Trusted and independent TrustCenter ensures safe automated and connected driving

The Passau Declaration of the EU Transport Ministers for a **"Smart Deal for Mobility"** outlines the way in which the EU can become an international pioneer in the approval of highly automated and connected vehicles. Highly automated driving offers the chance to make traffic safer, more efficient and more environmentally friendly. At the same time, with its data strategy and plans for a common **European mobility data space**, the EU is creating a comprehensive ecosystem for intelligent mobility data management and for fundamental mobility transformation.

The sector of independent testing bodies believes that the political discussion about a European mobility data space does not sufficiently considers road safety, especially with regard to automated and connected driving. In this context, **independent and trustworthy data sharing and utilization** are basic preconditions for safe, highly automated mobility as well as for new mobility services and concepts that make our cities and communities more livable in the long term.

However, new driving assistance systems, highly automated vehicles and their connectivity with each other, as well as with the infrastructure, are **redefining vehicle testing**: Vehicle safety and environmental compatibility no longer depend solely on mechanical components, but increasingly on electronic and digitally integrated components, as well as on the respective software versions and AI algorithms. Therefore, the **"third party principle"** remains substantial also to software testing and self-determined and non-discriminatory data access, which is essential for the approval and inspection of such vehicles, thus guaranteeing road safety, consumer protection and a fair market economy.

An independent **TrustCenter** will act as a neutral entity to facilitate trustworthy, non-bureaucratic cooperation in data exchange between different players in the mobility sector. It will administer the necessary equal data accesses and thus contribute to solving existing challenges in the vehicle type approval and inspection of highly automated vehicles.

Requirements for vehicle type approval and inspection of highly automated vehicles

The complexity of all possible traffic scenarios and situations cannot be fully mapped when approving new vehicle types with highly automated driving functions. Furthermore, at the beginning of the product life cycle, possible deterioration of the vehicle due to degradation, manipulation or damage cannot be predicted for all possible cases. In order to ensure operational, road and environmental safety, the software of a motor vehicle as well as its electronic and connected components must not only be checked periodically throughout the entire vehicle life cycle, but also continuously by independent authorized bodies (third parties). For example, Over-the-Air updates installed at ever shorter intervals can change the driving behavior and/or the emission behavior of a vehicle. In addition, new challenges such as cyber security and manipulations are emerging, which make a technical inspection of the entire vehicle system necessary.

Consequently, the sector of independent testing bodies takes the following positions.

1. non-discriminatory access to the original vehicle data by the vehicle owner/user or by third parties commissioned and authorized by the latter
A legal framework for fair, non-discriminatory access to the environmental and safety-relevant data generated in the vehicle, accessible via a data interface, must be created. The focus is on the owner/user of the vehicle as the data owner. Mandatory rules are needed that define who can directly access specific data or request access.

2. ensuring that authorities and testing bodies are able to perform sovereign functions
In the case of highly automated and connected motor vehicles, the performance of sovereign tasks demands unrestricted access to original environmental and safety-relevant vehicle data, including over-the-air. Independent access to safety-relevant data and diagnostic functions in the vehicle is a necessary basis for the definition of universally valid, unambiguous and objective evaluation criteria and methods for the validation of automated and connected vehicles as well as for efficient, independent vehicle testing during the whole vehicle life cycle. #

3. definition of requirements for a self-determined and fair access to in-vehicle data with respect to data security and data protection
The authenticity of safety and environmentally relevant data, the security and confidentiality of data transfer, and compliance with all data protection rules must be legally regulated. For this purpose, qualified certification by authorities or independent certification bodies should be carried out according to internationally defined standards. Data control remains the domain of the person affected by data protection, i.e. the user/owner of the vehicle. These requirements must also be checked as part of the technical inspection during the vehicle life cycle. In addition, the communication requirements of all digital interfaces of the vehicles must be standardized in the long term and referenced in the corresponding international regulations.

4. setting up a manufacturer-independent body - a trust center - for access to vehicle data for sovereign tasks and a European mobility data space

A trust center functions as a trustworthy and independent entity that acts on behalf of the government. It creates secure, equal and non-discriminatory access to relevant data of automated and connected vehicles for authorities, testing institutions and other authorized bodies.

For instance, the TrustCenter verifies the identity of the communication partners. In this way, vehicle data can be made available to third parties via the available digital infrastructure according to defined usage profiles. The necessary storage or processing of vehicle data for sovereign purposes such as the roadworthiness test, which require the highest level of data protection, data security, trustworthiness and independence, can thus be realized. These requirements also exist in the design of legal regulations for a Data Storage System for Automated Driving (DSSAD) and a future mandatory Event Data Recorder (EDR).