gap estimated at over €200 billion. For decades, Europe's digital and telecommunications sectors have operated under an increasingly outdated and fragmented regulatory framework – most notably the European Electronic Communications Code (EECC), which has been transposed unevenly across all 27 Member States and interpreted inconsistently by national regulators. Rather than addressing these structural shortcomings, successive EU initiatives have added layers of new digital legislation, often accompanied by duplicative reporting requirements and inconsistent enforcement. The result is a fragmented regulatory landscape that does not reflect market realities, discourages long-term investment, and slows the deployment of critical connectivity and compute infrastructure.

The Digital Networks Act should become the true Omnibus for the telecom sector: a comprehensive framework capable of addressing market fragmentation, with enhanced simplification of existing rules, reducing administrative complexity, and creating the scale and investment conditions required for Europe to remain globally competitive. While the DNA proposal includes positive provisions to support investment in the mobile sector with substantial changes proposed on the spectrum allocation rules, other key aspects of the draft need to be improved to deliver a truly simplified and modernised regulatory framework. In a geopolitical context characterised by strategic dependencies and intensifying global competition, Europe cannot afford another incremental or narrowly scoped legislation. The Digital Networks Act must be sufficiently ambitious to reflect market realities and lay the foundations for Europe's digital sovereignty and competitiveness.

Europe also lacks a coherent framework for data-centre development aligned with AI and cloud requirements. It is critical that the forthcoming Cloud and AI Development Act (CAIDA) addresses the need for a much stronger and more explicit linkage between infrastructure regulation and the EU's broader digital sovereignty objectives.

To support Europe's digital competitiveness and unlock the full potential of AI, cloud, and connectivity, several key regulatory improvements are needed:

- **Reinforce the role of industry in shaping Europe's cloud, compute, and connectivity ecosystem by ensuring that regulatory frameworks support private-sector contributions to infrastructure resilience, scalability, and innovation.** Industrial players developing strategic data and compute hubs require clear, predictable, and technology-neutral rules to support investment at scale.
- **Ensure coherence across digital, energy, and industrial policy frameworks to enable high-performance, low-carbon infrastructure.** Insufficient infrastructure remains a structural barrier to competitiveness in sectors such as mobility, energy, and Industry 4.0.
- **Advance high-performance connectivity through the Digital Networks Act,**

which should modernise outdated market regulations, simplify remaining rules while supporting the EC proposal on reforming spectrum rules with unlimited licenses duration, or at least 40 years duration with automatic renewal process to enable sustained private investment. Those rules should apply once the DNA is approved.

- **Streamline permitting and administrative procedures** to accelerate the deployment of digital networks and related infrastructure.
- **Recognise data centres as strategic infrastructure and align regulatory measures with the AI Continent Action Plan, the Apply AI Strategy, the forthcoming Strategic Roadmap for digitalisation and AI in the energy sector, and CAIDA.** Data centres are essential to digital sovereignty, AI deployment, and industrial competitiveness. Their development should be supported by a harmonised, forward-looking EU framework that enables reliable and efficient operations, powered by a diversified, low-carbon, and technologically neutral energy mix.
- **Ensure energy frameworks enable data centre development, guaranteeing reliability, affordability, and speed of deployment.** To meet growing cloud and compute demand, permitting and regulatory processes should prioritise timely access to adequate energy supply – through grid connections or complementary solutions – while preserving flexibility across technological pathways.
- **Accelerate the deployment and modernisation of electricity grids**, which form the backbone of digitalisation, data centre expansion, electric mobility, and industrial transformation. The rapid growth of data centres and AI is fundamentally reshaping energy demand, requiring integrated planning across energy, digital, and industrial policy. Europe must at least double annual investment in electricity grids by 2040 – from approximately €36 billion today – and maintain elevated investment levels thereafter. This should be accompanied by incentives for digital grid upgrades, harmonised standards, and the development of energy data spaces.

Conclusion

The Digital Omnibus provides an important foundation for reducing fragmentation and strengthening the European digital environment. With ambitious improvements, the EU can ensure the Omnibus delivers meaningful simplification, reduces regulatory burden, and enhances Europe's competitiveness. ERT stands ready to work with the Commission, Parliament, and Member States to ensure the Digital Omnibus achieves its full potential and supports Europe's technological leadership.

To maximise its impact, the Omnibus should prioritise: harmonised and internationally aligned standards for AI, data, and cybersecurity; streamlined and mutually recognised reporting and audit frameworks; and pragmatic risk-based approaches that reduce administrative duplication while preserving robust safeguards. The EU should also ensure regulatory clarity for high-value industrial data, promote trade-secret protections, and provide guidance on the interaction between sectoral legislation and horizontal frameworks, including GDPR, CRA, NIS2, and DORA.

Moreover, the Omnibus must complement broader initiatives to modernise Europe's digital and energy infrastructure. Strategic investment in ultra-fast connectivity, data centres, and electricity grids is essential to support AI, cloud, and industrial transformation, while regulatory frameworks should facilitate private-sector contributions, minimise fragmentation, and enable cross-sectoral coherence. By embedding these elements, the Omnibus can create a predictable, innovation-friendly environment that strengthens Europe's digital sovereignty, unlocks industrial and technological potential, and positions Europe as a global leader in the digital economy.

This expert paper has been produced by the working group of the ERT Committee on Tech, AI & Data.

For more information, contact hanno.woelm@ert.eu

ERT

The European Round Table for Industry (ERT) is a forum that brings together around 60 Chief Executives and Chairmen of major multinational companies of European parentage, covering a wide range of industrial and technological sectors. ERT strives for a strong, open and competitive Europe as a driver for inclusive growth and sustainable prosperity. Companies of ERT Members are situated throughout Europe, with combined revenues exceeding €3 trillion, providing around 5 million direct jobs worldwide - of which half are in Europe - and sustaining millions of indirect jobs. They invest more than €100 billion annually in R&D, largely in Europe.

Boulevard Brand Whitlocklaan 165
1200 Brussels, Belgium

+32 2 534 31 00

contact@ert.eu