
JOINT STATEMENT

Preserving Europe's leadership on fair and effective access to connected vehicle data

COM(2025) 837 — Digital Omnibus / Data Act — July 2026

As national associations representing public transport operators and/or rail operators, UTPF, VDV, ATUC, OV-NL and IGKM call on the European Parliament and the Council to preserve the European Union's leadership on fair and effective access to connected product data in the framework of the Digital Omnibus package (COM(2025) 837).

Recent international developments confirm that the global regulatory landscape is moving closer to the EU model — not further away. This reinforces the importance of maintaining the ambition and clarity of the Data Act, rather than weakening it.

1. Europe has set the global benchmark on data access — and must now protect it

With the adoption of the Data Act in December 2023, the European Union established the most advanced and operationally relevant framework worldwide for access to data generated by connected products. Its core principles — real-time, machine-readable, user-controlled access to data, including for authorised third parties — are essential to enabling innovation, competition, digital sovereignty and resilience across industrial ecosystems.

The organisations signing this statement collectively represent operators serving **in total nearly 25 billion passenger journeys per year in France, Germany, Spain, the Netherlands and Poland¹**. The vehicles we operate — increasingly battery-electric and hydrogen buses, trams, and rail units — are connected products generating operationally critical data. Our 12-to-20-year maintenance contracts depend on the ability to access that data independently.

The Digital Omnibus amendments must therefore be assessed against a simple benchmark: do proposed changes strengthen or weaken the EU's ability to deliver real, usable data access in practice?

2. Global developments confirm — not challenge — the EU approach

Since the consultation closed, significant legislative progress in the United States has reinforced the direction taken by the EU.

On 21 May 2026, the U.S. House Committee on Energy and Commerce voted **48 to 1** to advance H.R. 7389, the Motor Vehicle Modernization Act of 2026 — the first federal right-to-repair legislation in US

¹ Annual public transport ridership reaches 9.8 billion journeys in Germany, over 6.4 billion in France, around 4 billion in Spain, 1.273 billion in the Netherlands, and 3.4 billion in Poland.

history for motor vehicles. Critically for our sector, the legislation covers not only light-duty vehicles but also **heavy-duty and commercial vehicles including buses and coaches**, codifying the 2015 commercial vehicle Memorandum of Understanding into binding federal law, enforceable by the Federal Trade Commission with civil penalties.

The broader REPAIR Act (H.R. 1566), from which this subtitle derives, goes further: it would prohibit manufacturers from using any technological or legal barrier to prevent owners from accessing vehicle-generated data — including wirelessly transmitted telematics data. The bill's sponsor committed publicly to expanding the bill before the full House floor vote to cover telematics explicitly. The debate over wireless operational data is active and unresolved.

This follows a February 2025 federal court ruling in Massachusetts upholding that state's open-access telematics law against a four-year OEM legal challenge. The court found that compliance was technically feasible and that cybersecurity concerns did not justify blanket restrictions on standardised data access (appeal is ongoing). More than 20 US states have active right-to-repair legislation in 2025–2026.

These developments demonstrate that:

- Data access is technically feasible at scale, including for wireless vehicle data;
- Cybersecurity concerns do not justify blanket restrictions where proportionate solutions exist;
- Public authorities increasingly support enforceable access rights.



The United States has historically been among the most industry-protective jurisdictions on data sharing. The fact that it is now moving to enforceable federal law confirms that our approach is technically achievable and politically sustainable. Any weakening of the EU framework would risk placing Europe behind developments it has itself inspired.

3. What this means for public transport operators and authorities

The Data Act, as adopted in December 2023, is architecturally better designed than any US right-to-repair legislation to deliver effective data access: machine-readable, real-time, directly to users and authorised third parties. The Digital Omnibus, in several of its proposed amendments, risks moving in the opposite direction — narrowing the definition of access and widening the grounds for manufacturer refusal — precisely as the US demonstrates that enforceable data sharing is technically feasible and politically achievable.

In practice, there are still too many cases where manufacturers restrict access through reclassification of operational sensor data as 'derived data', through cloud-only delivery models that recreate structural dependency on a competitor's infrastructure, and through broad invocation of trade secrets to block access to basic operational parameters. Operators across Europe have spent millions of euros installing redundant sensors on vehicles they own, simply to reconstruct data already collected by the manufacturer's own onboard module.

As our fleets transition to battery-electric and hydrogen technologies, this problem becomes acute. A traction battery represents approximately 30% of an electric bus acquisition cost and uses rare earth materials. Access to battery health data — charge cycles, degradation parameters, thermal events — is operationally critical for maintenance planning, warranty management and end-of-life assessment. These are connected components within connected products. The right of access under the Data Act must cover them.

4. Key messages to EU co-legislators

We, national associations representing public transport operators and/or rail operators, call on the European Parliament and the Council to:

- **Welcome the deletion of the proposed “access” definition and confirm that “direct access” under Article 2(4c) means actual, transmissible access to data in machine-readable format (amendment 13 of the draft by EU Parliament rapporteurs).**

The proposed formulation “without necessarily implying the transmission or downloading of data” must not be reinstated. For operators and independent service providers, access that does not permit machine-readable data transmission is operationally meaningless. This right must extend to component-level data, including battery management systems.

- **Ensure that historical data is explicitly included within the scope of the right of access**

Manufacturers who retain and exploit historical operational datasets for their own services must make those datasets accessible to the operators who generated them. Access limited to future data streams does not enable the long time series on which AI-driven fleet management depends.

- **Reject proposed amendments that widen trade secrets refusal grounds**

The current balance — refusal possible but justified, motivated and proportionate — must be maintained. Operational parameters, physical measurements and status codes resulting from the normal operation of a connected product cannot be presumed to fall under trade secrets.

- **Build on the Commission’s “Guidance on vehicle data” of 12 September 2025 and extend it into binding sectoral guidance for public transport and rail within 18 months**

The current balance — refusal possible but justified, motivated and proportionate — must be maintained. Operational parameters, physical measurements and status codes resulting from the normal operation of a connected product cannot be presumed to fall under trade secrets. The existing guidance is a welcome first step, but it is expressly limited to the automotive sector and, by its own terms, cannot be extrapolated to the public sector. It does not address rail rolling stock, the specific operational use cases of heavy (public-)transport fleets, or certain access to component- and sub-assembly-level data. Given the size of the public transport sector and its importance for public services, social stability and energy management, this extension should be developed in consultation with operator representatives, entrusting CENELEC with a formal standardisation mandate.

About the signatories:

UTPF (Union des Transports Publics et Ferroviaires) is the French federation of public transport and rail operators, representing urban, suburban, regional and intercity services throughout France.

VDV (Verband Deutscher Verkehrsunternehmen) is the leading German public transport and rail freight association, representing over 600 companies.

Atuc Movilidad Sostenible, the Association of Urban Public Transport Operators brings together Spain's public transport companies, working towards sustainable mobility and the continuous improvement of a sector that generates more than 25,000 jobs and has an annual turnover of more than 5,000 million euros. Thanks to the bus, metro, train and tram companies that make up this association, more than 4,000 million people are able to travel each year. Further information is available at www.atuc.es

OV-NL is the association for all public transport companies in the Netherlands. Every day, about 2.2 million passengers use various forms of public transport. With their services, the public transport companies make an important contribution to the quality of life and accessibility and the economic and social development of the Netherlands.

IGKM: The Chamber of Urban Transport (IGKM) is a Polish organisation that brings together around 260 members, including public transport companies and authorities, as well as firms and institutions associated with urban public transport. Approximately half of its members are public transport operators. IGKM works to promote the development of public transport in cities by representing the interests of transport authorities, operators, vehicle manufacturers, technology providers, and other stakeholders involved in the public transport sector.

Contacts:

UTPF: Sigrid Claviéras - sclavieras@utpf-mobilites.fr

VDV: Annika Degen - degen@vdv.de

ATUC: Jesús Herrero - jherrero@atuc.es

OV-NL: Lisa van Ginneken - l.vanginneken@ov-nl.nl

IGKM: Dorota Rondtke - dorota.rondtke@igkm.pl

ANNEX

OPERATIONAL EVIDENCE | DIGITAL OMNIBUS / DATA ACT — COM(2025) 837

Why “access” without transmissible, documented and locally available data is no access at all
Three documented cases from operating fleets — and why the documentation manufacturers claim they cannot share already exists and is already disclosed to public authorities.

▪ Case 1 — The fuel cell that reports to Canada, not to its owner

RVK operates approximately 170 hydrogen buses equipped with fuel cells supplied by a Canadian manufacturer. Every fuel cell continuously transmits its operating state, running hours, fault codes and performance parameters directly to the component maker via 3G — and also to the bus OEM.

The operator, who owns the vehicles and is legally responsible for maintenance and safety, receives none of this data.

This produces a three-tier hierarchy: component manufacturer (full visibility) → vehicle OEM (partial visibility) → fleet owner (none). It is the default architecture of any modern heavy vehicle with a connected sub-assembly carrying its own SIM — battery management systems, ADAS modules, smart cameras, ZF drive units. The party with the least stake in the asset has the most access to its data.

This problem is now being extended deliberately. In late May 2026, Volkswagen Group switched its vehicle data API to a closed authentication scheme, cutting owners of VW, Audi, Cupra and Škoda vehicles off from their own data through independent tools. BMW had done the same a year earlier, routing access through paid commercial partnerships. **Data the customer already owns is being converted into a recurring subscription.** The OEMs themselves are not immune: when a connected sub-assembly reports exclusively to its own maker, the vehicle manufacturer who integrated it loses visibility too. The closed model damages everyone except the party holding the keys.

Manufacturers cannot invoke cybersecurity as a justification for withholding OBD data access: under UN Regulation No. 155, vehicle type approval already requires OEMs to demonstrate that onboard diagnostic interfaces are secured by design through a certified Cybersecurity Management System (CSMS), and the Court of Justice of the European Union confirmed in Case C-296/22 that cybersecurity requirements do not restrict the data access rights established under Regulation (EU) 2018/858 — security must be achieved through vehicle design, not by controlling who can read the data.

Legislative implication

The Data Act's access right must be “direct” and reach component-level data — not only data routed through the OEM's gateway. The proposed Article 2(4c) definition of access “without necessarily implying transmission or downloading” would formalise this exclusion. Access must mean transmissible, machine-readable access — not a manufacturer-mediated view.

▪ Case 2 — The documentation exists. It has already been disclosed to regulators.

When operators request interface documentation — the signal lists and component communication specifications needed to interpret onboard data — manufacturers too often refuse, citing trade secrets or technical infeasibility. Both defences are contradicted by existing law and by the manufacturers' own prior conduct.

To place a vehicle on the EU market, manufacturers must submit a complete technical dossier to the national type approval authority under Regulation (EU) 2018/858. That dossier includes full documentation of every electronic control unit and its interfaces — precisely what operators are being denied. **The manufacturer who claims this documentation cannot be shared has already shared it with a public authority as a legal precondition for selling the vehicle.**

The trade-secret objection fails on its own terms. An interface specification — the messages a component exposes and how to read them — reveals nothing about how the component was designed or built. Competitors already know this: OEMs have run reverse-engineering programmes on each other's vehicles for decades. Capte was itself commissioned to reverse-engineer the CAN bus of the Tesla Model X on behalf of PSA (now Stellantis). Withholding documentation protects no IP; it simply re-monetises engineering already paid for by the customer.

The “same-as-dealer” floor reinforces this. Under Article 61 of Regulation 2018/858, confirmed by the CJEU in Cases C-296/22 and C-319/22, manufacturers must provide independent repairers with the same diagnostic data available to their authorised dealer network. A manufacturer cannot claim technical infeasibility for data it already delivers to every dealer workshop in Europe.

Note also that standardised signal lists — FMS, rFMS, VDV 238, OBD-II — were useful but are structurally insufficient: vehicle technology evolves faster than standardisation committees can ratify. The right lever is not a new list; it is requiring the documentation that already exists to travel with the product. Three operational consequences of the current gap:

- **Fault tracing across sub-assemblies**

Many malfunctions arise from interactions between components. Without documented interfaces, operators cannot trace faults across component boundaries and are left replacing whole assemblies by trial and error — pushed back to the OEM to diagnose a problem they are fully capable of solving with documentation the OEM already holds.

- **ADAS recalibration after repair (Iveco front assist)**

Front-collision assist and equivalent systems depend on continuous calibration data exchange between sensors and actuation units. Without interface documentation, operators cannot verify correct behaviour after a repair, nor commission an independent workshop. The operator who is legally responsible for the vehicle's safety cannot access the data to discharge that responsibility.

- **Smart cameras with their own SIM**

Onboard video-processing units stream data directly to the component maker over their own cellular connection. The operator receives neither the data nor the documentation to read it locally — yet carries full legal accountability for the vehicle's behaviour.

Legislative implication

The Data Act's requirement to provide 'metadata necessary to interpret and use the data' must be read to cover interface documentation. The feasibility objection is foreclosed: type approval law already requires this documentation to exist and to be disclosed to national authorities. Restricting access to acting on a product — writing parameters, clearing DTCs — can legitimately be reserved for qualified professionals. Restricting the documentation of the interface should not be permitted at all.

■ Case 3 — When the manufacturer disappears

Server-dependent access fails permanently when manufacturers cease to operate. Two European heavy-vehicle makers failed within two years: Van Hool (Belgium, bankrupt April 2024) and Quantron (Augsburg, insolvency late 2024, narrowly rescued). The Fisker case shows the mechanism: after its Chapter 11 filing in June 2024, owners of ~11,000 Ocean SUVs watched vehicle capabilities degrade as cloud servers went dark. They reverse-engineered the CAN bus themselves and published open-source tools on GitHub — the right to repair asserting itself the hard way, with no documentation, because none had been shipped.

For public transport authorities on 12-to-20-year maintenance contracts this is not theoretical: a fleet that cannot be serviced because a manufacturer has ceased to exist is an authority in breach of its public service obligations. Beyond resilience, there is a procurement competition effect. Today, operators think twice before contracting a small or new OEM precisely because of this risk. Remove that risk — by guaranteeing that documentation exists and ships with the vehicle — and the calculation changes: an operator who knows they can

service the vehicle regardless of the manufacturer's survival has every reason to give a challenger a chance. Documented interfaces lower the barrier to entry and reduce lock-in to incumbents.

Legislative implication

Data access rights and interface documentation must be available locally, shipped with the product and independent of manufacturer servers. The type approval dossier already establishes that this documentation exists. What is missing is the obligation for it to travel with the vehicle to its owner — a requirement that, far from constraining the market, is one of the most effective things the EU could do for competition and for the smaller European manufacturers it says it wants to support.