FIGIEFA
Automotive Aftermarket Distributors

Brussels, 4th of May 2020

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

FIGIEFA is the European federation representing the independent wholesalers and retailers of vehicle replacement parts and components. It brings together 20 national associations representing over 30.000 distribution companies and 355.000 employees delivering solutions for safe, sustainable and affordable vehicle servicing and repairs for the more than 300 million vehicles in the EU. FIGIEFA's aim is to maintain effective competition and consumer choice in the automotive aftermarket sector as important value chain serving Europe's automobile mobility.

We welcome the EDPB Guidelines which bring important clarifications on the processing of personal data in the context of connected vehicles and mobility related applications. This document will be instrumental in ensuring the unleashing of the potential of automotive data while respecting the most ambitious practices in terms of data privacy throughout the entire European Union.

FIGIEFA and in general companies active in the wider automotive aftermarket of vehicle parts, diagnostics, servicing and repairs, are fully committed to respecting the highest standards in terms of data privacy.

In an increasingly digitised automotive sector, the whole automotive value chain is changing. With the advent of the 'connected car', the repair process starts now in the vehicle where the data quality and the ability to safely access car functionality determines the quality of the service.

The connected car enables a wide scope of completely new and innovative services and entails new customer expectations. With increasing digitisation, consumers expect smart digital services with remote and *predictive* information about the 'health status' of their vehicle. Nobody wants any longer to have a breakdown, but the aim is to *avoid* a breakdown. In order to ensure a competitive market for European consumers, independent businesses need to be able to take up their new role in this quickly changing environment to meet the new customer expectations (for example remotely detect the health status of the vehicle and reduce spare parts delivery times, optimise parts stocks, or even to make the parts "smarter" by advising how to add sensors that can improve the predictability of the vehicle components' wear and tear).

Any market operators, may it be car manufacturers, parts suppliers or independent service providers, will consequently have to base their services on in-vehicle data - often deemed to be personal data. The full and comprehensive respect of data privacy rules is of course crucial in this context. Processing data in a lawful, fair and transparent manner in relation to the data subject is key to build the confidence in, and to unleash the potential of, connected vehicles.

Data privacy rules are crucial for independent service providers, who are well aware of consumers' rights and our responsibilities on the matter, as recently stressed in the Manifesto for Fair Digitalisation Opportunities, signed by a broad alliance of 11 European associations representing automotive sector and mobility services operators, insurers, SMEs representatives and motorist consumers.

FIGIEFA
International Federation of Automotive Aftermarket Distributors
Boulevard de la Woluwe 42, Box 5
BE-1200 Brussels

Tel.: +32 2 761 95 10
Fax: +32 2 762 12 55
E-mail: figiefa@figiefa.eu
Web: www.figiefa.eu

EC Transparency Register ID: 69678928900-56

Against this background, **we welcome** the EDPB Guidelines and fully support the clarifying emphasis that processing must be transparent to and under the control of data subjects (e.g. typically by informed consent or by a contractual agreement). Consent – if required – must always be free, specific and informed.

Particularly noteworthy is in this context the recommendation that local in-vehicle processing of data is the most secure option (operators "should, wherever possible, use processes that do not involve personal data or transferring personal data outside of the vehicle", points 70-72). FIGIEFA welcomes and underlines the importance of this local data processing mode to minimise the risk of exposure of personal data and to optimise the economy of data. It would be fully realised with embedded applications operating in the vehicle and with a direct (commercial and GDPR) relationship between the customer and the independent service provider of his/her choice. This would be feasible with an 'in-vehicle interoperable, standardised, secure and open-access platform' (OTP), as proposed in the Manifesto for Fair Digitalisation Opportunities referenced above.

Indirect data access models, where the car manufacturer becomes the data gatekeeper and interposes himself between the customer/user/data subject and the independent service provider, do not comply with the principle of 'Privacy by Design'.[1] It creates an unnecessary duplication of data, access and GDPR controls in the hands of the vehicle manufacturer. To avoid this, direct access models to in-vehicle data allow independent service providers to manage GDPR compliance with "their" customers accordingly, instead of having to rely on the vehicle manufacturer's processing, permission and control schemes to do so. There is no need to have the vehicle manufacturer interposing himself in a gatekeeper function.

* * * *

Concerns and suggestions for clarifications:

While we believe that the draft EDPB Guidelines give valuable clarifications on the handling of data generated by connected vehicles, **we have a number of concerns over specific points, which we believe require some additional clarifications.**

Point 28 ("what constitutes personal data")

Point 28 gives a qualification of which connected-vehicle-related data are deemed to be personal data, i.e. when these are identifiable to a natural person. We would like to stress the importance of such a definition, as we see attempts of vehicle manufacture to downplay the relevance of data qualifying as personal data (by e.g. categorising them) which could form the basis for wider service offers based on an analysis this data.

In particular in instances, where a general technical improvement of the 'product quality' or 'vehicle improvement' are quoted as justification for data collection, this would not prevent this data being analysed in a different context, e.g. to form the basis of *personalised* services. In other words, this data is *acquired* as 'technical data', but could in turn become the basis of economically-related *specific* service proposition to the customer.

[1] Access to in-vehicle data, and the conditions for it, are the topic of an ongoing political discussion at EU level between different economic stakeholders, the independent automotive service providers on the one hand, and the vehicle manufacturers (who are also competitors in the automotive aftermarket) on the other hand. The effect of the technical design of vehicle manufacturers' in-vehicle telematics systems and the subsequent **application of data privacy rules** (i.e. whether it would enable or hamper effective access to in-vehicle data for independent service providers) was subject of discussions in the **Commission's Motor Vehicles Working Group Sub-WG on "Access to Data and Cybersecurity"** (10/2019-3/2020) to which FIGIEFA contributed proactively. Data privacy was legitimately one of the angles that was taken into consideration during the debates/analysis'. The European Commission is planning, as announced in the Work Program for Automotive and Mobility Industries 2020-2021 of DG GROW, to issue a legislative proposal on the topic by the first quarter of 2021.

Protecting data by using *per se* a generic classification, as the vehicle manufacturers' association proposes, has wider implications in relation to who should be authorised to access the data and subsequently use the data for alternative competing services (see also explanation in Point 82 below). Data does not lose their relevance under privacy law, neither because information describe technical circumstances nor because the privacy relevance with technical aspects like sensor data seems to be limited. After all, the combination of supposedly irrelevant data in itself quickly results in highly sensitive information.

Vehicle Identification Number (VIN)

In addition, we strongly recommend that the nature of the vehicle identification number (VIN) should be clarified. While we strongly advocate not downplaying the qualification of data as 'personal', the EDPB comments with regard to the VIN are unfortunately somewhat ambiguous and could be interpreted as if the VIN *per se* would be a personal data, which is not correct here.

It is however important to clarify that the VIN, which in itself is just an abstract number (marked on the chassis, frame of even publicly visibly through the windscreen of a vehicle), does not constitute per se a personal data. Only if and when the VIN can be referenced to a person, then it becomes personal data[2]. The capability of combining these two elements, i.e. the abstract VIN number with a person's identity (e.g. via the dealer when the vehicle is purchased, the vehicle manufacturer, type-approval authorities for product recall actions or in countries where by law, the VIN is linked to the owner) makes the difference. In analogy: any device ID, for example the number of the vehicle's motor block or of a smartphone, do also not constitute per se personal data. This clear distinction is very important, because the VIN is used as important technical data for unequivocal vehicle and parts identification in the market for vehicle servicing and repairs, and would therefore be potentially blocked by privacy restrictions on the basis of a misconception as personal data. We therefore strongly suggest a deletion of the VIN in point (28) or clarification, for example :

(28) Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver's/**owner's** complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle parts) **or the vehicle identification number (VIN)**, which, by cross-referencing **with other files ~~and especially the vehicle identification number (VIN)~~, that** can be related to a natural person**, such as e.g. the address/identity of the owner**. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

Point 82 ("transparency obligations for indirect collection of data")

This paragraph is about the specific rules that should apply when the data user gets these data from an intermediary (data controller) which has an agreement with the data subject.

Via intermediaries, but also directly without the interposition of intermediaries, often, a number of data is collected under the general, unspecified labelling of "product improvement" or "product liability", but this can comprise a very wide range of vehicle data. We are particularly concerned about the excessive

[2] This is also in compliance with the ECJ's landmark decision clarifying the definition of what personal data is (**ECJ judgement C-582/14 of 19.10.2016**) where it explained that information is only deemed personal data if the given data controller has direct – or via legal means indirect – knowledge allowing such information to be linked to an individual person. Therefore, many information must no longer be deemed personal data in the hand of given companies. As such all will depend on a company's possibility to link such data to a given person. In other words, what is personal data is no longer to be decided in an absolute way on a data-level but rather on a relative, individual level. In the past, technical (vehicle or sensor-generated) data were commonly and generally deemed personal data. But as a result of the ECJ ruling, these non-personal data can qualify as personal data under control of one company (due to additional knowledge about the actual car owner or driver) whilst it does not qualify as personal data in the hands of other companies without relevant additional information.

use of data in the context of alleged product monitoring obligations under product liability law. We see a practice whereby vehicle manufacturers invoke a very far-reaching obligation to collect data, and then use this data - once it has been collected - for their own, other interests. Obligations under product liability law justify, at best, a random sample analysis. Further collection would be a violation of data minimisation. Furthermore, the pursuit of own commercial purposes would also be incompatible with the original purpose of collecting data, also data collected in the interest of public safety. This should be clarified by the EDPB Guidance paper.

At least, we believe that for the sake of transparency, consumers should be informed in greater detail which vehicle - or component-generated data are more precisely intended to be collected. We suggest including this example into point 82 (*but also clarify in general more explicitly in the Guidance Paper*):

(82) In some cases, personal data is not collected directly from the individual concerned. For instance, a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service, **or to seek data for 'product improvement'.**

Point 89 ("change of ownership – deletion of any personal data")

This paragraph stipulates that an ensuing change of ownership should trigger the deletion of any personal data. However, our concern is that the deletion of the historical technical data will make it impossible for aftermarket operators to perform requested services where a number of historically registered data (for example the service history) are necessary to perform the service for the vehicle or to determine its state.

In other words, the absoluteness with which the requirement is formulated could result in the deletion of a certain number of technical data necessary to trace/document the state and safety of the vehicle and to perform essential repair and maintenance services.

Point 91 – ("storing a log history" – last bullet point)

In this paragraph, the Guidance Paper recommends that vehicle manufacturers should store a log history of any access to the vehicle's information system as a security and confidentially measure.

We have serious concerns over this recommendation, and request that this point would be deleted, as it would violate GDPR principles and even more, grant vehicle manufacturers (who are competitors to almost all service providers 'around the car', from aftermarket to leasing and insurance services…) undue tracking of access and use activities of independent service providers.

It would significantly impair independent service providers by giving vehicle manufacturers a monitoring right over processes, functions calls and vehicle data transferred, allowing them to draw conclusions from individual data access and thereby also the scope of data accessed. In other words, a possibility to directly monitor their competitor's business activities.

There are other technical means to ensure the vehicle's information system are secured/ensure confidentiality without direct monitoring or analysis of the data, such as authenticated access and run-time environment management, which should be conducted in the vehicle itself rather than storing log-files on the vehicle manufacturers' servers.