VDA | Verband der Automobilindustrie

Data Protection Principles for Connected Vehicles

I. Aim of the Principles

Connecting a vehicle to the Internet and connecting road users with each other will lead to changes in the upcoming years, which are of general interest to the public. The associated technical innovations in the automotive industry have the potential for further progress with regard to environmental friendliness, convenience and an increase in road safety. Various sources of information can be connected with each other in the vehicle and its environment, enabling a more efficient traffic flow management, and an improvement in road safety. In addition, based on the demands and expectations of customers[1], new vehicle functions and traffic telematics applications (online services) are being developed, e.g. in the area of convenience, servicing and multimedia.

Due to these advancements in connectivity and the new services associated with it, the requirements to be met for the protection and responsible handling of the data to be processed are increasing. In light of this responsibility and a customer relationship built on trust, the members of the VDA are formulating principles for the safe and transparent processing of data. With these principles they also want to assist customers with recognising their own responsibility for the protection of data.

The manufacturers and suppliers in the VDA take into account the principles presented herein as principles of "privacy by design" when developing and operating the aforementioned innovations.

II. Scope of Application of the Principles

The scope of application of these principles extends to the innovations in networked vehicles, such as e.g. new driver assistance systems and vehicle functions, as well as to new mobile online services, which the members of the VDA provide responsibly in their portfolio.

To implement and optimise customer demands with respect to said innovations, members of the VDA partly also co-operate with companies from the information technology sector, and strongly push for compliance with these principles also in these co-operations. If other companies, with whom the VDA members cooperate, provide their own services the member companies inform the customers at the respective interface who the service provider is and, where appropriate, who the contract partner is. Where the products and services provided are the products and services of other companies, they are the responsibility of the respective provider and are subject to its terms and conditions of use. Customers should be able to decide the extent to which they wish to use the products and services of third parties.

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

In addition to the existing statutory provisions the members of the VDA will take into account the principles set out below.

III. VDA Principles

1. Transparency

The members of the VDA strive for an adequate information about the data in connected vehicles and the use of these data.

The VDA has drawn up the attached chart for categorising the data in connected vehicles (see Attachment). Correspondingly the following categories can be distinguished:

- the processing of data is required by law
- modern data services on the basis of contractual provisions
- the customer's own data / data introduced by the customer
- vehicle operating values generated in the vehicle and displayed to the driver
- aggregated vehicle data generated in the vehicle
- technical data generated in the vehicle

The data of in-vehicle systems generated in the vehicle are primarily technical data showing the status of the system and environment in order to be able to trigger appropriate vehicle functions. The data are partly transient and are partly stored as a snapshot of a particular moment in time, e.g. for reporting a fault or for displaying operating values. They are stored in aggregated form, e.g. as fault codes, to assist with servicing and diagnosis.

The data relevant for the servicing can be read via interfaces in the vehicle and can be processed and used by trained technicians for diagnosing and repair of any malfunctions or by the manufacturer for analysing and further improving vehicle functions. The customer can obtain information about the diagnostic data through the service organisation.

The members of the VDA enable customers to inform themselves about categories of processed vehicle data and their purpose. This is done, for example, through online services or online portals or user manuals, but also through displays in the vehicle itself so that the customer can gain an overview of the active functions of the connected vehicle.

If the members of the VDA process personal data in connection with the connected vehicle they ensure that the customer can exercise his rights to this information.

2. Self-Determination

The members of the VDA are striving to enable customers to determine themselves the processing and use of personal data through various options.

The members of the VDA will enable these options through contractual provisions, consents or technical features in the framework of optional features and choices that are given, through which the customer can activate or deactivate services, unless the processing is regulated by law.

If the customer can enter, manage and use data himself, for example in the case of infotainment systems, he must also be able to delete them. Through corresponding features, which are also supposed to include a delete function, the members of the VDA enable customers to have self-determination. In addition to technical features, contractual data protection provisions and declarations of consent are offered. This also applies to apps and Internet-based services provided by the members of the VDA.

For personal data on the communication platforms provided by the VDA member companies, the companies providing the platforms are responsible in terms of data protection law. For the use of services provided by third parties, the responsibility in terms of data protection law lies with the respective third party provider and, if applicable, with the customer.

The VDA member companies want to enable vehicles to communicate with intelligent traffic systems. As far as possible, these data are to be used anonymously. If this is not possible, or is only possible via a pseudonym, the members will provide the customer with decision options either through use of the service or through technical features or through consents or contractual provisions, which the customer can reverse at any time, unless the function is required by law.

At the customer's request, data can also serve as a basis for additional optional services. The data can only be transmitted to third parties on the basis of a statutory permission or on the basis of contractual agreement with the customer having due regard for data protection law.

3. Data Security

The members of the VDA strive to implement the strong safety culture in the automotive industry also in the connected vehicle.

With intelligent technical systems road users nowadays can be better protected against many dangers such as the vehicle losing traction, microsleep and rear-end collisions. The member companies want to protect customers at the same technical level against manipulation and misuse of the data required for these systems. The protection of data in the case of connected vehicles requires data security to be constantly and proactively developed along with the progressing IT development.

The VDA member companies implement appropriate technical and organisational measures for protecting the data generated in the vehicle. The VDA members are

promoting standards, which will continuously provide a high level of technical safety, and which are to be established and further developed for the software and hardware architectures of the vehicles as well as remote access to the vehicle via the telecommunications networks. This also includes the use of suitable cryptographic processes.

The member companies feel responsible for ensuring the protection of the data generated in the vehicle and of the data assisting the customer. These principles on data security apply to technical data as well as personal data.

Verband der Autmobilindustrie e.V.
Behrenstrasse 35
10117 Berlin

03 November 2014

Attachment (Chart of Data Categories)

Chart of Data Categories in Connected Vehicles

VDA

Data Categories	No Data Protection Relevance	Low Data Protection Relevance	Medium Data Protection Relevance	High Data Protection Relevance
A. The purpose limitation is regulated by law		OBD-II	e-call (EU)	event data recorder (USA)
B. Modern data services	anonymised services car to x	pseudonymised services car to x	Predictive diagnosis, remote display (e.g. electric vehicles)	Movement profile; remote locating
C. Customer's data / data introduced by the customer		Infotainment settings and convenience settings, e.g.: Seat setting, sound volume	Navigation destinations	Address book/ Telephone personalized access to third-party services
D. Vehicle operating values generated in the vehicle and displayed to the driver	e.g. fill levels, consumption			
E. Aggregated vehicle data generated in the vehicle	e.g. fault memory number of malfunctions, average fuel consumption, average speed			
F. Technical data generated in the vehicle	e.g. Sensor data, actuator data, the engine's injection behaviour, the shifting behaviour of the automatic transmission			

Framework conditions should allow customer-oriented and practical solutions

- As far as possible the data collected in the vehicle should be and should remain **"technical data"**
- With some of these data the data controller may have an overriding legitimate interest in terms of **vehicle and product safety**
- A combination of data can lead to data protection relevance.