UNIFE statement on the Digital Omnibus

July 2025

Rail transport has always been a frontier of technological progress, with the European Rail Supply Industry leading the way. In the past years, the pace of change in the rail sector has moved up a gear with digital innovation, from signalling (European Rail Traffic Management System (ERTMS)), Automatic Train Operation (ATO) to the integration of Artificial Intelligence. Digital transformations shall profoundly improve the performance and overall attractiveness of the sector, thereby helping to achieve the ambitious objectives of the European Commission's *Sustainable and Smart Mobility Strategy*, but also of the carbon neutrality objective fixed by 2050 as per the EU Climate Law.

What is at stake?

While fully committed to EU policy objectives in the digitalisation field, in particular when it comes to the critical topic of cybersecurity, UNIFE underlines that **certain regulations focus on consumer goods sectors and not on the characteristics of tailor-made industrial goods sectors such as rail which is characterised as follows:**

1) Long project timelines (design and production phase) – up to 7-years from signing a contract through to design, certification and type authorisation of a railway vehicle type, followed by typically 7-10 years of production and delivery of vehicles in conformity to the type.
2) The long lifespan of rail products and assets in operation – more than 30 years for rolling stock such as trains, metros and tramways.
3) Business is governed mostly by public procurement contracts and Business-to-Business (B2B) and not through Business-to-Consumer (B2C).
4) Very complex goods involving dozens of suppliers across the entire value chain, and interconnected and sophisticated subsystems.

Our main asks

UNIFE welcomes the announcement from Executive Vice-President Virkkunen of her simplification package for digital regulation, the so-called "Digital Omnibus" with initiatives to simplify EU regulation to allow European companies to remain competitive. The Digital Omnibus will be essentially based upon the Draghi report The future of European competitiveness, which suggests that the European Commission should streamline and harmonise digital regulations to foster a more conducive environment for tech companies to scale up.

UNIFE calls on the European Commission to use the opportunity of the Digital Omnibus to:

- **Revise the Cyber-Resilience Act (CRA), the Data Act and the Artificial Intelligence Act (AI Act)**, in order to streamline and simplify these pieces of legislation.

- **Protect existing projects** by exempting contracts signed before 11 December 2024 for the CRA (i.e. entry into force) and before 12 September 2025 for the Data Act (i.e. entry into force). Due to the complexity, long duration, and multi-tiered structure of railway projects, the introduction of the new rules during the contract execution (at manufacturing or validation stage) severely impacts project costs, on time delivery and the continued operation and delivery capability of this critical sector. It will also increase the diversity of legal frameworks to be applied to a single fleet, resulting in additional complexity.

- **Ensure that the Data Act and the AI Act clearly distinguish between B2B and B2C** because the level of required protection, the need for details and standards and the coverage of already existing legal framework is different. A horizontal and "one-size-fits-all" regulatory approach can harm European rail suppliers, including hundreds of SMEs, because of the specificities highlighted.

- **Propose to pause the application of the Data Act and the Artificial Intelligence Act by 24 months**. Indeed, the necessary standards for the timely implementation are already in delay and far from finalised, and an extended transition period will benefit the entire ecosystem by providing companies and national authorities with the necessary time to prepare and adapt to the new regulations.

What are the risks of not acting?

- **Significant increase in project costs and delays**

Without adjustments to timelines and scope, the application of these digital regulations to ongoing rail projects will significantly drive up costs, cause delays due to the possible consequences on vehicle authorisation, and jeopardise compliance with existing contracts and funding conditions. This would have a negative impact for the entire rail sector, including the railway operating community.

- **Reduced innovation and technological leadership**

If companies are not granted sufficient time to adapt to new digital requirements, they will be forced to shift resources away from R&D to compliance tasks. This risks slowing down innovation, weakening Europe's technological leadership, and delaying deployment of green and smart mobility solutions.

- **Weakened global competitiveness**

Due to the complex value chains, a rushed implementation will disproportionately burden rail suppliers and in particularly SMEs, straining financial and human resources. This could result in reduced competition in tenders and commitments to fewer projects due to the high level of risks and costs, which would destabilise the European rail ecosystem. This will in turn put EU manufacturers at a competitive disadvantage in terms of greater compliance costs. Foreign competitors not subject to similar rules may undercut European firms in global markets, undermining the EU's strategic autonomy in a critical and strategic sector.

ANNEX

Cyber-Resilience Act (CRA)

With the recent and predicted rapid increase of digitalisation throughout every sector of the economy and daily life, low security in digital products, such as consumer-facing IoT devices, risks leaving large sections of digital infrastructure exposed to the rising threat of cyberattacks.

The Cyber Resilience Act tackles cybersecurity from its foundation by requiring all the building blocks of this digitalised infrastructure – the products themselves – to fulfil essential cybersecurity requirements and be capable of receiving security updates, to ultimately strengthen the cyber resilience of the EU as a whole.

While UNIFE fully supports the objectives of the Cyber Resilience Act, the Regulation as currently formulated lacks references to the procedures and legal framework of the rail sector, leaving it ambiguous in its application. In the absence of legal certainty and mitigating measures to accommodate the sector's time constraints, the CRA may , cause counterproductive effects to its stated goals. In fact, implementation paralysis due to uncertainty and the mandatory modification of already approved projects risks disrupting the delivery of critical projects and unintentionally impairing the mobility of citizens, goods and military throughout the EU for several years.

UNIFE calls on the European Commission to:

1. **Clarify that obligations of the Cyber-Resilience Act apply only to projects whose contracts have been signed after its entry into force (11th of December 2024). Legacy contracts, due to their complexity, long duration, and multi-tiered structure, should be excluded from retroactive application.**
   In several industries, projects of large scale and complexity take years to develop with contracts already locked into place well in advance, and appropriate procedures are adopted for the introduction of new requirements. Within the rail sector, for instance, the Interoperability Directive and the Technical Specifications for Interoperability (TSIs) integrate mechanisms to avoid disrupting projects in an advanced stage of development. Imposing new obligations retroactively would lead to serious disruptions, increased costs, delays in delivery and possible non-compliance with existing contractual frameworks, impairing mobility and ultimately slowing down the rollout of digital and green innovations in the sector.

2. **Ensure that extensions to existing major infrastructure systems, such as rail or grid systems, are exempted from the scope of the CRA.**
   Extensions to such systems should be feasible without the need of a complete replacement or upgrade of the current infrastructure as this would incur disproportionate compliance costs for system owners and operators. Provisions to avoid such disruptions are already present in other EU legislation. For instance, article 7(1)(c) of the Interoperability Directive allows derogations from the application of a TSI when its application compromises economic viability or compatibility. The CRA already foresees the inapplicability of certain requirements where these are incompatible with the nature of a product with digital elements. However, the legal basis provided by CRA Article 13(4) & Recital 55) is too brief and in need of clarification regarding its derogations. Thus, a clear exemption under Article 2 (scope) would be preferable.

3. **Clarify that vulnerability disclosure requirements only mandate disclosure to the customer/user.**
   Annex I, Part II, (4) requires to "publicly" disclose information on fixed vulnerabilities. In the railway domain there are high risks associated with the publication of information regarding security vulnerabilities. It should thus be clarified that targeted information to the customer/ user specifically is sufficient in duly justified cases like critical infrastructure sectors etc.

4. **Clarify the definitions of "placing on the market" for rail products.**
   It needs to be safeguarded that the CRA and TSI definitions are understood similarly regarding the term "placing on the market". It could be understood that this occurs after receiving an authorisation to be placed on the market whilst according to the CRA this takes place when it is supplied for

distribution, consumption, or use. This discrepancy in understanding might impact the identification of the starting point for support obligations and is causing uncertainty in the railway sector. A clarification of definitions applying to rail products could further ensure a correct and smooth implementation of the CRA.

Data Act

Data is at the centre of the ongoing digital transformation of many economic sectors, including rail., generating billions of data points annually. Indeed, many rail assets, including signalling, ticketing and trains, among others, already incorporate digital capabilities which produce every day a significant amount of digital information. The effective regulation of the collection, management, and processing of these data is crucial. Public procurement is also a fundamental aspect for rail suppliers as their customers are often public authorities that might request access to data.

UNIFE believes that, to fully harness the benefits of data-focused solutions, it is indeed essential to remove barriers to information-sharing between operators (mainline and urban), infrastructure managers and suppliers.

While the general objectives of the Data Act, namely to improve access to and use of industrial data in the EU, are commendable, the Regulation as currently formulated raises significant concerns for the European rail supply industry. It risks imposing disproportionate burdens on complex, long-lifecycle industrial B2B systems, and could unintentionally undermine Europe's strategic autonomy and innovation potential in our sector.

UNIFE calls on the European Commission to:

1. **Pause the application of the Data Act of 24 months to allow for the completion of necessary standards, provide legal certainty, and enable meaningful preparation across the value chain.**
   The Data Act introduces requirements that remain poorly defined in many aspects and depend on technical standards still under development A two-year pause of the Act's application would give the industry and national authorities the necessary time to establish implementation guidelines, avoid legal uncertainty, and properly integrate the Act into existing procurement and engineering processes.

2. **Clarify that obligations of the Data Act apply only to projects whose contracts have been signed after the Regulation's current application date of 12 September 2025 (+24 months). Ongoing contracts, due to their complexity, long duration, and multi-tiered structure, should be excluded from retroactive application.**
   Due to their scale and complexity, rail projects often take years to develop, with contracts already locked into place well in advance. Imposing new obligations retroactively would lead to serious disruptions, increased costs, and possible non-compliance with existing contractual frameworks, ultimately slowing down the rollout of digital and green innovations in the sector.

3. **Exclude B2B contracts from the scope of the Data Act in complex industrial sectors such as rail.**
   The Data Act is designed to address imbalances typical in B2C markets, where end users have little negotiating power. In contrast, B2B relationships in sectors like rail are governed by complex contractual arrangements, often established through public tenders or negotiated between parties with comparable bargaining power. Imposing one-size-fits-all obligations risks duplicating or conflicting with existing contracts, adding legal uncertainty and undermining effective data cooperation. We therefore call for the explicit exclusion of B2B contracts from the scope of the Data Act in order to preserve legal certainty and avoid undermining established industrial practices for data sharing and cooperation.

4. **Ensure cost recovery for data generation. Data production in rail requires expensive hardware, sensors, and long-term maintenance, regulation must allow suppliers to develop sustainable data business models with fair commercial conditions.**
   In B2B markets such as rail, data generation is not incidental, it requires deliberate investment in additional infrastructure, software, sensors, and integration capacity. If the Data Act mandates broad, no-cost data access without appropriate safeguards, it will undermine the business case for generating and maintaining high-quality data in the first place. This discourages innovation while risking to shift costs unfairly onto suppliers, including many SMEs. In that context, several clarifications in the text are needed:
   1. The principle laid out by recital 17 that regular repair and maintenance is not part of "related services" must be made explicit,

2. The definition of “data processing services” must clarify that it targets only data processing power, i.e. storage capacity and not any service using a scalable processing resources.

5. **Introduce clear exemptions for sensitive business data and trade secrets and simplify the burden of justifying those exemptions to avoid disproportionate legal and administrative overhead.**
   Although the Act includes exceptions for sensitive data, the procedures for invoking them remain unclear and may be burdensome. Suppliers could face high administrative and legal costs simply to protect their intellectual property, with unclear outcomes. Simplifying these provisions and streamlining the documentation burden would help strike a better balance between openness and competitiveness.

6. **Limit data access obligations towards third parties under Article 5 to entities located in the EU.**
   It must be ensured that obligations of data-holders vis-a-vis third parties (Art. 5) are only binding when both the user and any involved third party are located within the European Union. As currently drafted, the provision poses a significant risk of critical data being shared with entities outside the EU, particularly in strategic sectors such as rail. This could undermine Europe’s industrial competitiveness by forcing the disclosure of valuable product data to third-country competitors, potentially weakening the EU’s industrial base.

Artificial Intelligence Act (AI Act)

UNIFE supports the goals of the Artificial Intelligence Act and shares its commitment to safe, transparent, and rights-respecting AI. As providers of complex, safety-critical systems, the rail supply industry is dedicated to aligning AI solutions with these principles. However, we urge that the regulatory framework be adapted to the realities of industrial B2B sectors like rail, where AI is embedded in long-lifecycle products, developed in mature safety environments, and governed by extensive sector-specific regulations.

In this context, UNIFE demands targeted adjustments and clarifications to ensure that the implementation of the AI Act is proportionate, technically feasible, and aligned with the sector's innovation potential and competitiveness.

UNIFE calls on the European Commission to:

1. **Pause the application of the AI Act by 24 months to allow time for the development of harmonised standards, clarity in guidance, and national preparedness.**
   The AI Act is a far-reaching requiring significant adaptation from manufacturers, authorities, and conformity bodies. Yet, key implementation tools, including harmonised European standards (hENs) for high-risk AI systems and codes of practice for general-purpose AI (GPAI), are still in development and delayed. Essential work to develop these standards is underway within the Joint Technical Committee | CEN-CENELEC JTC 21. As this work is still in progress, additional time is required to allow for its completion and for the subsequent integration of the resulting standards into industrial practices. Postponing enforcement will allow stakeholders to rely on clear, applicable criteria and prevent unnecessary disruption to innovation and deployment.

2. **Refine the definition of AI to ensure the scope only includes systems with actual cognitive or autonomous capabilities, not basic automation or rule-based systems.**
   The AI Act's current definition of AI is overly broad, capturing traditional software like rule-based control systems that lack autonomy or learning capacity. In sectors like rail, this could impose high-risk requirements on long-used, safely regulated systems. To avoid legal uncertainty and regulatory overload, the definition of AI should be narrowed to target those systems with genuine autonomy, adaptability, or decision-making in line with the Act's risk-based approach.

3. **Ensure consistent and adequate treatment of rail systems (including Urban Rail) through sector-specific legislation rather than through the AI Act.**
   Under Article 2(2) of the AI Act, high-risk AI systems integrated into products or systems governed by EU sector-specific legislation, such as the Technical Specifications for Interoperability (TSIs) in the rail sector, are subject to tailored conformity assessment procedures that take into account existing safety and compliance mechanisms. While Main Line rail benefits from this alignment, Urban Rail, despite sharing similar safety-critical features and procurement structures, is currently not covered by the TSIs and therefore not considered under this tailored approach. To ensure consistency, the AI Act should apply a harmonised approach to Main Line and Urban Rail.

4. **Exemption for Legacy and Embedded AI Systems.**
   To avoid retroactive compliance burdens on systems that are already proven safe and would otherwise require costly and unnecessary reassessment, a grandfathering clause for AI systems embedded in rail products already certified under existing EU rail safety legislation before the AI Act's application date should be enacted.

5. **Clarify obligations for fine-tuning General Purpose AI (GPAI).**
   GPAI is increasingly used in various contexts, including product development. A common practice involves fine-tuning an existing GPAI model, typically provided by a large developer, using domain-specific data to perform a narrower, specialised function (e.g., for use in the rail sector).. However, the AI Act currently lacks clarity on the regulatory obligations in such cases.. It should be clarified that narrowing or targeting the functions of an existing GPAI model, regardless of whether systemic risks are present in the original model, must not trigger the full set of obligations applicable to GPAI models, unless the fine-tuning demonstrably results in the development of a general-purpose AI model with systemic risk as defined in Article 52(1). This applies both to the provider of the fine-tuned GPAI model and to the AI system provider deploying the model in a specific application.

6. **Establish a clear distinction between B2B and B2C applications, and clarify the notion of "high-risk" in industrial contexts.**
   The AI Act should explicitly distinguish between business-to-business (B2B) and business-to-consumer (B2C) applications, acknowledging that most AI systems used in the rail sector are industrial, technical, and non-user-facing. Typical use cases, such as predictive maintenance, energy optimisation, traffic management, or automated train operation, are B2B applications that operate under stringent engineering controls and sector-specific safety legislation. Applying the same regulatory requirements to industrial B2B systems as to consumer-facing AI creates unnecessary complexity and risks stifling innovation in sectors like rail, where safety is already embedded through well-established engineering practices, legislation, and contractual frameworks. In this context, the definition of "high-risk" AI should be refined to reflect the actual risk posed to fundamental rights and safety, rather than relying solely on technical complexity or deployment context. We propose a differentiated classification of AI systems used in the rail sector:
   1. Internal Corporate AI Systems – Tools used within company operations (e.g. HR analytics, internal forecasting, document automation) that are not safety-critical and do not interact with rail infrastructure or passengers. Their minimal risk profile should justify proportionate regulatory oversight.
   2. Production and Engineering AI Systems – Systems used in design, simulation, testing, and validation phases. These do not operate in live environments and are governed by internal quality processes. Their outputs are subject to further verification before any potential safety-critical application.
   3. AI Systems in Revenue Service – AI deployed in rail vehicles or infrastructure operating in live environments (e.g. predictive maintenance, ATO). These systems already undergo rigorous assessment and certification under EU rail safety law and should be the main focus of high-risk regulation. Any new AI requirements must align with existing sectoral frameworks to avoid duplication and ensure legal clarity.

7. **Prioritisation of sector-specific harmonisation**
   The European Commission must mandate standardisation organisations to develop sector-specific harmonized standards for AI in rail, in collaboration with other agencies like ERA (European Union Agency for Railways). This will ensure that conformity assessments and technical documentation align with existing safety and certification frameworks (e.g. CSM-RA, Railway Safety Directive), avoiding duplication and regulatory friction.

UNIFE - The European Rail Supply Industry Association

Avenue Louise 221
B-1050 Brussels, Belgium
Tel: +32 2 626 12 60
general@unife.org

@UNIFE

UNIFE - The European Rail Supply Industry Association

unife.org

unife
THE EUROPEAN RAIL INDUSTRY ®