Verband der TÜV e.V.

TÜV®

Author
Richard Goebelt

Date
15-Jan-18

Data Protection, IT Security & Compliance as a Basis for New Business Models in a Digital Connected Mobility

In-vehicle data has increasing importance in the automotive industry's business models. However, any use of this data must adhere to the restrictions imposed by data protection, safety and competition law. The concept of a secure and neutral platform inside and outside the vehicle proposed by the Association of Technical Inspection Agencies (VdTÜV e.V.) with the "Automotive Platform" and the "TrustCenter" enables commercial use while taking into account the legitimate interests of all parties involved, from vehicle users to manufacturers, suppliers and providers of third-party mobility services. A neutral and complete provision of the relevant data is essential, especially with regard to the further development of the periodic technical inspection (PTI) into a persistent automated inspection (PAI).

Data is a commodity, so legal and economic conditions must be created for its use

The modern motor vehicle is no longer simply a piece of hardware, but rather a component of a digitally connected system. The safety and security of the motor vehicle and the design of the mobility market are decisively defined by the best and most up-to-date software for the respective vehicle components over the entire vehicle life cycle. Vehicular communication systems in which vehicles and roadside units are the communicating nodes provide new business cases with the potential to widely transform the services market in the automotive sector.

Only a comprehensive security-related analysis and assessment of data-based mobility services and digital functionalities in the vehicle can provide the necessary trust and acceptance in the automotive industry between manufacturers, suppliers and the aftermarket as well as among the general public. From the point of view of VdTÜV, protection of personal data and protection against cyberattacks necessitates special security requirements for vehicles, which must be considered and implemented during development both in the car and in the connected system (Security & Privacy by Design).

The policy aim should therefore be to push for solutions establishing a mobility market that is as large and open to competition as possible, where all service providers and third-party providers start from an equal, fair and non-discriminatory position. Firstly, they can offer their digital services in the vehicle to the respective users securely and fully compliant with data protection regulations. Secondly, this will allow for a high degree of innovation to develop and ensure consumer protection in the automotive and mobility sectors.

Data protection, IT security, usability and competition law can be reconciled

From our point of view, however, this requires regulatory support for development through legislative measures in coordination with the EU institutions (targeted closing of gaps in protection up to and including a “data law”) and extra-legal measures (promotion of a uniform market through standardisation, promotion of awareness etc.) in the short and medium term.

All the concepts of the automotive industry are based on the assumption that the relevant vehicle data is first sent and processed to a back-end server at the disposal of the vehicle manufacturer. These concepts can only be regarded as interim solutions, but they do not in any way develop the technological possibilities of a cooperative, automated and connected mobility of the future. Product safety and product liability, as stated by the vehicle manufacturers, do not justify an exclusive right to data processing on the back-end servers of individual manufacturers, nor is this sufficient to justify preventing third parties from directly accessing the vehicle data. The decisive issue remains that drivers should be able to choose how to handle their own data. For this reason, customers of cloud-based services must be able to independently decide which data they want to disclose and what happens to it. They must be able to detect, control and, if necessary, stop the transmission of data.

The TrustCenter in combination with the Automotive Platform provide the template for the vehicle of the future

With the TrustCenter concept, VdTÜV wants to provide its own contribution to the discussion and complement the existing approaches to data use with the idea of a secure, neutral and data protection-compliant cloud-based solution. Vehicle owners and drivers should benefit from the use of their own data through cloud-based services. In contrast to other concepts the vehicle owner and driver shall also enjoy complete transparency and data sovereignty, which the TrustCenter realises in combination with an IT security architecture in a digitally connected vehicle (Automotive Platform). They can decide to which service provider they want to release the data, when and under which conditions. In accordance with the principles of Compliance by Design and data neutrality, the TrustCenter creates technical precautions to prevent competition barriers. Automobile manufacturers and other service providers can provide their services to the vehicle owner or operator without being able to permanently read out the data and data streams of the potential competitor. This presumes that their servers meet the TrustCenter criteria, which e.g. separates the tasks of the entity granting access authorisation from those of the entity offering data-based services.

To ensure IT security and compliance with the statutory data protection requirements (Security & Privacy by Design), VdTÜV also recommends the use of a new, highly secure automotive platform that uses an appropriate interface in the vehicle to secure communication both within the system and externally. This component is urgently needed, among other things, in order to be able to securely offer Car2X functionalities in the future. According to the Automotive Platform concept, the various IT systems in the car are logically separated from each other. Entertainment and comfort systems are only connected to safety- and emission-relevant systems via the security architecture. Access to the vehicle's electronic systems via an on-board diagnostic (OBD) connector or a telematics interface (TCU) will therefore continue to be possible in the future via a highly secure IT security architecture in the vehicle.

Together, the TrustCenter and the Automotive Platform concepts enable direct, secure and data protection-compliant access to the vehicle. Data generated in the vehicle is transmitted securely and transparently via the Automotive Platform to a TrustCenter for the provision of further functionalities by partners and service providers.

Relevance to the further development of the PTI

From a technical point of view, the PTI adapter allows TÜV organisations to check the stipulated presence and functional status of safety-relevant electronic systems and to detect unauthorised manipulations and illegal tuning in engine management and emissions control. The PTI adapter has thus been in compliance with the requirements of the EU Commission since 2015. However, there is still a lack of willingness on the part of a number of vehicle manufacturers to cooperate in providing diagnostic data and software versions, although the legal basis in accordance with Regulation (EC) 715/2007 and Regulation (EC) 595/2009 already demands this. This means that we are often forced to identify the relevant data ourselves using complex re-engineering procedures. This possibility of primary control by independent third parties will also be called into question in the future. For instance, the core element of the concept presented by the German Association of the Automotive Industry (VDA) is to close the OBD interface – at least step-by-step and especially during vehicle operation.

In addition, for automated driving functions at level 3 (highly automated driving) or higher a PTI procedure as currently performed no longer seems adequate for valid testing results. From level 3 onwards, the system complexity and the combination of situations in which the system must be inspected increase exponentially. In this respect, it is necessary to supplement the periodic technical inspection with persisting automated inspections of on-board systems by independent and competent bodies.

That way, the electronic systems can be continuously monitored and do not have to be inspected during the PTI. The PTI for these systems can, for example, follow critical software updates or individual emission specifications in real time without the customer having to visit a testing centre. The prerequisite for this is direct access to the safety and emission-relevant components and their digital identification parameters over the entire life cycle of the vehicle. The periodic inspection at a testing centre would then be more focused on hardware and mechanical components.

The functional safety, security and integrity of the software of individual vehicle components can be monitored via highly secure data transfer between the vehicle, TrustCenter and/or independent inspection organisation throughout its entire life cycle. The independence of the periodic technical inspection from manufacturer specifications and its significance in terms of electronic and digital systems and uniformity are thus increased.

The aim must be to keep up with technological developments in legal and regulatory terms in order to make the best possible use of the security potential of digitisation, connectivity and automation in the interests of both the population and the economy. Under the appropriate conditions, the PTI will continue to make a significant contribution to road safety in the future and will keep pace with digitisation.