Position

VDA | Verband der Automobilindustrie

Access to the vehicle and vehicle generated data

Subject contacts

Executives

Klaus Bräunig
Dr.-Ing. Damasky
Dr. Kay Lindemann

Department leader

Graham Smethurst
Tel.:+49 30 897842-426

E-Mail: smethurst@vda.de

The need for action:

Modern vehicles already have up to one hundred on board control units that constantly communicate with each other to ensure correct driving and customer functionality. Theoretically with increased connectivity and digitalization vehicles and vehicle data can be accessed from every corner of the world. This possibility opens the door to lots of untapped potential, for example, preventing traffic accidents, making vehicles more energy efficient, reducing carbon dioxide emissions and fuel consumption whilst increasing driving comfort. Data exchange creates the foundation to link transport carriers and realize the full potential of seamless inter-modality. Data builds the intelligence for the whole traffic system, enabling highly automated and autonomous vehicles to realize their full potential. The vehicle is becoming a data generator. The secure exchange of its data builds the foundation for new business activities/ applications

There are, however, significant risks and challenges regarding safety, security and privacy. This makes the automotive industry different from already established platforms. Vehicles require much higher standards in safety, security, and privacy compared with smartphones or other consumer devices – a car is not a smartphone.

- Vehicle Safety: The objective is freedom from unacceptable risk of physical injury or damage to the health of people either directly or indirectly.
- Automotive Security: Aims to adequately protect the integrity and availability of vehicle functions, electronic components and data, against both cyber-attacks and manipulation.
- Data Privacy: The goal of data privacy is to protect the individual and to ensure that individuals are informed about any personal data usage (transparency), giving them the choice of which data is made available to which third parties for what.

Whilst enabling new customer features and business opportunities, vehicle connectivity in all forms increases vulnerability to possible cyber-attacks. Unlike the smart phone a vehicle is a safety relevant device. The integrity and security of the vehicle is paramount and must be protected at all times to guarantee predictable vehicle behavior and ensure the safety of its occupants. In the absence of a broadly accepted approach that ensures these requirements are fulfilled, the benefits of connectivity and automation will not be realized and customer confidence will be undermined.

Summary

The VDA has established a position that meets the requirements for safety, security, privacy and discrimination free innovation.

Concept for the transfer of data

This position is based on a two-level architecture:

1. Each OEM has the role of a system administrator and takes the responsibility for the safe and secure transfer of vehicle generated data from the vehicle to a standardized and maintained business-to-business (B2B) OEM interface.
2. Third parties can access vehicle data directly over the OEM B2B interface or via neutral server(s) which gather data from the OEM servers. Behind the neutral server providers can dock any services.

Access to vehicle data via the B2B OEM interface is based on B2B agreements.

There is no direct access to the vehicle by third parties to avoid risks to customer and public safety, but this concept for the transfer of vehicle generated data ensures access in a fully non-discriminatory manner contributing to innovation and allowing fair and open competition without the abuse of market power and the establishment of monopolies in digital markets.

The legally regulated status quo and further developments of the OBD-I /OBD-II interface will be retained for diagnosis and repair purposes. The OEMs reserve the right to take specific measures to protect vehicle integrity during normal operations.

Concept for data usage categories

Globally regulatory initiatives are under way to regulate the availability of data. All decisions made regarding data sharing influence competition, safety and product liability. A comprehensive and broadly accepted understanding of data and its usage is a prerequisite for a balanced debate.

The VDA position is built on four data categories.

Category 1 – Data for the improvement of road traffic safety: The focus is on the social benefits. Anonymized data is exchanged between contributing parties (including public authorities) to enable a significant improvement in traffic safety.

Category 2 – Data for cross brand services: a defined cross OEM dataset consisting of non-differentiating anonymized vehicle data.

Category 3a – Data for brand specific services: a differentiating OEM specific dataset consisting of OEM specific anonymized data and data with particular IP relevance.

Category 3b – Data for component analysis and product improvement: a differentiating component specific anonymized dataset which is made available by the OEM only to the relevant component development partner for product improvement purposes.

Category 4 – Personal data: a defined cross OEM as well as OEM specific dataset which is made available to parties authorized by the customer to process the data by law, contract or consent. The data in this category supports services that require identification of the user or the vehicle, or include the use of personal data including but not limited to the VIN. The data is made available taking into account the customers' privacy rights.

Data for the improvement of road traffic safety (category 1) will be made available by the German automobile industry to public authorities specifically for this purpose. It will be made available discrimination free

over the OEM backend servers, based on individual agreements with the OEMs. It should be a reciprocal agreement. All those who contribute data of the required quality are entitled to use the shared data.

Data in the categories 2 to 4 is characterized by different data privacy needs and data usages. Data is provided discrimination free via the B2B interface based on individual agreements with customers and third party market participants, if required. The data supply is discrimination free with respect to for example, pricing, the amount and type of data made available, timeliness of transfer and all other relevant quality criteria.

The two-step architecture applies to the handling of all four data categories and accommodates the varying privacy and usage requirements of each category. The target is to enable platforms for the exchange of mobility, aftersales and vehicle generated data in a similar way to those which exists for CE devices, offering customer choice and promoting open competition.

Political dialogue

Digitalization will bring about fundamental changes to mobility and the automotive industry. The opportunities created by this technological innovation will have greater influence on this industry sector in the next ten years than any other has in the previous thirty.

Given the very high economic and societal relevance that the rules for data usage have, the VDA wishes to actively engage in this discussion at national as well as EU level. The EU Commission has launched a number of initiatives that are related to this proposal made jointly by vehicle manufacturers and suppliers. Namely the discussion initiated by DG-Connect under the headline of "C-ITS" and the "Free flow of data initiative" directly affect the question how vehicle data can be transferred to third parties. At the same time the discussions and decisions around vehicle data affect the interests of various other corporate players e.g. the insurance industry, with whom VDA would also like engage in dialog.

This paper focuses on data for B2B and B2C usage which originates in the vehicle (vehicle generated data) and proposes an approach to making it available in a secure and discrimination free manner. From a data privacy perspective it considers only those services that address a consumer e.g. it does not consider data privacy aspects for professional drivers. As with all approaches it needs to take into account the customers' privacy rights, existing, and upcoming data protection legislation.

This position paper adheres to the VDA data protection principles published in 2014 and the joint declaration on data protection published by the VDA and the German data protection authorities in January 2016.

The digital automobile

The automobile has long been a digital device. Vehicles are rich in electronics and software controlled systems which generate and use data for in-vehicle functions. This data is already fueling more efficient engines and improved vehicle safety. A relatively recent development is the connected vehicle. Numerous types of connectivity enable the exchange of data with the vehicle.

Connected for comfort, convenience and entertainment services - Currently many vehicles are connected to enable comfort, convenience and entertainment services. The vehicle can be granted access to a customer smart phone, enabling safe in-vehicle use of apps and data hosted by the phone. The vehicle is connected to the backend to enable the exchange of data to further enhance comfort, convenience and entertainment services.

Connected for E-Call - E-Call introduces for the first time a safety element into vehicle connectivity. The reliability of E-call and the transfer of E-Call related data depends on a vehicle connection to the mobile cellular network, therefore comprehensive coverage is essential.

Connected for driving functions - The next level of safety relevance will be reached when connectivity plays a role in delivering data that directly influences vehicle behavior. This type of connectivity will enhance the capabilities of on board vehicle systems enabling automated and autonomous systems to realize their full potential in the delivery of a refined user experience. The introduction of automated and autonomous driving solutions will heighten the need for stringent security as the potential consequences of attack take on a new dimension.

Whilst enabling new customer features and business opportunities, vehicle connectivity in all forms increases the vehicles vulnerability to possible cyber-attacks. Unlike the smart phone a vehicle is a safety relevant device. The integrity and security of the vehicle is of paramount importance and must be protected at all times to guarantee predictable vehicle behavior and ensure the safety of its occupants.

Guiding principles

The EU Commission C-ITS platform project final report from January 2016 identified the following "five guiding principles that should apply when granting access to in-vehicle data and resources".

a) Data provision conditions: Consent
   The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.

b) Fair and undistorted competition
   Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.

c) Data privacy and data protection
   There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.

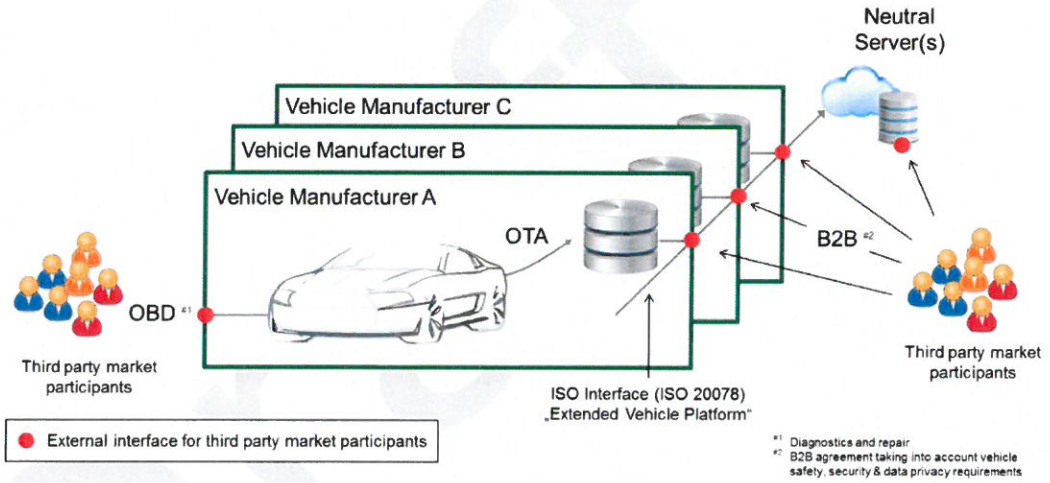
d) Tamper-proof access and liability
Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and resources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

e) Data economy
With the caveat that data protection provisions or specific technologic prescriptions are respected, standardized access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources.

The VDA proposal has been developed in accordance with these guiding principles. The approach addresses both the method of vehicle access and the vehicle generated data to be made available.

Access to the vehicle

Direct connections to the vehicle present a potential security risk, but access to vehicle generated data requires a connection. To minimize the risk, access to the vehicle must be limited to managed interfaces.



For reasons of safety, security and data privacy the transfer of data from the vehicle over the "last mile" will take place only over the OEM-Backend. In addition to the OEM backend one or more neutral servers can be installed, from which third parties can also access data for their services. The neutral servers are neither operated nor financed by the OEM.

To guarantee safety, no direct ECU trigger events are allowed over the air by third parties. Exceptions must be handled in bilateral agreements taking into account the security and safety constraints.

The legally regulated status quo and further developments of the OBD-I /OBD-II interface will be retained for diagnosis and repair purposes. The OEMs reserve the right to take specific measures to protect vehicle integrity during normal operations. Against the background of increasing threat, measures may be required for the OEMs to fulfil their legal obligations regarding data privacy, product liability, product and traffic safety.

Vehicle data outside of the diagnostic and repair focus that is currently accessed via the OBD-I /OBD-II interface and transferred via third party products will, as far as possible and in accordance with bilateral B2B agreements be migrated to the OEM backend server and therefore become available on neutral downstream servers.

Diagnostic Services requiring write functionality over the air are not permitted by third parties, subject to bilateral agreements between involved parties. This functionality is available over the OBD I and OBD II interface in accordance with block exemption regulations, to enable 3rd parties to diagnose and repair vehicles whilst stationary.

The OEM has the role of system administrator for the transfer of data between vehicle and OEM backend. The OEM will take responsibility for the aggregation gateway in the vehicle, the over the air connection and the backend. The OEM has the responsibility to ensure that this path is working and that privacy, safety and security requirements are fulfilled. The data made available by the OEM on the B2B interface will be of the same quality as the data on the OEM backend.

The vehicle data transferred from vehicle to OEM backend will appear without undue delay on the external ISO 20078 B2B OEM interface.

Data usage categories

The vast majority of vehicle generated data is raw technical data. It exists momentarily, is used locally within vehicle systems and is never stored. The remainder of the vehicle generated data can be put to various uses. The VDA has defined four usage categories for vehicle generated data which correlate with the categories described in the VDA data protection principles published in 2014.

Category 1 – Data for the improvement of road traffic safety: The focus is on the social benefits. Anonymized data is exchanged[#1] between contributing parties (including public authorities) to enable a significant improvement in traffic safety e.g.

Vehicle data: activation of hazard warning lights

Infrastructure data : emergency vehicle position

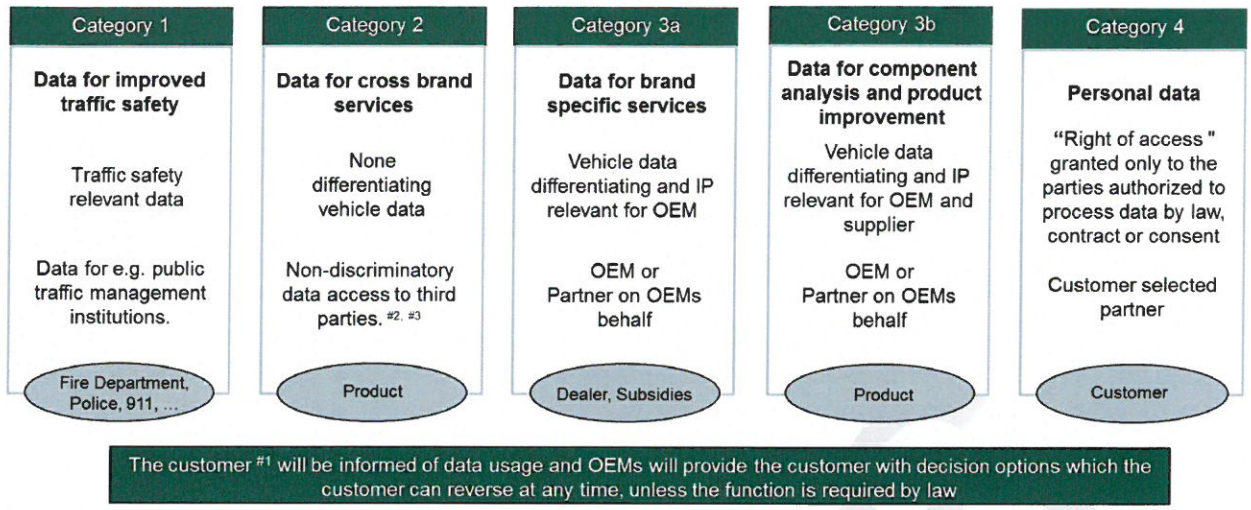
Category 2 – Data for cross brand services: a defined cross OEM dataset consisting of non-differentiating anonymized vehicle data e.g. ambient temperature, traffic flow

Category 3a – Data for brand specific services: a differentiating OEM specific dataset consisting of OEM specific anonymized data and data with particular IP relevance e.g. lane marking, chassis sensor data determining road condition

Category 3b – Data for component analysis and product improvement: a differentiating component specific anonymized dataset which is made available[#1] by the OEM only to the relevant component development partner for product improvement purposes e.g. fuel pump performance data

Category 4 – Personal data: a defined cross OEM as well as OEM specific dataset which is made available[#1] to parties authorized by the customer to process the data by law, contract or consent. The data in this category supports services that require identification of the user or the vehicle, or include the use of personal data including but not limited to the VIN. The data is only made available with the consent of an individual user or on the basis of a contract with an individual user and may only be used by the specific partner selected by the individual user e.g. vehicle position (associated with the VIN)

#1 Data is made available by the OEM to third parties within the framework of a B2B agreement.



Data usage categories

Access to vehicle generated data

Vehicle data to improve road safety (category 1) will be made available by the German automobile industry to public authorities specifically for this purpose. It will be made available discrimination free over the OEM backend servers, based on individual agreements with the OEMs. Data must be provided only when standardized and available in the vehicle. There is no obligation to create the data in a vehicle e.g. if it does not have the necessary equipment level. It should be a reciprocal agreement. All those who contribute data of the required quality are entitled to use the shared data.

Data of the categories 2 to 4 are non-differentiating anonymized data, competitively differentiating anonymized data, and personalized data made available from the OEM backend servers. Data is provided discrimination free via the B2B interface based on individual agreements with customers and third party market participants, if required. The data supply is discrimination free with respect to for example, pricing, the amount and type of data made available, timeliness of transfer and all other relevant quality criteria.

Data access is executed over a defined and certified interface to the OEM backend server. Access to the data and the creation of functionality inside the vehicle using this data requires an agreement between solution provider (third party or the operator of the independent server) and OEM (B2B Agreement). Data access takes place trusted and certified. Monitoring by the OEM is performed only to protect against unauthorized access, system attacks, and to the extent required by data protection legislation. When accessing the data the guiding principles, especially those relevant to security, safety and liability must be taken into account.

The operator of the neutral server(s) can negotiate the inclusion of additional data fields with the OEMs and make the new data fields available on the neutral server(s) without revealing the usage or the requesting provider (B2B agreement), thereby enabling new business models independent of the OEM.

#1 The term customer is used uniformly and is to be interpreted broadly. Depending on the context, it comprises drivers, owners and users.

#2 Participation and technical adaption of the vehicle cannot be demanded of the OEM.

#3 The guiding principles are to be observed when using the defined data interface. Use of the interface incorporates rights and obligations.

The anonymity of the party accessing the data will be supported to the extent permitted by data protection legislation. For personal data accessed by a third party via the B2B OEM interface the OEM is responsible for the collection and management of the customers consent and must ensure that the customer has consented to the transfer of the specified data from the vehicle, to the specified recipient, for the performance of specified purposes. For personal data accessed by a third party via a neutral server the OEM must ensure that the customer has consented to the transfer of the specified data from the vehicle e.g. via the operator of the independent server. In this case the operator of the independent server must ensure that the customer has consented to the transfer of the specified data from the vehicle, to the specified recipient, for the performance of specified purposes.

The OEMs will continue to define, design and be responsible for their respective product portfolio. Individual agreements to enhance the product portfolio are possible in the context of bilateral business relationships, taking into account technical possibilities and safety / privacy requirements.

There are no objections to the creation of third party services based on data supplied via the standardized B2B interface to the OEM backend server, provided that privacy and security requirements are fulfilled and there is an agreement in place between the service provider and the OEM.

To promote innovation and in support of research and development activities bilateral contracts for the transfer of anonymous and anonymized data will be considered. Framework agreements for development purposes need further definition.

Making data available for commercial usage via an open standardized interface is an effective approach. The generation, processing and transmission of data for commercial services will generate cost and should be part of any contractual negotiations for data usage. Frameworks for business models, usage rights and "data platform" creation etc. are to be developed in a fair, reasonable and non-discriminatory (FRAND) manner taking into consideration the separation of data cost and cost of services (a level playing field).

VDA
Verband der Automobilindustrie e. V.
Behrenstr. 35
10117 Berlin
Telephone +49 30 897842 - 0
Fax +49 30 897842 - 600
info@vda.de
www.vda.de

VDA | Verband der Automobilindustrie

Veröffentlicht am: xx.xx.xx