



FEDERATION INTERNATIONALE DE L'AUTOMOBILE
EUROPEAN BUREAU

European Data Protection Board consultation on the Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications (28 January 2020)

Fédération Internationale de l'Automobile (FIA) Region I is a consumer body comprising 104 Mobility Clubs that represent over 36 million members from across Europe, the Middle East and Africa. Our members provide roadside assistance, legal advice, insurance and many other products to their members.

The FIA Region I office aims:

1. to provide a strong representation of European Member Club interests towards the European Union institutions - for example on road safety, consumer protection, environmental protection and the promotion of sustainable motoring;
2. to build up links and support the exchange of best practices between our Member Mobility Clubs across Europe, Africa and the Middle East, and;
3. to engage in new campaign activities together with Mobility Clubs throughout the region, such as the FIA Action for Road Safety campaign.

FIA Region I 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 that could be considered in this consultation process:

Categories of data

FIA Region I welcomes the support from the Board to our campaign '**My Car My Data**'¹. Considering the increasing amount of data generated by connected vehicles, the Guidelines state most of it can be considered personal data, once they will relate to drivers or passengers.

FIA Region I believes that **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 has commissioned a Legal Study² looking into the matter. The study revealed that it is neither relevant whether data comprises technical data, nor whether data is vehicle generated or provided by the individual for the data to be qualified as personal data since vehicle manufacturers can typically easily identify the driver, owner and user with reasonable efforts.

On the back of our Mobility Clubs' expertise in consumer and data protection in transport, we recommend the Guidelines give further attention to the close and **sensitive relationship** between the **consumer** (either the owner, holder or driver of the car) and the **connected vehicle**. When clarifying the legal definition of the data subject (paragraph 37), it should refrain from portraying the consumer as a mere subject of the data treatment, but, instead, as the **origin of the data**. Therefore, when defining the data subject, the Guidelines should also mention that the **user** is the one **entitled to decide** on the data generated by the connected vehicle.

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.



Regarding the special categories of data, our Mobility Clubs support the special attention given highly **sensitive categories of data**. Geolocation data, biometric data and data revealing criminal offences or infractions, successfully highlight the need to protect personal data.

FIA Region I encourages these three categories to be also **reinforced in national legislation**, to ensure that the sensitivity is addressed in different levels of governance. Therefore, recognising in legislation the special attention to the processing of such categories of data can further protect individuals' data protection and privacy rights.

Scope

FIA Region I welcomes the Guidelines' clarification of the scope of the processing of personal data in the context of non-professional use of connected vehicles. Besides, it endorses the fact that the Guidelines considers the collection of personal data through several means, either vehicle sensors, telematics boxes, or mobile applications, when they are related to the environment of driving. This interpretation clarifies the protection of motorists' personal data not only for current means of collecting data but also for **new applications and devices** in the coming future.

Road Safety Concerns

Our Mobility Clubs share 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.

Vehicles must be safe even when the driver chooses to stop the collection of the personal data from connected vehicles, as exercising this right should not mean the individual is put at risk. In other words, **vehicles and their functionalities** must be **designed** considering all necessary safety measures to ensure that drivers are able to **safely stop the collection of data**.

Therefore, FIA Region I endorses the Guidelines provisions incentivise vehicle manufacturers and other data controllers to **implement specific tools** allowing drivers to **effectively exercise their rights**.

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 transparently and understandably, following Art. 13, GDPR.

FIA Region I 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.

Besides, FIA Region I 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),

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



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

FIA Region I recognises there are several concerns over potential unauthorised access to the data stored in the vehicles for purposes of repair maintenance. However, these concerns should not cloud the path towards achieving **authorised and trustworthy access** to in-vehicle data, functions and resources.

To address these concerns, our Mobility Clubs call for uniform and binding specifications on access to in-vehicle data, functions and resources to be established in legislation. FIA Region I has developed a discussion paper⁴ 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.

FIA Region I recommends the Guidelines to address this concern by **including a case study** looking into the particularities of data processing and security of personal data for **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

One of the objectives of FIA Region I is to bring the consumer's perspective into the current debate on increased autonomous driving trends. 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 encourage the Guidelines to consider this envisioned automation of the sector to make sure that the parameters for a **futureproof application of data protection rules** to connected vehicles are set.

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