Subject: Respons on consultation European Data Protection Board regarding draft Guidelines 1/2020 on connected vehicles and mobility related applications (28 January 2020)

Introduction

Royal Dutch Touring Club ANWB[1] is the largest association of private consumers in the Netherlands representing 4.7 million members. Located in the Hague - the Netherlands – we are active in the areas of mobility, tourism and recreation for our members. Having supported the My Car My Data campaign of FIA, we gained experience on the difference between data rights of motorists and the gaps in practise. Therefore ANWB welcomes the opportunity to provide input on the Guidelines on processing personal data in the context of connected vehicles via the public consultation. 12 Major points to be considered are listed in this memorandum.

Categories of data

1. ANWB 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 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 since vehicle manufacturers can typically easily identify the driver, owner and user with reasonable efforts.

2. On the back of our 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 as owner, holder, passenger or driver of a 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 of the vehicle** is the one entitled to decide **on use of the data** generated by the connected vehicle.

3. Regarding the special categories of data ANWB supports 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. ANWB 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 and definitions

4. ANWB 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

[1] ANWB is registered in the EU Transparency Regsiter as an NGO under number 81229841768-34

[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.

Contact information: Mike Pinckaers, mpinckaers@anwb.nl, tel. +31 653 37 48 54

protection of motorists' personal data not only for current means of collecting data but also for new applications and devices in the coming future.

ANWB would **welcome further clarification on processing of data by different public authorisities**. When are they considered to be one singular controller and when do they have to be treated as different entities and to be as third parties.

Road Safety Concerns

5. ANWB 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. 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, ANWB 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

6. 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.

ANWB 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.

7. Besides, ANWB 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?

Security of personal data

8. ANWB 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

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

concerns, ANWB calls 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 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.

9. ANWB 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 the purposes of **vehicle diagnostics**, **repair and maintenance** services under the section '3.1 Provision of a service by a third party'.

Data minimisation

10. ANWB 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**.

Case studies

To be considered in the case studies:
11 a. In practise besides eCall, bCall (business call) is applied on a large scale converging with eCall. It would be helpful if additional clarification on the obligations of the the b Call controller would be added in the case study.
11 b. Accidentology studies includes research of risky architecture of infrastructure. Connected vehicles are effective means to detect 'black spots'. This entails that location data and the extra obligations to be fulfilled for ocation data are also part of accidentology. We recommand to include these in this case study.
11 c. Tackling auto theft: in practise more and more private stakeholders (insurance, security services etc.) are concerned tracing the vehicle. It would be helpful for the case to include the duties they have to observe.

Futureproofing the protection of motorists' personal data

12. One of the objectives of ANWB 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 February 2020.