



## Access to vehicle data functions and resources for HDV – Revision of Type Approval necessary

*Brussels, 24 October 2023*

**Executive summary:** The digital services market for Heavy-Duty Vehicles (HDV) is currently more advanced compared to that of Light-Duty Vehicles (LDV) in leveraging vehicle data for the provision of services<sup>1</sup>. This advancement is facilitated through the Fleet Management Systems Interface (FMS), which serves as a standardised gateway for accessing vehicle data. Access to vehicle data via the FMS interface is contingent upon Original Equipment Manufacturers (OEM) authorisation. However, despite allowing such access, the data scope available is notably limited, often insufficient to support a wide variety of potential use-cases.

As a result, many services must rely on data sourced from third-party communication devices retrofitted to vehicles. This individual, direct vehicle data access is the foundation of an innovative and highly competitive telematics service market with numerous independent players. **The impending full implementation of UN R155 raises questions about the continued viability of this individual direct vehicle data access.**

Consequently, there is a pressing need for a **revision of the vehicle Type Approval Regulation** to address the specific challenges of the HDV market. This revision should ensure that sector-specific regulations tackle issues such as the equitable utilisation of the standardised FMS-interface, the creation of **equal opportunities for accessing vehicle data, functions and resources**, and the establishment of defined processes for the regular review and adaption of the available data scope, guaranteeing a level playing field for all actors.

**State-of-play:** The digital services market for HDVs is experiencing robust growth in Europe, with a variety of competing Telematics Service Providers. The existing standardisation of vehicle data<sup>1</sup> has played a crucial role in driving market expansion. However, this standardisation alone falls short of ensuring a level playing field, particularly in light of the forthcoming cybersecurity requirements set to take effect in July 2024.

Presently, this market is significantly fragmented and largely dominated by independent service providers. Furthermore, the full implementation of UN Regulation No.155 for Cybersecurity and Cybersecurity Management Systems<sup>2</sup> is poised to impose potential limitations on the installation and operation of retrofit devices. This, in turn, could significantly impact data retrieval methods, narrowing access primarily to OEM-controlled interfaces, such as the FMS port or vehicle manufacturers' backend solutions. Such a shift in the current market may introduce distortions and pose exclusionary risks to existing and potential players, as well as limiting innovation opportunities while simultaneously reinforcing the position of vehicle manufacturers as gatekeepers with a privileged ability to provide services.

### What is required from regulation?

The following elements are currently missing and need to be addressed through regulation:

- Ensure full transparency on accessible data, functions and resources in heavy-duty vehicles across all communication interfaces (whether in the vehicle, remote or on webservers);
- Establish rules on non-monitoring of service providers' activities by the data holder;

<sup>1</sup> SAE J1939

<sup>2</sup> <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>

- Enforce non-discriminatory access to vehicle data, functions and resources, regardless of the entity acting as the gatekeeper;
- Provide access to all readily available data, functions & resources available in heavy-duty vehicles for service providers at a level of quality, quantity, and service equivalent to that offered to vehicle manufacturers;
- Mandate a core set of data points that manufacturers must make available whenever technically feasible within the vehicle;
- Implement a standardised process for regularly updating mandatory data points within the FMS without necessitating the disclosure of specific use-cases;
- Establish a well-defined and regulated authorisation and authentication process for gaining access to vehicle data, functions and resources, particularly within this highly customised professional-use segment;
- Create a clear framework to allow standardised communication interfaces to evolve over time, taking into account emerging market and technological demands; and
- Outline explicit provisions for the implementation of UN R155, particularly in cases where aftermarket tools are fitted in N category vehicles, necessitating interaction with the main truck body, and in O category scenarios where trailer and semi-trailer parts need to connect with the truck network.

**Future Outlook:** Taking into account all the above, it is imperative to establish a **comprehensive EU legal framework for accessing vehicle data functions and resources**. This framework should address the unique challenges of the evolving automotive landscape, including advancements in vehicle software interfaces, new powertrains, the imminent shift towards full automation and the growing importance of cybersecurity. Such a framework will ensure that all market players can benefit from the opportunities and innovation potential enabled by telematics.

The recently finalised **Data Act needs to be complemented in a timely manner with sector automotive rules** covering all vehicle segments, included but not limited to heavy-duty vehicles. This can be achieved through the relevant revision of the Type Approval regulation. This approach provides industry with the necessary lead time and stability to focus on developing the next generation of digital services, ultimately benefiting society, the environment and the broader EU economy.