

Handling access to in-vehicle data at the GRVA

I. Context

1. Contracting parties have full latitude to regulate the access to the vehicle data independently. This would raise the issue of harmonization between the contracting parties.
2. In the international arena, UNECE' WP.29 has the tools to regulate and harmonize access to vehicle data.
3. GRVA, as part of WP.29, is addressing the international harmonization of technical aspects of vehicles. The vehicles which are currently coming to the market and used on the roads create an amount of in-vehicle data. It should be of global interest to have a discussion on this global level on how to handle these data (e.g. "How is a sufficient way to store what data?") in front of different use cases (B2B or B2G). It may also be of interest for the industry to have as far as possible a kind of global harmonization on how to go on with the in-vehicle data. Otherwise, they may have to adapt their vehicle configuration to several different acting markets. These discussions may result in a regulation concerning this topic.

II. Way forward

4. Currently, there are different possible ways (models) how to handle in-vehicle data. Every model which proposes to handle the in-vehicle data includes its own advantages and disadvantages. The diversity of the models creates an overview of the different possibilities. Therefore, an evaluation covering a wide range of different items may be helpful to realize what model includes what. The evaluation of existing models will create knowledge concerning the necessities and the challenges of a harmonized way to handle in-vehicle data.
5. GRVA should work on minimum requirements for each of the systems and each of the use cases. The GRVA has instruments that can ease regulating the access to the vehicle data:
 - (a) UN Regs, UN Rules and UN GTRs
 - GRVA shall regulate from the technical point of view all aspects needed, for instance:
 - i. Data to be collected
 - ii. Transmission of data
 - iii. Authenticity and non-repudiation of data.
 - iv. Encryption requirements of data to be transmitted
 - Transmission control via trust centre
 - Conditions of transmission: Transmission only in compliance with rules for access to safety relevant and other sensitive data.
 - Identification of data that shall be available for sovereign tasks
 - Requirements to the stakeholders (Manufactures, Technical Services, Authorities, etc.) and auditing.
 - (b) Recommendations

- Provide advice to Contracting Parties on the establishment of the national rules to provide access.
 - Advice on the penalties of non-compliance with the rules when it happens.
6. A GRVA task force or informal working group should assess the existing access models, as stated in GRVA-12-11 Chapter D, regarding their readiness for sovereign tasks¹ (discuss if it is necessary to add more items to the structure, the subcategories or existing items; discuss and clarify how to handle proposed items and its answers).
7. Tasks of the informal working group:
- Assessment of the importance to the access to the in-vehicle data for sovereign use cases, such as type approval and vehicle life cycle compliance.
 - Defining the principles guiding the access to the in-vehicle data (e.g. Fair, Non-discriminatory, Reasonable, Cybersecure, Trustworthy, Independent, Available for sovereign tasks).
 - Working on the different definitions (e.g. access to the in-vehicle data, sovereign uses cases).
 - Review of existing regulations and guiding principles (at the national and the international level) regarding the access into vehicle data.
 - Assessment of the possibility of harmonizing the different legislations.
 - Harmonize between the different access to the in-vehicle data models proposed by the different stake holders.
-

¹ "Sovereign tasks": means tasks that are performed by sovereign public bodies and authorities. This could, for example, be in the field of roadworthiness testing, road safety and environmental compatibility.