Position Paper

Brussels, October 2026

Strengthening the Cloud and AI Development Act: a rail perspective

CER aisbl – **COMMUNITY OF EUROPEAN RAILWAY AND INFRASTRUCTURE COMPANIES**
Avenue des Arts 53 – 1000 Bruxelles | T: +32 (0)2 213 08 70 | F: +32 (0)2 512 52 31 | E: contact@cer.be | www.cer.be

Submitted by: CER – Community of European Railway and Infrastructure Companies
Consultation: Feedback on the draft AI Continent – new cloud and AI development act

1. About CER

CER represents railway undertakings and infrastructure managers across Europe. In relation to the Cloud and AI Development Act, our members are above all users: they buy cloud services and deploy AI to run safety-critical public services, from traffic management and maintenance to passenger information and, increasingly, automated train operation.
Rail is one of Europe's most heavily safety-regulated sectors, governed by the Interoperability Directive (EU) 2016/797, the Safety Directive (EU) 2016/798, the Common Safety Method for risk evaluation and assessment (CSM-RA), the Technical Specifications for Interoperability (TSIs), and authorization by the European Union Agency for Railways (ERA). Rail companies also manage cyber risks under the NIS2 Directive and, where designated as critical entities, resilience risks under the Critical Entities Resilience Directive. Rail is also European by design: infrastructure managers and train operators share systems and data across borders every day.
Our overriding interest in the Act is therefore twofold. We want its support for AI to reach applied and safety-critical uses, so that AI can move from pilots into everyday rail operations. And we want its cloud rules to build on the framework that already governs rail: one coherent set of obligations, integrated into existing safety, interoperability and cybersecurity processes, not duplicated alongside them.

2. Summary

CER supports the Cloud and AI Development Act and its aim of making Europe more competitive and resilient through its own cloud and AI capacity. This paper proposes ways to make the Act more effective, drawing on the experience of a sector that is safety-regulated, works across borders and is central to the EU's climate and resilience goals. Rail is a demanding test case: what makes AI work in rail will help most of Europe's "physical AI", from automated vehicles to industrial robots. Our proposals fall under four headings:

1. moving AI from pilots into everyday use: linking testing to approval, investing in methods that prove AI is safe and secure, and enabling data pooling, long-life edge computing and access to computing power;
2. a trusted cloud framework that works across borders;
3. continued access to state-of-the-art AI;
4. a good fit with the rules that already govern rail, including cybersecurity.

3. Moving AI from pilots into everyday use

The Act invests heavily in computing capacity and in frontier AI. Its support for applying AI in real operations, especially where safety is at stake, is less developed. Six changes would close that gap.

3.1. Turn successful tests into approved systems

The Act supports datasets and real-world testing for physical AI (Article 4(4)) and testing facilities for industrial AI (Annex I, grand challenge 5). What it lacks is a route from a

successful test to an approved system. For safety-critical AI, testing only pays off if the authorities that approve systems can use the results. We propose that testing programmes be designed together with these authorities - for rail, the European Union Agency for Railways and the national safety authorities - linked to the regulatory sandboxes of the AI Act, and that their evidence be reusable in approval procedures.

3.2. Invest in methods that prove AI is safe and secure

The Act funds what AI can do, but not how to show that it is safe. Only for AI agents does it support testing methods (Article 4(6)(b)). Not all useful AI can be classified under the Agent umbrella. In many cases useful AI models are much simpler and focused on a specific task. For any AI that moves a vehicle, a robot or a train, the hardest step is not building the model but proving that it behaves safely in every situation it may meet and that it cannot be manipulated. We propose a dedicated line of research and innovation on verification, validation, runtime monitoring, security testing and safety evidence for physical AI, under grand challenge 4, including protection against manipulated training data and misleading inputs. This would give substance to Europe's commitment to trustworthy AI and would benefit automated vehicles, drones and industrial robots as much as automated train operation.

3.3. Let companies pool data without giving it away

Rail AI often needs data held by several parties: the infrastructure manager knows the track, the train operator the service, the manufacturer the condition of the train. The Act supports secure data pooling with confidentiality-preserving technologies (Article 4(5)(c)) and shared European AI models (Annex I, grand challenge 6). The neutral intermediaries ("trusted third parties") that make such pooling possible are, however, mentioned only in the context of manufacturing (recital 19). We propose extending them to other sectors with shared assets and building on the access rights to equipment data that the Data Act already provides.

3.4. Build edge computing for the long haul

Much of rail's AI will run at the edge: on board trains and along the track, where connections are limited and decisions must be fast. The Act supports open cloud stacks that include the edge (Article 4(2)(a)) and AI servers based on European processors (Article 4(2)(b)). Rail equipment, however, stays in service for decades and must be certified for safety. We propose that long service lives, long-term support (including security updates, vulnerability handling and a transparent software supply chain for the whole service life) and certifiability become design criteria for the European edge hardware and software the Act supports. The Cyber Resilience Act already requires security updates for as long as a product is expected to be in use. For rail, the challenge is to install them quickly without each update triggering a new safety assessment; edge technology designed for this from the start would close that gap. Energy, water and manufacturing, with their own long-lived assets, would benefit as well.

3.5. Give applied AI firm access to computing power and skills

The Act commits the Union to match Member States' computing resources for frontier AI projects, but only to "endeavor" to provide computing power for industrial, physical and public sector AI (Article 9(3)). Yet applied AI is where most economic and societal benefits will arise. We propose fair and transparent access conditions for sector consortia, including companies owned by public authorities, and sector-specific training paths in the Experience and Acceleration Centres for AI (Article 5).

3.6. Shape the priorities with the sectors that will deliver them

The grand challenges set the Act's priorities and can be updated over time (Article 6(4)). Advice comes through broad alliances (recital 30), but sectors and their EU agencies have no defined role. We propose a structured way for them to contribute. The text should also reflect the sectors it wants to reach. The Apply AI Strategy, on which the Act builds, states that "the term 'vehicle' covers all transport modes, i.e. road, rail, air, maritime, and inland waterways". Where the Act refers to autonomous vehicles, the automotive sector or mobility (Article 4(4)(a) and (7)(e), Article 7(2)(c), Annex I), it should follow this reading and include rail. The Europe's Rail Joint Undertaking could act as a delivery partner alongside the joint undertakings the Act already names.

4. A trusted cloud that works across borders

We welcome a single EU framework for trusted cloud services. It replaces a patchwork of national approaches and lets a service be assessed once for the whole Union. The Act creates an EU label with four "assurance levels"; public buyers must use at least the first level, and the higher levels where their Member State considers a service relevant to "public order". The following points would make the framework work for a sector that operates across borders and under safety rules:

- **One EU method for deciding which services need the higher levels.** Each Member State will decide for itself and may depart from the methodology the Commission is to set (Article 29(3)–(4)), so systems shared across borders could face different requirements in each country. A common EU method, with sector guidance developed with the European Union Agency for Railways, and a clear definition of "public order" would prevent this. The method should rest on objective, transparent and predictable criteria and assess services by activity and by the criticality of the data and applications concerned, at the level of each legal entity: many rail groups consist of several companies with different systems and risk profiles. Before an assurance level is set or revised, including by the Commission (Article 29(5)), the operators concerned should be consulted and their own risk assessments taken into account. Being an essential service under NIS2 should not automatically make a service relevant to public order.
- **Migration that follows safety procedures.** Where a risk assessment requires a change of cloud service, the Act allows at most 12 months (Article 29(6)). For systems that support train operations, a change of hosting can trigger formal safety procedures. Deadlines should follow these procedures and normal contract cycles, be set in a migration plan proposed by the operator concerned and approved by the Member State, be updated if the required assurance level changes, and build on the cloud-switching rules of the Data Act.
- **Joint buying for essential services.** The Commission's joint procurement and the EuroCloud Federation are open only to public bodies (Articles 34–40). Voluntary access for operators of essential services that are owned by public authorities would spread their benefits further. The Federation's governance should be transparent and involve large public users, including these operators.
- **Obligations for private companies decided by the legislators.** The Commission could impose new assessments and measures on private companies in critical sectors by delegated act (Article 31(3)), a Commission decision that Parliament and Council can only reject, not amend. Obligations of this kind should be decided in the normal legislative procedure and build on existing sector rules.
- **Time to prepare.** The Act should apply no earlier than 24 months after entry into force, and changes to the assurance-level criteria should come with transition periods and should not apply to contracts already awarded. The new procurement rules should

apply only to procurement procedures started on or after the date of application. Framework agreements concluded before that date, and contracts awarded under them during their term, should remain under the rules that applied when the procedure was launched.

5. Continued access to state-of-the-art AI

We support including AI services delivered from the cloud in the assurance framework. In the Commission's own consultation, however, almost half of the respondents who answered the question said that only the large non-EU providers offer AI computing services today. Where public buyers must use the higher assurance levels, the best AI may therefore not be available. The Act should include a clear exception: where no recognized service offers comparable capability, buyers may use the best available service (building on Article 30(4)(a)). Common, objective criteria should define when no adequate alternative exists, for example because no recognized provider offers the service, its functional coverage is insufficient or its delivery timeline is incompatible, and how a "disproportionate cost" under Article 30(4) is calculated, including the full cost of migration. This exception, like the others in Article 30(4), should rest on a documented risk assessment within the security risk management the buyer already carries out, for example under NIS2, and come with appropriate security measures. This keeps public services able to use leading AI securely while European offers grow.

6. A good fit with the rules that already govern rail

Rail is governed by detailed EU rules on safety, interoperability, cybersecurity and data. The Act will work best if it builds on them rather than adding parallel layers.

Existing rules	Where they meet the Act	What would make them fit together
Cybersecurity: NIS2 Directive and Critical Entities Resilience Directive	Sovereignty risk assessments (Articles 29 and 31); transparency obligations of recognized providers (Article 23)	One process for three distinct questions: NIS2 covers cyber risks, the Critical Entities Resilience Directive physical and other non-cyber risks to continuity of service, and the Act risks from non-EU control or jurisdiction. The Act should state this division and let companies answer all three within the risk management they already carry out under NIS2, recognized under each regime. The same should apply to the supplier-risk rules in the proposed revision of the Cybersecurity Act. Sovereignty measures should not lower security; the Commission's impact assessment itself notes that sovereign set-ups can create new configuration risks. Providers of recognized services should inform customers directly about significant incidents, actively exploited vulnerabilities and material changes, such as a change of owner, and give them access to the security logs they need, so that companies can manage supply-chain risk and meet their own reporting duties. Today, the Act requires providers to report such changes only to their auditor and national authority. This could become a condition for recognition rather than a new general obligation.
EU cybersecurity certification for cloud services (EUCS)	Entry condition for the higher assurance levels	EUCS has not been adopted. Until it is, existing certifications should be recognized across the EU.
Cyber Resilience Act and rail cybersecurity standards	Boundary between products and cloud services; connections between operational systems and the cloud	On-board, trackside and other operational rail systems should stay under product and rail-specific rules, outside the cloud criteria. Their connections to cloud services and AI solutions remain covered by companies' NIS2 risk management and rail cybersecurity standards, so the existing security requirements for these systems are maintained.

Existing rules	Where they meet the Act	What would make them fit together
Rail safety rules: Railway Safety Directive and the common safety method for risk assessment	Migrations between cloud services; evidence from AI testing	Align migration deadlines with safety change procedures; make test evidence usable in safety cases.
Rail interoperability rules (TSIs) and the AI Act	Under the AI Act, AI used as a safety component in rail systems is to be regulated through the TSIs. The Act adds its own AI definitions and cloud criteria	State that the Act does not change the AI Act or the TSIs, and that new terms such as "AI agent" apply only within the Act. Keep sovereignty requirements for shared sector platforms consistent with the data-exchange arrangements set by the TSIs.
Data Act	Switching between cloud services; access to equipment data	Base migrations on the Data Act's switching rights, and data pooling on its access rights.