European Data Protection Board consultation on the Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

Currently representing over 21 million members, ADAC e.V. is the largest automobile club in Europe and the second-largest in the world. The ADAC acronym stands for an association offering its members around-the-clock assistance, protection and advice and actively promoting their interests in all mobility-related issues. As a recognised consumer protection organisation and a leading mobility services provider, ADAC focuses on individual mobility, consumer rights, road safety and road safety education.

ADAC e.V. welcomes the opportunity to provide input on the Guidelines on processing personal data in the context of connected vehicles via the public consultation. We have outlined seven points which we would like to bring to your attention:

Categories of data

ADAC welcomes the Board supporting the campaign 'My Car My Data'[1] from our umbrella organization, FIA.

Regarding the statement in the Guidelines that most of the data from connected vehicles can be considered personal data, once they relate to drivers or passengers, we would like to use this oportunity to present our position. From our point of view not most, but all data in connected vehicles qualify as personal data unless anonymized, in which case European data protection law no longer applies. In fact, FIA Region I commissioned a Legal Study[2] looking into the matter. The study revealed that it is neither relevant whether data compromises technical data, nor whether data is vehicle generated or provided by the individual for the data to be qualified as personal data due to the fact that vehicle manufacturers can typically easily identify the driver, owner and user with reasonable efforts. We support the conclusion of the study.

Regarding the special categories of data, we support the special attention given to highly sensitive categories of data like geolocation data, biometric data and data revealing criminal offences or infractions. Both European and national legislation should reflect the importance of protecting such highly sensitive personal data.

Scope

ADAC welcomes the Guidelines' clarification of the scope of the processing of personal data in the context of non-professional use of connected vehicles. In addition, we support the fact that the Guidelines considers the collection of personal data through several means, either vehicle sensors, telematic boxes, or mobile applications, when they are related to the environment of driving. This interpretation clarifies the protection of motorists' personal data does not only apply for current means of collecting data but also for new applications and devices in the coming future.

---

[1] FIA Region I Campaign and Survey 'My Car My Data', May 2017

[2] 'What EU Legislation says about car data - Legal Memorandum on Connected Vehicles and Data', Osborne Clark, Legal Study Commissioned by FIA Region I in the context of the My Car My Data Campaign, 16 May 2017.

Road Safety Concerns

ADAC shares the same concerns raised by the Guidelines regarding the driver's ability to stop the collection of certain types of data at any moment, either temporarily or permanently.
ADAC is also of the opinion that except for certain data whose use is required by law (e.g. eCall, exhaust gas control, digital tachograph), the vehicle user should have the option to easily deactivate the processing and transmission of data whose use is not absolutely necessary for safe vehicle operation (cf. key switch for passenger seat airbag deactivation).

Therefore, ADAC endorses the Guideline's provisions to incentivise vehicle manufacturers and other data controllers to implement specific tools allowing drivers to effectively exercise this right. On this note we would also like to adress a open question: Is point 88 of the guidelines to be understood as a legal right of a data subject to claim from vehicle manufacturers that a vehicle be delivered with a switch off button for data transmission? A clarification on this issue would be more then welcome since we have heared voices claiming that the "switch off" possibility/button is a legal right deriving from the GDPR.

Purposes for processing personal data

The Guidelines rightfully clarify the application of Art. 6(1)(c), GDPR to connected vehicles. As exemplified with the eCall case study, the processing of personal information can be necessary for compliance with a legal obligation to which the controller is subject. In fact, the Guidelines add that such processing still must be done in a transparent and understandable way, following Art. 13, GDPR.

ADAC welcomes this initiative and recommends the Guidelines to clarify the processing of personal data and its limitations regarding the application of the General Vehicle Safety Regulation [3] and its implementing regulations. All new cars put on the market as of July 2022 will have to be equipped with a set of mandatory safety technologies which will necessarily involve the processing of personal data, such as event data recorders, drowsiness and attention detection, and distraction recognition. Therefore, clarifying the processing of personal data coming from the mandatory application of new vehicle technologies would further increase the protection of motorists' data and privacy.

In addition, ADAC recommends that the Guidelines clarify the situations where personal data from connected vehicles might fall under the processing under legitimate interest, as described in Art. 6(1)(f), GDPR. How far can vehicle manufacturers rely on Art. 6(1)(f) GDPR when processing personal data? How can it be ensured that this article is not abused by vehicle manufacturers (for example by arguing that they have the legal obligation to observe their products on the market) when consent is not given or withdrawn? Unfortunately, the Guidelines do not enter this discussion. Such clarification could avoid data processors, including vehicle and equipment manufacturers, abusing this legal basis and processing a wide set of motorists' data, for instance, by claiming that all the information is security-relevant.

Security of personal data

ADAC recognises there are several concerns over potential unauthorised access to the data stored in the vehicles for the purpose of repair and maintenance. However, these concerns should not prevent independend third parties from getting authorised and trustworthy access to in-vehicle data, functions and resources.

[3] Regulation (EU) 2019/2144, OJ L 325, 16.12.2019, p. 1–40

To address these concerns, we call for uniform and binding specifications on access to in-vehicle data, functions and resources to be established in legislation. Together with FIA Region I we have developed a discussion paper[4] with a proposed architecture for authorised access to vehicle data taking into account the different roles and responsibilities of all the after-market competitors and vehicle manufacturers.

By implementing a uniform IT security standard for the future mode of data exchange via the vehicle's telematics interfaces, the objectives of reaching authorised and trustworthy access to in-vehicle data can be achieved. This way not only access and fair competition are ensured, but also data protection and IT security over the lifetime of the vehicle, so that consumers can trust this new digital world in their connected cars.

Data access must, therefore, be tailored according to the level necessary to perform a specific task or service, with the processing of personal data being specified, explicit and legitimate.

We recommend to address this concern by including a case study looking into the particularities of data processing and security of personal data for the purposes of vehicle diagnostics, repair and maintenance services under the section '3.1 Provision of a service by a third party'.

Data minimisation

FIA Region I welcomes the discussion of data minimisation principles in the context of connected vehicles. Motorists have strong concerns that data controllers might use the legal obligations from product liability to gather excessive personal data. We recommend that, next to the example of geolocation data, the Guidelines also mention the limits for processing personal data for purposes of liability.

Futureproofing the protection of motorists' personal data

Vehicle automation can bring significant safety and efficiency improvements in the medium-to-long term by assisting drivers in critical situations. Great uncertainties remain, however, on how and when higher levels of automation will be available to regular drivers and what this will mean for the processing of personal data.

We would appreciate it if the Guidelines adress the issue of automation and make sure that the parameters for a futureproof application of data protection rules are set.

[4] 'FIA Region I Technical Discussion Paper: Trustworthy access to in-vehicle data, functions and resources', FIA Region I, February 2020.