COMMENTS FROM ARVAL ON EDPB DRAFT GUIDELINES ON CONNECTED CARS

(comments dated 30 April 2020)

ARVAL welcomes the EDPB's effort to present guidelines (the "Draft Guidelines") on the processing of personal data by connected vehicles. ARVAL believes it is very important to find a common interpretation of the GDPR and e-Privacy Directive and appreciate the opportunity to contribute to the EDPB's discussions prior to finalizing these useful guidelines.

1. Alignment of EDPB draft guidelines on connected cars and with new e-Privacy Directive

As a general and starting statement, we would like to make the point that negotiations on the adoption of an e-Privacy Regulation are ongoing. In this context, we are concerned that the adoption of detailed guidelines relying upon current provisions of the e-Privacy Directive would not be timely. The e-Privacy Directive is indeed not aligned with GDPR and is consequently due to be abrogated and replaced sooner or later by the e-Privacy Regulation.

Adopting guidelines in such an uncertain legal environment may significantly affect the development of connected vehicles in the European Union and its benefit for both the society at large and the economy. It may force businesses to amend their operating schemes pending the adoption of the upcoming Directive while the upcoming rules may ultimately impose different approaches. This would force businesses to incur adaptation costs twice, especially considering that the Draft Guidelines recommend hardware adaptations that are going to be burdensome and expensive.

Additionally, under the hierarchy of norms principle, a Directive (even though being recognized of *lex specialis* nature) is not of direct implementation by Member States and should not prevail over an EU Regulation (such as GDPR) which is of direct implementation by Member States.

We would therefore recommend to either postpone the finalization of the Draft Guidelines until the e-Privacy Regulation is adopted or to reconsider the Draft Guidelines focusing primarily on GDPR, rather than the obsolete rules set out in the e-Privacy Directive.

2. Reliance on legitimate interest as an alternative to consent

2.1 Why consent is not a relevant legal ground

Regarding the legal grounds for the processing of personal data through connected vehicles, the abstract and automatic application of Article 5(3) of the e-Privacy Directive to connected vehicles denies certain realities on the ground and thus risks undermining services that in fact serve legitimate and, to some extent, even public interests.

A more nuanced approach taking into account the particularities of each case should therefore be preferred to an absolute and generic position, as is the case of the current Draft Guidelines.

Even if the EDPB considers that Article 5(3) of the e-Privacy Directive is a general provision, its scope of application cannot be extended inappropriately.

The application of this article should be circumscribed taking into account the specific features of the connected equipment. In this respect, the Draft Guidelines assimilates the connected cars to a "*terminal equipment*" within the meaning of the e-Privacy Directive while also recognizing that Article 5(3) of the e-Privacy Directive does not automatically apply (see par. 13: "*provisions of art. 5(3) e-Privacy directive must apply* [to connected vehicles] *where relevant*"). In other words, the draft Guidelines admit that not all connected vehicles should fall under the scope of Article 5(3) of the e-Privacy Directive.

In the context of the leasing of connected vehicles, reliance on consent may raise significant issues. Indeed, long-term leasing of cars often takes place in an employment relationship, where the employer selects a number of brands amongst which employees make their choice. Obtaining direct consent from the user of the connected vehicle is complex and may actually not be valid under the GDPR, taking into account the subordination link existing between the employer and its employees.

The draft Guidelines exclude the monitoring by employers of the use of company cars by their employees from its scope of application. In the latter case, the employers are controllers and they are relying on the equipment installed in the cars by or on behalf of the leasing companies acting as processor.

However, it may also happen that some data are collected directly by the car leasing company for the monitoring of the vehicles of which it is the owner. In that case, the company is the controller. It has often no relationship with the drivers as it deals directly with its customer which is the employer of the drivers. Given the tripartite relationship and where the use of a company car is necessary for the employees for their working activities, their consent may not be valid as it may not be freely given within the meaning of Article 7 of the GDPR.

2.2 Legitimate interest as an alternative legal ground

As a result, given the leasing context thereof, a more realistic alternative to the use of consent as a legal ground for the processing of personal data in the context of connected vehicles would be to rely on the legitimate interests referred to in Article 6(1)(f) of the GDPR.

In that respect, it is worth noting that the Article 29 Working Party ("**WP 29**") published an opinion on data processing at work on 8 June 2017. In that opinion, it considered that employers may rely on their legitimate interest for processing of personal data collected through vehicle telematics (par. 5.7). This opinion was in line with an earlier opinion, wherein WP 29 held that employers may rely on their legitimate interest for processing vehicle telematics data (Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices p. 14).

Furthermore, in the context of the Internet of Things, another WP 29 Opinion acknowledges that processing of personal data of connected device's users can be justified by legitimate interests (Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, p. 15). While, according to this opinion, a processing may not merely be justified by the economic interest of the stakeholder, other interests may come into play for the processing to be lawful. In that respect, it is important to note that the processing of data collected through connected vehicles responds to a range of interests. These include increasing the security and health of drivers, preventing accidents, detecting car theft, combatting insurance fraud, etc.

In the latter respect, Recital 47 of the GDPR recognizes that "*the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned*". Requiring the user's prior consent for processing personal data collected through car telematics and the subsequent right of withdrawing such consent would jeopardise these legitimate interests with significant societal impacts (including forcing insurance companies to raise premiums to compensate the loss incurred as a result of frauds), making such interests even close to a public interest.*

Transmitting personal data to third parties: The EDPB recommends in para.95 that "the data subject's consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller". A distinction should be made between transmission of data to third parties for the purposes of carrying out electronic marketing communications (which indeed requires consent of the individual) and transmission for other various purposes for which the legal ground can be one those stated in Art. 6 GDPR. The recommendation in para. 95 makes no distinction between such types of transmissions and is in practice unfeasible. Moreover, it is contradictory to the EDPB's statement in para.93, where the guidelines note that "the data controller may transmit personal data to a commercial partner, to the extent that such transmission is based on one of the legal bases stated in Art.6 GDPR".

It is apparent from the above references that there are circumstances where it is permitted to process data originating from connected vehicles with the legitimate interest as a valid legal basis. This further validates the point that personal data processing through telematics does not necessarily fall under the above Article 5(3), the scope of which should be further assessed, fine-tuned and adapted with more granularity than set out in the current draft Guidelines.

We therefore invite the EDPB to re-visit its Draft Guidelines, allowing more flexibility, assessments on a case-by-case basis, and considering the legitimate interest as an appropriate alternative to consent in this context.

3. **On the lack of clarity of scope of the draft guidelines**

Notwithstanding the foregoing and should the EDPB not be convinced by our above arguments to demonstrate that the Draft Guidelines should not apply to all connected cars and mobility related applications, a general clarification on the scope of application of the Draft Guidelines would be welcome.

a. Point 19, the sentence "The scope of this document focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects" seems to indicate that the Guidelines could have a broader scope than the personal data processing in relation to the non-professional used of connected cars. Point 30, the Guidelines also state "This is a non-exhaustive list". This create some legal uncertainty as to which services are covered by these Draft Guidelines and what is the scope of the same.

b. More importantly, the rationale to separate what falls within or outside the scope of the Guidelines can sometimes be unclear. For example, point 27 states, without more explanation, that data collected by the GPS are covered by the Guidelines but other types of applications, including those using geolocation, are not. Similarly, point 32 details that passive tracking is not covered by the Draft Guidelines but it is unclear as to the reasoning behind this assumption.

In addition, under section 3 of the Draft Guidelines, and as already mentioned above, almost no consideration is given to the fact that the end user is not always the client and the service provider is not always in direct contact with the end user. For example, the "Pay How You Drive" case study (point 103) focuses entirely on cases where the policyholder is the end user and is in direct contact with the insurer, then perceived as the service provider. Although we understand that the case studies cannot draw an exhaustive list of services which are considered by EDPB as falling into the scope of the e-Privacy Directive, car leasing companies are left with very few guidelines applicable to the service they might provide to end-users of cars leased by their employers.

4. <u>On the lack of proportionality between unrealistic requirements to data controllers and risks for data subjects</u>

The Draft Guidelines' aim of protecting personal data is often set out in a way that is wholly disproportionate to the potential risks posed by use of these personal data, in light of both the way in which the ability to use these personal data was obtained (on a voluntary basis) and the nature of the data in question. For example, paragraph 176 would require leasing companies to delete data stored on the car's dashboard after every customer finishes using the vehicle. These data are entered by a customer on a purely voluntary basis and are entered solely for the customer's convenience (for example if they opt to connect their mobile device to the car, or use the vehicle's infotainment or navigation systems).

As already mentioned above and in addition to the problems posed by paragraph 176, the Draft Guidelines do not take into account cases where a vehicle user is not also the sole user of the same (*eg*. when a car sharing service is provided to an employer for its employees usages of the car, how could we consider that the unfair wear and tear of a vehicle at the end of the leasing period would be a personal data).

<u>Specific considerations with respect to the insurance telematics</u>

Data subject's control over their data: The draft guidelines state in para.74 that "the data subject should be able to control how their data are collected and processed in the vehicle". We agree with the EDPB's concerns, however, some of the statements proposed in para.74 could only apply in accordance with the terms and conditions of the insurance contract. For example, the paragraph notes that "data subjects should be able to delete permanently any personal data before the vehicles are put up for sale". In this regard, the EDPB should clarify that only personal data stored in the vehicle application/mobile phone can be deleted. Data provided for the performance of the contract may be subjected to a different retention period.

More importantly, the statement in para.74 contravenes how insurance telematics works in practice. This is because data retention is often required after the expiration of a contract and/or where a data subject may request its deletion to enable the insurer to (i) handle/defend claims (deleting all data could fuel fraudulent claims); (ii) respond to complaints. Again, this is not only critical for the functioning of the product as such but also a requirement to comply with conduct regulation rules.

Hybrid processing: The draft guidelines state in para. 75 that "while it is not always possible to resort to local data processing for every use-case, hybrid processing can often be put in place". Moreover, the guidelines note in para.75 that the data is to be processed inside the vehicle or by the telematics service provider, generating scores that should be transmitted to the insurer at predefined intervals, ensuring compliance with the principle of data minimization.

To ensure an adequate performance of PAYD policies, it must be possible to transmit the score to the insurance undertaking at shorter intervals. It should be noted that transmission intervals are contractually agreed with the policyholder. Importantly, being able to transmit at short intervals means that the driver can see how they have driven after each ride, something that has a positive impact on road safety. If only long intervals between the transmissions of the score values are allowed, the insurance customers would be deprived from the spontaneous evaluation experience, a requested feature by customers.

Moreover, the EDPB has formulated the principle of data minimization in para. 75 too narrowly. It is unclear in the paragraph who can be considered a telematics service provider. It is currently not apparent, if the term "telematics service provider" encompasses vehicle manufacturers or the providers of the electronic communication services through which the data are transmitted. It might also mean that according to the EDPB the telematics infrastructure must be provided by an independent third party, which is not always possible. Unless the EDPB clarifies who can be considered a telematics service provider, companies might not be able to properly conduct "hybrid processing" as envisioned by the EDBP.

Additionally, it should also be possible for raw data to be transferred to a processor commissioned by the insurer. The processor could process the data into a score and transfer it to the insurer. This would also be an effective way to ensure data minimization.

6. MISCELLANEOUS

Disabling data collection: The EDPB notes in para.88 that "drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, except if a specific legislation provides otherwise or if the data are essential to the critical functions of the vehicle".

However, telematics insurance contracts rely on the concept that risks are correctly assessed by analysing driving behaviour. If the driver is able to temporarily stop the collection of data, it would not be possible to determine fair insurance premiums.

Comments on the case study on pay as you drive (PAYD) insurance:

Limitations to access raw data: the draft guidelines recommend limiting insurers' access to raw data in para.108 to prevent the creation of precise profiles of the driver's movements. This limitation is also suggested in para.74. However, access to raw data remains essential to provide fair pricing for PAYD insurance. More importantly, the insurer needs access to at least one identifier (eg name, VIN) to be able to provide the insurance cover.

Furthermore, the EDPB's interpretation on insurers' access to raw data can have a serious negative impact on competition and innovation in the motor insurance market, and impact insurers' ability to comply with regulatory requirements:

- The EDPB's view suggests a uniform approach to risk scoring. This is a concern as it would lead to a market where risk is viewed exactly the same by all insurers, with the consequent impact on free competition and European competition Law and policy;
- It would result in the lack of direct access to raw data for insurers which would restrict the ability to create accurate risk models and algorithms, with the consequent negative effect on the quality of the insurance product;

- If a scoring algorithm has been developed by a third party, the insurer will be required to understand the raw data that has been used to create that score to ensure that it is meeting its obligations from a regulatory, contractual and data protection perspective (e.g. to ensure fair customer outcomes) and;
- Raw data must be regularly audited and reviewed for accuracy and relevance - this is necessary to comply with both data protection and financial services regulations. The inability to access raw data impedes insurers from complying with legal obligations.