Verband der TÜV e.V.

TÜV®

Author
Richard Goebelt

Date
11-Mar-20

Comments on Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

by Richard Goebelt, Director Automotive & Mobility, TÜV Association (VdTÜV)

General Remarks

- The connected and automated vehicle is in the area of conflict between the security of the vehicle against cyberattacks on the one hand and the protection of intellectual property, legal data protection regulations and the freedom of choice of the vehicle users between data-based service providers on the other hand.

- Modern vehicles are equipped with numerous sensors that measure technical parameters and environmental conditions. Consequently vehicles record a mix of personal raw data, such as the position of the pedals or steering angle, and non-personal raw data, such as wheel speeds, engine output, brake pressure, which are available via the standardized data interface (on-board diagnostics - OBD).

- Vehicle manufacturers have begun to restrict direct access via OBD by means of electronic certificates and processes. Increasingly, data is also being transmitted via over-the-air interfaces by mobile communications. Data generation and data traffic are becoming increasingly incomprehensible for the vehicle user. Violations of data protection are more likely.

- The basic principle today is that if machine-generated data can be associated with a natural person, it is considered personal data and accordingly subject to the requirements of the EU General Data Protection Regulation (EU) 2016/679 (GDPR).

- Vehicle system, operating, location and communication data always contain information that can at least be assigned to the owner or user, as it relates to his/her vehicle.

- Therefore, the challenge arises in providing the consumer with adequate information so that he or she is able to understand the flow of data or to make a conscious decision as to which data he or she wants to make available for use or processing, when, for what purpose, under what conditions and for which company.

- Technical developments in vehicle construction as well as a changed mobility culture (multi-modal transport) must be able to map the current regulations of data protection over the entire usage framework and period of mobility offers.

Proposal of the VdTÜV:

In order to avoid data monopoly structures and to ensure the authenticity of vehicle-generated data, the VdTÜV has proposed the establishment of a sovereign TrustCenter as data administrator and the implementation of corresponding security requirements in modern vehicles. Please, read further details in the following position paper.

Central messages

- As a trustworthy authority, the TrustCenter can provide secure, neutral and non-discriminatory access to relevant data of highly automated, connected vehicles. As a trustworthy third party, it certifies and administers the respective identity of the communication partner in electronic communication processes.

- Future data processing in the vehicle must already take into account the principles of Privacy by Design and Privacy by Default during design and production. Thus, personal data should in principle remain in the vehicle itself and only be processed anonymously or pseudonymously in the backend server of the manufacturer or service provider.

- Data protection requirements should be checked both during the type approval of the vehicle and during the periodic technical inspection according EU-Directive 2014/45/EU. Suitable test and inspection specifications still need to be developed for this purpose.

- Future wireless communication requires a particularly high level of resistance and protective measures against unauthorized access, manipulation and cyberattacks. The basis for this is a corresponding security architecture in the connected vehicle.

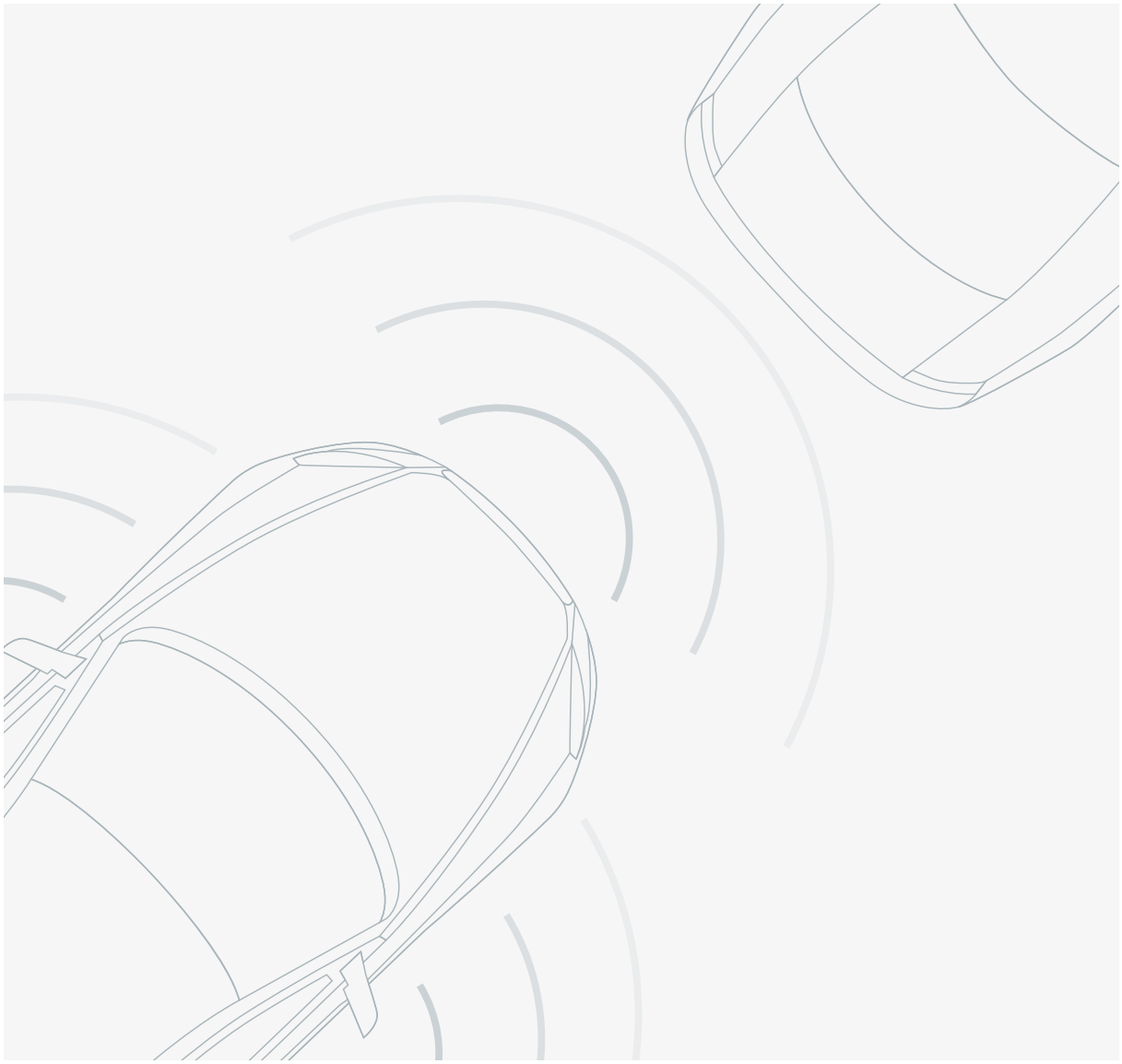
- Security architectures of this kind create security for all parties involved:
    - **Security by Design** - The vehicle protects itself against remote attacks (endpoint security).

    - **Data Protection by Design** - For all data leaving the vehicle, the data protection of personal data is automatically guaranteed by the built-in technology. The necessary data and application scenarios can be flexibly designed and modified.

    - **Tamper-resistance** - The vehicle is protected against local manipulation by a built-in, highly secure element in the security architecture.

    - Web service providers for commercial transactions in the vehicle should prove their data protection efforts by means of an appropriate audit or certification.

Verband der TÜV e.V.



POSITIONING AUTOMOTIVE TRUSTCENTER

Remote Access to Vehicle Data for ensuring Road Safety and Environmental Protection

Secure, neutral and standardised access to vehicle data – the basis for the PTI of the future

Digitalisation is increasingly shaping the environment of people and companies. The Internet of Things (IoT) has the potential to connect everything with everything else, including in the mobility sector; functionalities no longer originate in the component itself, but rather in the system context (smart services). The complexity is becoming more challenging to fully comprehend, providing more opportunities for ill-tempered entities to compromise (sub)systems or IoT components. This could impact the entire mobility ecosystem and have detrimental effects on the environment of people and companies.

In light of this situation, the TÜV companies are dedicated to the following key principles in the age of digitalisation:

1. IoT components and their smart services are to be designed and outfitted with the goal of eliminating susceptibility to cyber-attacks in order to avert damage to people, companies, and infrastructures.

2. Data of individuals and companies must be protected. At the same time, their right to secure data transmission must be ensured on a technical level.

3. Independent testing and certifications must be established in order to provide a reliable foundation to ensure trust in a digitally connected world and enable a fair competitive environment.

Technological changes in the mobility sector require the TÜV companies, as bodies entrusted with tasks of public authority, to face the challenge of further developing the testing procedures for the periodic technical inspection (PTI).

Continuous software check

The proportion of vehicles with software components is steadily increasing. However, even despite extensive software quality assurance, not all potential vulnerabilities can be detected and eliminated during development. It is therefore necessary to continually provide vehicles with software updates from the respective vehicle manufacturer, especially security patches, even after they are put into operation. To ensure that only vehicles with approved and unaltered software are allowed on the road, this also needs to be ensured through testing. Software in all vehicles must therefore be tested regularly to ensure its validity and integrity, insofar as this is relevant with regard to vehicle safety and environmental impact and/or compliance with data protection regulations. The PTI is one of the best options available for this purpose, and hence it must continually undergo further development to keep pace with the current state of technology. In the future, the PTI can only be successfully completed “without defects” if all necessary updates have been properly installed and no other defects have been detected on the vehicle.

One of the basic requirements for bodies entrusted with tasks of public authority, to be able to further develop the PTI is non-discriminatory and independent access to original vehicle data.[1] This is the only way to efficiently assess the operational safety of modern vehicles in the digital age. This requirement currently also applies to the regulation of data processing in the motor vehicle, including data recording in the form of a data storage system (DSSAD) and a prospective event data recorder (EDR) for Level 3 autonomous driving. Product and service providers of modern mobility services (e.g. automobile associations, workshops), which are to be given access to mobility data with user approval, are faced with the same challenges today.

VdTÜV therefore calls on legislators to provide the legal framework for fair, non-discriminatory access to vehicle data via an interface.

[1] The scope of specific vehicle data required for a future-proof PTI results from the respective applicable laws on vehicle approval and inspection (currently: 2007/46/EC or from 1/9/2010 (EU) 2018/858 for type approval, (EC) No. 715/2007 with regard to RMI data, 2014/45/EU (PTI Directive).

I. Authorisation and access rights by a TrustCenter entrusted with tasks of public authority

Under current practice according to the technological state of the art, data generated in the vehicle by sensors and other integrated systems is exclusively transmitted to the servers of the respective vehicle manufacturers via a mobile network interface in the vehicle and processed there. User administration and access control is the sole responsibility of the respective manufacturer. A direct transfer to an authorised body is hindered by the fact that the format, parameters, aggregation level, and quality of the data in the vehicles currently do not conform to a uniform standard. Standardised provision of data or access to third parties is currently handled via an interface in the manufacturer's backend and not directly in the vehicle. As a result, there is a non-negligible risk of data manipulation and filtering, impeding an independent technical assessment of the vehicle.
VdTÜV considers this to be an untenable state of affairs. In order to avoid data monopoly structures and to ensure the authenticity of vehicle-generated data, VdTÜV proposes the establishment of a TrustCenter entrusted with public authority as a pragmatic and easily implementable solution. As a trustworthy authority, the TrustCenter could provide secure, neutral, and non-discriminatory access to relevant data of highly automated, connected vehicles for the purpose of technical inspection. In the interest of a rapid and both technologically and economically efficient implementation, this solution could be directly mandated by EU law.

According to the officially recognised definition, a TrustCenter serves as a trusted third party operating as an intermediary to verify and administer the identity of the communication partner in electronic communication processes.

To fulfil its task of public authority, a TrustCenter is granted a state licence, for example governing access to specific vehicle data for authorised bodies. If a TrustCenter entrusted with tasks of public authority were to be involved, data access would be organised as follows:

Whenever the system queries specific data points from the vehicle, they would be transmitted to a standardised virtual interface via a mobile network using a server backend. This mobile data transmission would be "highly secure", meaning that security requirements in the vehicle would also have to be taken into account by means of relevant certifications and assessed independently. Processing or tampering with the data in the backend would be legally and technologically prohibited and explicitly would not take place. Only the respective cloud infrastructure would be used, with the vehicle data being secured end-to-end from the vehicle to the interface. At a backend interface, data provision would be handled according to a uniform standard defining both the protocol and the data format. In the medium term, standardisation for the purpose of vehicle compliance tests should preferably be based on ePTI standard ISO 20730.

Authentication/identification of participants in a transaction and authorisation of access by the TrustCenter would be independent of the provision of data via the cloud infrastructure. No user data would be stored and processed in the TrustCenter itself. The TrustCenter would assume an administrative function handling access for authorised third parties to a standardised interface in the backend. The TrustCenter, operated by a public authority, would thus control access (identification/authorisation), e.g. of a data trustee for driving mode data, a data trustee for accident data (EDR), a data trustee for diagnostic data, or direct access by a technical inspection institution for motor vehicles.

The storage of data by a neutral and independent data trustee would provide the necessary basis for efficient and purpose-related use of the data in the interest of the vehicle users pursuant to the data protection principles "privacy by design" and "privacy by default". Administrator and data processing functions would be strictly separated from each other in this context.
Since the PTI use case exclusively involves a task of public authority, the vehicle user's consent for the transfer of data to third parties, which is generally indispensable for this purpose, would not be required in this case

(pursuant to Article 6 (1) GDPR). Other examples of use cases involving tasks of public authority could include traffic control centres, or insurance companies in the context of the legally mandated liability insurance for all motor vehicles in Germany. For a possible extension to non-sovereign services, e.g. by the OEM or an insurer, the TrustCenter would have to handle communication with the vehicle user and obtain/manage their consent. In addition to access control by the TrustCenter, which would have to be regulated by law, this technical approach to mobility data management also aims to guarantee the integrity of the data, i.e. to protect it from potential manipulation.

The authenticity, security, and confidentiality of data transmission as well as compliance with all data protection regulations must be legally regulated and ensured by impartial and qualified certification pursuant to internationally defined standards at specified intervals or – in the event of technical changes – on data-relevant systems. Self-certification by the manufacturers must be prohibited by law.

Overall, the principles of "privacy by design" and "privacy by default" already play an important role during the conception phase of certification. The legal basis for this is Article 25 EU-GDPR, which requires data protection by appropriate technological design. This comprehensive security-relevant assessment of digital functionalities of the connected vehicle would foster the necessary trust and the acceptance of a future digital PTI by authorities and the general population.

II. Automotive gateway solution

The design of direct and non-discriminatory access to original data from the vehicle via a uniform interface in a uniform data format must remain the primary task of further technical development and the development of international regulations in the field of vehicle type approval. VdTÜV maintains that the objective should be the technical and legal specification of an interoperable security architecture (automotive gateway) in the connected vehicle, enabling direct data access without a backend server structure.[2]

This security architecture would provide a uniform and interoperable security standard regarding IT security in the connected vehicle or IoT product itself (endpoint security) and associated smart services. The vehicle itself would thus be able to provide suitable protection against unauthorised external access (robustness against remote attacks). Vehicle data would be allocated according to specific usage profiles. These profiles could be changed during operation by a highly secure, neutral service provider (TrustCenter as administrator), who – as mentioned above – would not have direct access to the data to be used, pursuant to data protection regulations. In this case, access control via a backend structure would no longer be necessary. The EU Commission formulated an analogous approach in the C-ITS delegated act regulating communication standards for connected cars. The international Car2Car Communication Consortium thus supports the creation of Europe-wide standards for manufacturer-independent vehicle communication. These types of security architectures ensure the following for everyone involved:

1. Security by design: the vehicle protects itself against remote attacks (endpoint security).

2. Data protection by design: data protection of any personal data leaving the vehicle is automatically ensured by the built-in technology. The requisite data and use cases can be designed flexibly and modified accordingly.

3. Protection against manipulation: the vehicle is protected against local manipulation by highly secure hardware (HSM – hardware security module or secure element) built into the security architecture.

[2] See also VdTÜV Position: Requirements for the Telematics Interface in Vehicles, January 2017.

4. Furthermore, the condition of the vehicle and the associated smart services can be monitored at any time via highly secure logging by a testing authority. Any cyber-attacks or unauthorised function changes (mode switching) would thus be detected.

The key idea behind this concept and its implementation is to focus data communication on a highly secure communication platform that is uniformly installed in all vehicles. This central platform would connect all electrical control units of the different vehicle domains (powertrain, driver assistance systems, infotainment services, as well as chassis and comfort electronics). It would control both the outgoing flow of information from the connected vehicle to individual demand carriers and the possible incoming flow of information, e.g. from administrators to the vehicle (endpoint security). Depending on the data protection regulation governing the data subject's (vehicle user) power of disposition, it could be clearly specified who receives which data. This decentralised approach applies directly to the data's point of origin and avoids more complex centralised trust service centres.

The information or data flow control would be achieved by means of encryption and signature by a secure element, so that only authorised data recipients could view the data. In a vehicle's factory condition, the platform would be set to the "highest data protection level" (privacy by default). If users/owners of the vehicle give their consent, their personal data could be transmitted for further processing. This would be mapped in user profiles.

To prevent unauthorised third parties from accessing the remote connection, more complex identification and authentication information would have to be implemented with additional access controls based on an access rights policy. All information transmitted in public networks should be encrypted in a manner ensuring that only authorised users have access to this information. In addition, control functions and update mechanisms should be protected with highly secure signatures. All remote connections should additionally be equipped with information flow monitoring to prevent the aforementioned security functionalities from being circumvented. Furthermore, remote connections should have integrated security monitoring.

A European legislative initiative based on the UN/ECE regulatory framework must impose appropriate provisions for the establishment of such a data exchange system in the interest consumers and promote the compatibility of connected vehicles in the European Single Market through uniform Europe-wide standards.

Summary

The Internet of Things is introducing revolutionary changes in all areas of our economy. The economic ecosystems emerging today will lead to increased digital interaction, deeper integration of value chains, and a growing interdependence among market participants. Increasing connectivity, the convergence of hardware and software, the spread of smart sensors, and the growing importance of big data require new approaches to data usage.

Data availability, freedom of choice for vehicle users, and confidence in the security of data use are essential for the functioning, innovation, and growth of this new digital economy. Cyber-security and data protection are key to ensuring a reliable, sustainable, and secure economy in the mobility sector.

In this spirit, the TrustCenter concept can contribute to a self-determined and transparent approach for vehicle users. It provides a practical solution for consumer-friendly consent to the use of data and also creates the conditions for fiduciary data administration by ensuring independent and fair access to vehicle data by a data trustee.

The appropriate legal basis for this must be created, especially for the purpose of safeguarding the tasks of public authority in the field of vehicle compliance in a

life cycle perspective. With a view to the future, a Trust-Center entrusted with public authority for the administration or access control of digital information could also provide a powerful prototype for data management that could serve as a template for other industries using the Internet of Things for direct access to the respective product.

The decisive factor is that users (data subjects pursuant to Article 4 (1) EU-GDPR) are given the freedom to choose how they wish to handle all data transfers exceeding the legally mandated requirements. Data processing must be made transparent for them: users must be able to identify, control and, if necessary, prevent it.

Contact
Richard Goebelt
Director of the Division Automotive & Mobility
T +49 30 760095-350
richard.goebelt@vdtuev.de