VOLVO

To:	**European Data Protection Board (EDPB)** Postal address: Rue Wiertz 60, B-1047 Brussels Office address: Rue Montoyer 30, B-1000 Brussels
From:	**Volvo Car Corporation AB**
Pages:	8

COMMENTS

ON THE GUIDELINES 1/2020 ON PROCESSING PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY RELATED APPLICATIONS

Whereas:

(A) On 28 January 2020 the EDPB has adopted the draft *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* (the "**Draft Guidelines**")[1];

(B) The Draft Guidelines have been subjected to public consultation and the EDPB welcomes comments from interested persons until 4 May 2020,

Volvo Car Corporation submits the following comments.

This document should be read in addition to the comments submitted by ACEA – European Automobile Manufacturers Association[2] (of which Volvo Car Corporation is a member), as the comments in this document represent additional matters that we considered useful to raise separately.

A. Controllership

1. The Draft Guidelines do not address controllership and much less joint controllership. However, we believe that at least for manufacturers this is a critical point. ACEA's comments already point out that the guidelines should clearly state that the manufacturer

[1] **Available online at:** https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en

[2] **Available at:** https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/edpb_guidelines_connected_vehicles_acea_comments_final.pdf

becomes a controller only from the moment the data leaves the vehicle and is transmitted to it via a network. In addition to this, we believe **it is important for EDPB to clarify when it is likely that a manufacturer becomes joint controller with another entity**, in particular in light of the recent CJEU case-law on joint controllership.

2. More specifically, given that the car manufacturer is the one deciding to implement a certain software in the car (such as infotainment operating system, autonomous driving software), and thus making the separate processing of data possible by the provider of the software, does this lead to joint controllership?

   In answering this question, the EDPB should take into account two essential aspects:

   a) First, that embedding a third party operating system is a long standing fact of life with regard to other types of platforms – smartphones and personal computers – without this ever being regarded as a matter of joint controllership between the manufacturer of the device and the provider of the operating system;

   b) Second, that in the Fashion ID case[3], CJEU has been asked whether *"the operator of a website, such as Fashion ID, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46, despite that operator being unable to influence the processing of the data transmitted to that provider as a result"*. If we replace operator of a website with car manufacturer, website with car and social plugin with software, we get exactly the question we are raising. In the *Fashion ID* decision CJEU held that there is joint controllership in such a situation, for all the reasons that we will not repeat (par. 64-85 of the *Fashion ID* decision).

3. If using a third-party operating system leads to joint controllership between the manufacturer and the software provider, this needs to be clarified by the EDPB as soon as possible.

B. Notion of personal data

4. Paragraphs 3 and 28 of the Draft Guidelines assume rather than demonstrate that "most [data] can be considered personal data since they will relate to drivers or passengers". We believe the EDPB needs to clarify **why should the different types of data generated by and in relation to a car be considered personal data, and in particular how is the "relating to" element of the definition to be interpreted.** As you can easily see in the classification proposed by ACEA, plenty of data types are very technical and relate to the car, not to the person driving or owning the car.

5. This could be a good opportunity for the EDPB to clarify **whether it considers that identifying a device equals to identifying the customer linked to that device**, which is the

[3] Case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=1D7D056DC497F6D7A170C3DBDEA5962A?text=&docid=216555&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2902258.

approach regulated under the California Consumer Privacy Act[4]. In such a case, the explanation should be taken further to **cover how information that does not identify a car but merely relates to the car, such as a serial number of a component, software version, etc., still relates to a natural person** (if this catch-all approach is indeed taken).

6. Identifiability and interpretation of Recital 26 GDPR are worthy of special attention. First of all, it is entirely unclear how far the "means reasonably likely to be used" by a car manufacturer go, especially since this can be done "either by the controller or by another person", without regard to whether this other person acts under the direction of the controller. For example, if the ride-sharing provider can identify the passenger, is this enough to consider that the passenger is identifiable for the car manufacturer? If the company buying a fleet of cars can identify who each car is allocated to, is this enough to make such persons identifiable for the manufacturer?

7. On a related note, an extremely relevant question is **who is this person that the data could relate to.** While car manufacturers usually have access to the data of the initial owner of the car (if the first owner is an individual ordering the car), the car is likely to be driven by other persons as well, not to mention further sold without this being notified to the manufacturer. Let's also think of pool cars and ride-sharing – would the technical data relating to the car relate only to the driver, or also to the passenger that ordered the ride?

8. One other aspect in this chapter is whether the degree of accuracy in identifying the natural person is relevant in any way. Aside from the natural occurring issues in identifying a natural person already mentioned above, a recent study showed that *"87% [identifying] accuracy is achievable using a single sensor (brake pedal) and only the first 15 minutes of open-road driving as a training database".*[5] What the authors of the study show is that patterns are unique to varying degrees, and the more time or other data allowed the more certainty there is in generating a unique collection. Some questions arise in connection to this:

   a) **Is a unique pattern identifiable in itself (location history, behavioural patterns such as braking, etc), even if not tied to the customer or another identifier?** WP29 Opinion 4/2007 on the concept of personal data states that "a mere hypothetical possibility to single out the individual is not enough to consider the person as 'identifiable'".

   b) **What degree of certainty is necessary for data to be personal?** Is it 100%, 85%, 66%, something else? Note that CCPA defines "Probabilistic identifier" as "the identification of a consumer or a device to *a degree of certainty of more probable than not* based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information", however under GDPR there is no indication as to the degree of identifiability.

---

[4] See CCPA section 1798.140 (x) : *"Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; [...]"*

[5] *Automobile Driver Fingerprinting*, Miro Enev, Alex Takakuwa, Karl Koscher, and Tadayoshi Kohno, Proceedings on Privacy Enhancing Technologies ; 2016 (1):34–51, available at http://www.autosec.org/pubs/fingerprint.pdf

C. Legal basis

C.1. Compliance with a legal obligation

9. In our view, the Draft Guidelines overemphasize the use of consent, and ignore the fact that a significant number of processing activities are mandated by our obligations as car manufacturers under the motor vehicles type approval and safety regulations, and in particular:

   a) Regulation No 78/2009/EC on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users,

   b) Regulation No 79/2009/EC of the European Parliament and of the Council of 14 January 2009 on type-approval of hydrogen-powered motor vehicles,

   c) Regulation No 661/2009/EC concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor

   d) All three to be replaced by Regulation 2019/2144/EU on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (the **"General Safety Regulation"**), which will apply from 6 July 2022.

10. The General Safety Regulation includes a vast array of requirements that **will make it mandatory for manufacturers to implement car features which involve processing of personal data, sometimes even special categories**. Some examples:

    a) intelligent speed assistance – warning the driver that the applicable speed limit is exceeded. This implies processing exact location, applicable speed limit at that location. Processing must be on by default, with the possibility to switch off only.

    b) driver drowsiness and attention warning, advanced driver distraction warning - systems that assess the driver's alertness and help the driver to continue to pay attention to the traffic. Driver Monitoring Systems (DMS) are already included in the Euro NCAP roadmap up to 2025[6], and aim to detect fatigue, distractions, and drowsiness in the driver. One key aspect in such systems will be detecting the position of the eyes of driver – if they are open, if they are watching the road.

11. The Euro NCAP requirements also go beyond the General Safety Regulation (and always have) in a number of situations. For example, a car will have a higher safety rating if it is equipped as a standard with child presence detection.

12. It is thus important for the EDPB to **recognize that safety regulations will always require processing of personal data to an ever-increasing extent** as cars become more autonomous, and that this will not be based on consent from the concerned data subjects. In addition, it is also important to recognise that **where the Euro NCAP certification requirements go beyond the General Safety Regulation, due to the fact that the rating is achieved only if the features are enabled by default, such requirements also fall under the scope of the legal obligation under Art. 6.1.c) GDPR.**

---

[6] Euro NCAP 2025 Roadmap. In Pursuit Of Vision Zero, available at https://cdn.euroncap.com/media/30700/euroncap-roadmap-2025-v4.pdf

C.2. Legitimate interest

13. In addition to this, we believe EDPB should **clarify when legitimate interest could be considered by the car manufacturer** (depending on the circumstances), as opposed to situations when consent *must* be obtained. In our view, the processing of data that supports certain specific functions of the car should not outright be subject to consent, but only if the legitimate interest test is not passed. That is because society as a whole has an interest that these functionalities exist, and that the generated information be used by manufacturers to research and develop safer cars, which leads to lowering the number of accidents. In our view, a minimum set of activities that would not require consent would be the following (non-exhaustive list):

    a) All features included into the General Safety Regulation (together with the delegated acts) and the Euro NCAP requirements (as well as foreign equivalents);

    b) Analysing data related to accidents. EDPB mentions accidentology studies as being based on consent (par. 146) and assumes that a "variety and [high] amount of personal data needed for accidentology studies", however manufacturers can perform analyses with regard to just technical data related to the car and in such a case there is no justification for consent. EDPB may want to differentiate between the studies looking into how the car performed and studies looking at the broader picture such as environment, impact on the persons inside and outside of the car and so on. EDPB should also clarify if consent is needed strictly because the data is collected remotely via a public network or because the intrinsic nature of the processing requires it;

    c) All features supporting autonomous driving;

    d) Public interest collaboration projects to enhance traffic safety and fluency, such as Nordic Way (https://www.nordicway.net/). Please see in particular the Functional Service Specification[7] which explains the advanced functionalities to be implemented in cars, all of which require personal data being processed, and which cannot be performed in the car since they require one or more external applications;

    e) Implementation of extended vehicle in accordance with ISO 20077:2017.

14. This is all the more important since data collected based on consent cannot be further used for research and development under Art. 5.1.b) GDPR. **EDPB should consider the critically important point whether it is suitable to condition researching and developing safer cars by the consent of customers.**

C.3. Consent

15. The Draft Guidelines overemphasize consent as legal basis, regardless of who the actors performing the processing of data are. In our view, there is a fundamental difference between the data processing performed by the car manufacturer and the processing (even of the same data) by other third parties, for their own purposes. Manufacturers not only have legal obligations in terms of safety and product warranty, but also have compelling legitimate reasons to make sure that cars operate as planned, to learn from both collisions and near-misses. When development of autonomous cars is concerned, this becomes even more obvious – autonomous vehicles will require a trove of data about the surroundings,

[7] Section 5, available at https://uploads-ssl.webflow.com/5c487d8f7febe4125879c2d8/5ca717e95f97512440b06072_NW2_A2_D21_2_ServiceDefinitions.pdf

about the car itself and about the passengers, just in order to operate properly. Making this based on consent is entirely misleading because, assuming consent were withheld, this would only lead to the customer not being able to benefit from functionalities they paid for, many of which are already customary – for example, refusing consent for use of location data by the car manufacturer would lead to not benefiting from all car features that are dependent on location, such as lane keeping assistance, parking assistance, autopilot, automatic cruise control, traffic sign information warning, etc.

16. While we fully agree that location data is sensitive and its processing should be considered very carefully, we also believe that there is a clear distinction between this data being processed by the manufacturer in order to provide functionalities of the car (including by using processors), as opposed to any other use of this data (including by third parties using it for their own purposes).

17. As a consequence, we believe **the EDPB should clarify which uses of data (and in particular location data) are allowed without consent and by which entity.** In particular, **we suggest taking a similar approach to that of the USA Alliance Of Automobile Manufacturers in their *Privacy Principles For Vehicle Technologies And Services***[8], namely:

> *Participating Members understand that the sharing and use of Geolocation Information, Biometrics, and Driver Behavior Information can raise concerns in some situations, therefore Participating Members also commit to obtaining Affirmative Consent expeditiously for the following practices:*
>
> - *using Geolocation Information, Biometrics, or Driver Behavior Information as a basis for marketing; and*
> - *sharing Geolocation Information, Biometrics, or Driver Behavior Information with unaffiliated third parties for their own purposes, including marketing.*
>
> *Affirmative Consent is not required, however, when Geolocation Information, Biometrics, or Driver Behavior Information is used or shared:*
>
> - *as reasonably necessary to protect the safety, property, or rights of Participating Members, Owners, Registered Users, drivers, passengers, or others (this includes sharing information with emergency service providers);*
> - *only for safety, operations, compliance, or warranty purposes;*
> - *for internal research or product development;*
> - *as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;*
> - *as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which, in the case of requests or demands from governmental entities for Geolocation Information, must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and*
> - *to assist in the location or recovery of a vehicle reasonably identified as stolen.*

[8] Available at https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principles for_VehicleTechnologies_Services.pdf .

> *Participating Members also need not obtain Affirmative Consent when sharing Geolocation Information, Biometrics, or Driver Behavior Information with Third-party Service Providers that assist in providing Vehicle Technologies and Services if those parties are not permitted to use that information for their independent use and the sharing is consistent with the notices that Participating Members have provided.*

18. One other important aspect related to consent is who the consent needs to be obtained from. As mentioned already both in this document and in the ACEA comments, cars have multiple users at various points in time (even personal cars). While we understand EDPB's point that "a profile management system should be implemented inside the vehicle in order to store the preferences of known drivers and help them to change easily their privacy settings anytime" (par. 88), we believe it is important that EDPB adds a few clarifications: first of all that the drivers will not be forced to create a profile, and secondly that the manufacturer is not under an obligation to identify the driver and thus process more data, but rather that the manufacturer will rely on the options and settings chosen by the driver. This clarification is critical because it means that consent will be operational for as long as the person driving doesn't make a contrary choice – and we believe this is how it should be.

D. Clarification of Biometric Data under Article 9 GDPR

19. Biometric data has been identified by EDPB among the three categories of personal data warranting special attention. As the Draft Guidelines point out, biometric data may be used to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver's profile settings and preferences. However, **the Draft Guidelines do not analyse what is and what isn't biometric data caught under the restrictions of Art. 9 GDPR – an aspect which in our opinion needs to be addressed.**

20. GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person" (Art. 4). Art. 9(1) GDPR contains an exhaustive list of so-called special categories of personal data, which due to their sensitivity are subject to increased regulatory protection. Among them we can find **"biometric data for uniquely identifying a natural person"**. In other words, Art. 9(1) GDPR clarifies that only biometric data that is used for unambiguously identifying a natural person falls under the scope of the article, and thus **if biometric data is processed for purposes other than unambiguous identification, the admissibility of the processing activity is assessed based on the general principles provided by Art. 6(1) GDPR, not under the special conditions provided by Art. 9(1) GDPR.** This position is supported also by a position paper issued in 2019 by the Conference of German Data Protection Authorities.[9]

21. We suggest the EDPB to clarify this point and make a statement in the direction outlined above, as this would greatly support the implementation of technologies that only detect certain human features (whether it is a human, whether it is an adult, whether the eyes are

[9] See Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, *Positionspapier zur biometrischen Analyse,* April 2019, p 18, available at https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Positionspapier_Biometrie.pdf.

open and where they are directed) but do not "uniquely identify" the person – such as the driver drowsiness monitoring which will soon become a common technology in the cars (see par. 10 above).

E. Law Enforcement Requests

22. While the Draft Guidelines include a case study on auto theft, they do not refer more generally to the law enforcement requests made to car manufacturers – which can occur in relation to any alleged wrongdoing, not just theft.

23. Firstly, we need to point out that we do not see the reason why "location data can only be transmitted as of the declaration of theft" – in the situation assumed in the Draft Guidelines (request made by the owner attempting to find their vehicle) it is clear that the owner should know the location as at the date of the theft, and is interested to find the location at a subsequent moment.

24. Secondly, in our opinion law enforcement requests covering "data related to the vehicle" as listed in the classification table included in the ACEA Comments (page 14f) should not pose any special issues since they represent facts about the car and do not, in themselves, aim to identify a person. This should be clarified in the Guidelines.

25. Thirdly, where other data is requested by a law enforcement agency, unlike what the Draft Guidelines seem to imply under par. 53[10] we believe that it should not be left to the car manufacturer to establish whether the request is justified or not, and whether the agency has the right to request such information under the Law Enforcement Directive (Directive (EU) 2016/680). In our opinion **the EDPB should clarify which are the conditions that must be fulfilled for a car manufacturer to be obliged to provide data to law enforcement agencies, depending on the category of data as listed in the ACEA Comments.**

26. We also believe the EDPB should specify **whether requests from law enforcement agencies to perform a future continuous collection and transmittal of data (such as movement of the car) is admissible and, if yes, under which conditions.**

*** END ***

[10] "Furthermore, data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when the specific conditions in the law enforcement directive are fulfilled. (...) Manufacturers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled".