Version 1.0 Date October 31st 2018 internal working translation

Common positions for data processing in motor vehicles with highly and fully automated vehicle operation according to § 63a StVG

On 21 June 2017, the Road Traffic Act was amended to include regulations on automated driving. This amendment regulates the permissibility and prerequisites for automated driving, the rights and obligations of the driver and the protection of personal data. According to this, vehicles operated by means of a highly or fully automatic driving function must store position and time information when a change of vehicle control takes place between the driver and the system and vice versa. This also applies if the system prompts the driver to take over control of the vehicle or if a technical fault occurs in the system. The question of how authorised persons can gain technical access and where the data should be stored has not yet been defined. This question is left unanswered by the law. In § 63 b StVG it merely authorizes the Federal Ministry of Transport and Digital Infrastructure regarding the technical design of the storage medium, the location of the storage medium as well as the type and method of data storage.
The signatories represent the following positions:

1. In order for highly and fully automated driving to be widely accepted by society, the driver must only be able to be prosecuted for his own misconduct It must therefore always be possible to clarify who is responsible (if the system has failed or if the person has failed). The legislator has therefore stipulated in § 63a StVG that this data must be available for investigation through storage in order to clarify whether the vehicle was controlled by the automated system at the time of the incident or by the driver or was in the handover phase between the human driver and the automated system.

2. The necessary data must be in the hands of a neutral, independent third party (data trustee) in order to allow all authorized persons access to the data under the same legal conditions. In addition to storing the data in the vehicle itself, transmission to an independent third party is therefore mandatory. In the event of a vehicle being sold or after the vehicle has been destroyed in an accident, the data trustee is the only source of clarification in the interest of all parties involved.

3. The storage and transmission of the data serves exclusively the legal purpose of the comprehensibility of the ultimate responsibility (driver or system). The data may only be transmitted to an authorized third party if the legal authorization in § 63a StVG expressly permits this.

4. The consumer and society expect a significant improvement in traffic safety as a result of automation. They therefore also have a legitimate interest in knowing whether and how often vehicles in automated driving mode are involved in accidents.

It must also be possible for the consumer to check whether the manufacturers are fulfilling their performance promise with regard to the safety of their systems. Only a digital transmission of the relevant data to a data trustee can ensure the anonymized statistical evaluation required for this and already provided for by law.

5. With the amendment of the StVG, Germany is currently a pioneer in the creation of a legal framework for high and fully automated driving. Germany should now also play a leading role in the still open question of the transmission of driving mode data to authorized persons and in the digitalization of road traffic. The data trustee can serve as a blueprint for international regulation.

6. It is particularly important that the transmission of data to authorized persons meets all requirements for the highest standards of data security. This applies in particular to ensuring completeness and non-modifiability and to preventing data misuse. Storage of the data in the vehicle as well as storage by the data trustee ensures that the risk of manipulation of the data is reduced to a minimum.

7. If an authorized person is allowed to receive the data for the defined legal purposes, a simple and user-friendly process is required. Exclusive storage of the data in the motor vehicle would lead to increased costs for all parties involved (e.g. costs for reading by an expert or the motor vehicle workshop). In addition, the process of deleting data in the vehicle after the statutory storage periods have expired or if the vehicle is sold is hardly feasible. In connected vehicles that constantly exchange data with backends, the necessity of reading data from the vehicle by means of physical access no longer seems contemporary.

The organizations and associations supporting this position paper are happy to provide support on detailed questions concerning the conception of the data trustee and the technical design. The supporters of these positions are:

Allianz Germany