CLEPA comments on the European Data Protection Board's guidelines (1/2020) on processing personal data in the context of connected vehicles and mobility related applications

General comments

CLEPA welcomes the publication of the EDPB's draft guidelines. Vehicle connectivity is increasing at a steady pace, changing both how cars are used and business models in the automotive sector. The European automotive suppliers, which CLEPA represents, are committed to ensuring a high level of personal data protection, in line with the GDPR and ePrivacy legislation. As such, we welcome the EDPB's initiative to work towards a common understanding of how personal data protection rules should apply in the particular context of connected vehicles and mobility services.

Nevertheless, we believe that additional stakeholder consultations are necessary before the EDPB moves to a final version of the guidelines, given that, from our point of view, both the guidelines' scope and some of its definitions require clarification. We are also concerned by the fact that ePrivacy rules are currently being revised, and the guidelines should be aligned with the provisions of the new ePrivacy Regulation, rather than the current legislation, to ensure legal certainty. CLEPA is keen to work with the EDPB to provide expert feedback and help foster a pragmatic framework for the protection of personal data in connected vehicles and mobility services.

More specifically, we are concerned with the unnecessarily high burdens that would be imposed on mobility service providers, should the guidelines be adopted in their current form, stifling innovation and making services based on data from connected cars very difficult to realise in practice, at a time when the European Commission is instead keen to increase data flows (European strategy for data) and to support the development of the Internet of Things (IoT). The extremely wide definition of personal data, together with the restricted ground of processing – which implies that consent is required for almost any type of data transfer from the vehicle – would make connected vehicles and smart mobility almost impossible in practice, due to the burdens it would create for third-party service providers.

Specific comments and requests for clarification

1) Scope

Non-commercial use of connected vehicles, company cars, commercial vehicle fleets:
CLEPA agrees with the EDPB that company cars and commercial vehicle fleets should not fall under the scope of the present guidelines. To include them would add undue burdens on telematic service providers and fleet managers.

CLEPA welcomes the EDPB's focus on the non-professional use of connected vehicles. However, the draft would benefit from some clarification by confirming the exclusion of data processing in the context of professional use in paragraph 19, and by stating that the guidelines will apply to the list of stakeholders in paragraph 30 insofar as they have a direct relationship and/or can identify individuals from the data they may collect from connected vehicles.

Mobile applications:
With regards to mobile applications, the guidelines should only cover such vehicle companion mobile applications that actively support vehicle functionality. The guidelines state that mobile applications that contribute to the vehicle's connectivity capacities are included in the scope, even when these applications don't effectively rely on the transmission of vehicle data. Paragraph 27 makes a distinction between in-scope applications: GPS navigation applications are in-scope while applications suggesting places of interest to drivers should fall outside scope.

These criteria seem to be discriminatory and unclear. It causes unnecessary confusion as many mobile applications collect location data to find information about a person's surroundings and suggest places of interest, while at the same time such applications often also offer GPS navigation functionality to get there. For example, according to the guidelines, the TripAdvisor app would not be in scope as it suggests places of interest, yet the app also offers users turn-by-turn GPS navigation for users to reach their selected restaurant. Should the Tripadvisor app then be considered covered by the guidelines?

This lack of clarity will cause confusion as many applications have functionalities to collect location data and movement. There doesn't seem to be a justification to bring in scope GPS navigation applications which don't establish a connection with a vehicle or rely on vehicle data at all (e.g. removable standalone GPS navigation devices, or mobile phones' GPS apps). Therefore, CLEPA believes that the EPDB should redefine the scope in a sense that the guidelines only cover mobile applications that actively support vehicle functionality by exchanging data with or receiving data from a connected vehicle.

Safety systems:
Finally, the draft guidelines' scope does not properly take into account specific safety-related regulations (for example, the recently adopted General Safety Regulation and its delegated and implementing acts). In particular, the guidelines target biometric data, but do not consider that their collection may become mandatory for safety reasons (e.g. alcohol interlock devices, drowsiness and distraction monitoring systems). The guidelines should give precisions on how personal data is to be processed in this particular context, or exclude them from their scope.

Compliance with other regulations:
Similar to the point above, fleet owners and vehicle manufacturers are required to demonstrate compliance with a number of regulations, including, for example driving time or real-time CO_2 emissions by sharing data which may be considered personal to regulators. The guidelines should give precisions on how personal data is to be processed in this particular context as well.

Legal grounds for processing, consent, and notice:
While the guidelines acknowledge the practical and legal challenge that a systematic collection of consent can bring, especially regarding commercial vehicles, we believe that they should also offer real solutions or guidance on how to address these difficulties. In our opinion, the guidelines should acknowledge that getting consent systematically will not always be possible and that alternative legal options should be explored. This is especially the case for used vehicles which change owner after a period of time, or for when services providers cannot be in contact directly with the vehicle driver but only with the vehicle owner. Contractual requirement and legitimate interest should be accepted alternatives in this case. We elaborate on this more under the GDPR compatibility chapter below. In addition, it would be helpful to recognise that, in some scenarios, provision of notice may not be possible or disproportionate, and suggest alternative approaches, as outlined in Article 14(5b) GDPR, e.g. where a service provider has no direct relationship with the driver of a connected vehicle.

2) Definitions

Data subjects:
The guidelines seem to imply that connected vehicle data already qualifies as personal data when it concerns or can be associated with the driver, passengers, or anyone else who can be linked to a car, such as car owners and renters. However, the range of data subjects should always be limited to individuals who can be personally identified with connected vehicle data. The definition of personal data in Article 4(1) GDPR – and more in particular the notion of (in)direct identification – should remain crucial to determine this. The inconsistencies in terminology should be eliminated by taking the definition of personal data in Article 4(1) GDPR as a starting point.

This is especially relevant in certain situations where some individuals in a vehicle would qualify as data subjects while others would not. For example, when technical vehicle data linked to the Vehicle Identification Number (VIN) is collected, this data can be considered personal data as it can be used to identify the car owner directly, however this does not necessarily apply to passengers or an occasional driver. When the passengers and an occasional driver cannot be (in)directly identified, they should not qualify as data subjects at all.

The guidelines do not provide enough guidance regarding such situations. Clarification is essential, especially considering other privacy topics such as the processing of data from minors, the execution of data subject rights, and the quality of consent.

In summary, connected cars create challenges when it comes to identifying the data subject. The driver, passengers, vehicle owner(s), or even passers-by who may be detected by the vehicle's outside cameras or sensors, cannot always be identified or distinguished from each other. The guidelines don't provide sufficient clarity to define the exact scope of data subjects based on the GDPR definition of personal data. Hence, implementing an adequate consent mechanism doesn't seem feasible.

Data controllers:
CLEPA would like the EDPB to provide additional explanation on service providers as data controllers. Paragraph 38 of the draft guidelines mentions that "data controllers can include service providers that process vehicle data to send the driver traffic-information, eco-driving messages or alerts," without further explanation.

We would like the EPDB to clarify that this statement is only applicable when service providers determine means and purposes of processing personal data (e.g. when they have a direct contract or commercial relationship with the data subject), to differentiate from situations where service providers act as a data processor and thus process vehicle data on behalf of another party who is the data controller (e.g. the car manufacturer or equipment provider).

More generally, CLEPA would welcome clarification on the definitions of data processor and data controller, in the specific context of connected vehicles and mobility services. Vehicle manufacturers are likely to mainly act as data controllers, with consequences in terms of responsibility and liability. The guidelines should bring clarity on whether and how third-party service providers may act as data controllers.

Technical data as personal data:
We stress that technical data need to remain by default readable by OEM technicians or independent repairers through the OBD (on-board diagnostics) port, even if that data is considered personal, in order for the vehicle to remain fixable. Technicians must be able to access the data of a vehicle to diagnose the vehicle and provide maintenance/repairs. This means that while consent may be refused for the transmission of data remotely, the data will remain physically accessible anyway in the garage or repair shop: the EDPB may want to provide guidance for such scenarios.
Overall, the draft guidelines deem that most of the data generated by and associated with connected vehicles will be considered personal data because it would relate to drivers or passengers. However, this position fails to recognise a wide range of scenarios where this may not be the case. It would be helpful for the guidelines to emphasise the GDPR definition of personal data: this should include highlighting that, in order to define personal data, consideration should be given to the "means reasonably likely to be used to identify an individual"[1] and recognise scenarios where a service provider will not be able to identify an individual from the data received.

Downgraded mode:
To avoid misunderstanding, additional clarification of how the EDPB defines a "downgraded mode" in paragraph 91 would be welcome.

Anonymisation and privacy by design:
CLEPA would welcome a more granular position from the EDPB on anonymisation and pseudonymisation. For instance, VIN numbers could be used for pseudonymisation purposes, if they are kept separate from personal identity details.
It would be helpful to clarify any distinction between personal data processed/anonymised "on the vehicle" vs "outside of the vehicle." The draft guidelines do not consider the scenario where the only processing of personal data by a controller is to anonymise it and, in such a case, what obligations fall on the controller. This scenario is foreseen by Article 11 GDPR and applies also to connected vehicles, when a controller processes personal data but does not need to identify data subjects. In the context of location data and alerts emitted from devices installed in connected vehicles, anonymisation plays a key role in protecting users. Anonymisation could be achieved via techniques that remove single vehicle identifiers and full journey details. This represents a best practice and effective safeguard to prevent identification, surveillance, or potential misuse of data. In particular, technical data can successfully be anonymised or be anonymous from the start. Such data can include, for instance, performance statistics related to a car's braking systems, where any identifying piece of information is either not collected or stripped out immediately after collection, ensuring that only non-personal data is processed. This also applies to other examples provided in the draft guidelines, such as engine temperature or tyre pressure.

Connected vehicles:
The EDPB mentions connected vehicles in general. This might lead to the impression that connected bikes, e-scooters, or other such vehicles are also included. CLEPA asks for clarification that connected vehicles is limited to automotive vehicles (i.e. passenger cars, light trucks, busses, and trucks & trailers).

[1] CJEU Patrick Breyer v Bundesrepublik Deutschland (C-582/14) and GDPR recital 26: the test for whether a person is identifiable depends upon "all means reasonably likely to be used" to identify the person, i.e. a test of likelihood, not simple possibility.

3) Compatibility with GDPR, ePrivacy directive

CLEPA is concerned that the draft guidelines contain a number of inconsistencies or outright incompatibilities with the rules set out by the GDPR and the ePrivacy Directive. In addition, as mentioned above, the latter is set to be replaced by the ePrivacy Regulation, raising risks with regards to legal certainty. The draft guidelines should be extended to provide more practical guidance on how to cover alternative and equally valid lawful bases of processing under the GDPR (and potentially the future ePrivacy Regulation), such as contractual requirement and legitimate interest.

GDPR:
Section 1.5.3 of the guidelines would benefit from a revision as it currently conflicts with Article 6 GDPR on the possibility to select legal grounds other than consent for further processing, or use the compatible purpose test.

According to the ePrivacy Directive, when data is collected on the basis of informed consent as required by Article 5(3), or if one of the exemptions under that article applies, it can be further processed only if the controller either seeks additional consent for this other purpose, or if the data controller can demonstrate that it is based on a Union or Member State law to safeguard the objectives referred to in Article 23(1) GDPR. However, this interpretation is too strict and ignores the alternative legal grounds set out in Article 6 GDPR.

The EDPB appears to consider that further processing on the basis of a compatibility test according to article 6(4) GDPR is not possible as it would "undermine the data protection standard" of the ePrivacy Directive. In paragraph 51 of the guidelines, the EDPB also recalls that initial consent will never legitimise further processing as consent needs to be informed and specific to be valid.

The EDPB seems to equate the "data subject" from the GDPR to the "user" from the ePrivacy Directive. This further increases the conflict regarding relevance of both regulations. It is not clear who is to be seen as the "user" able to provide consent. This blur and lack of further guidance also includes security relevant data processing. It is recommended to use only terminology from the GDPR.

In our opinion, the following comments can be made to with respect to paragraph 50 of the guidelines:

- **Additional consent.** The guidelines do not sufficiently elaborate on how additional consent by the various players in the ecosystem can be arranged. In elaborating on this, it would be helpful if the EDPB could provide guidance on how to arrange consent in an effective and user-friendly manner. Specifically, we request the EDPB to address the issue of end-users possibly being overloaded with requests to provide consent, as this can lead to a situation where consent request information is no longer read, and the protection offered by consent is undermined.

- **Parties involved.** The guidelines do not elaborate on the interplay between different parties in the ecosystem surrounding connected vehicles. As highlighted above, although most consumers associate a connected car as one single product with one service provider, which usually will be the car manufacturer, connected vehicles in fact are comprised of several services offered by several service providers. Connected vehicles almost always involve cross-industry collaborations, most commonly collaborations between automotive and original equipment manufacturers, telecom providers, mobile network operators, and technology companies. However, not all industry players and collaborations have the same role from a

data protection perspective, and not all such service providers can obtain and store a sequential informed consent. In addition to different players, different communications mechanisms (machine to machine, vehicle to vehicle, vehicle to infrastructure) are another complicating factor. The suggested consent scheme would be too static and cumbersome, the complexities of high-frequency data management making it virtually impossible to obtain valid consent in certain scenarios. Furthermore, it is neither feasible nor sensible to provide users with just-in-time choices as this could prove unsafe while driving a vehicle. We therefore advise the EDPB to give attention to this issue in the revised version of the guidelines. In this respect, we recommend mapping the ecosystem and its players and their roles in the context of connected vehicles.

- **Compatibility test.** Article 6(4) GDPR defines the factors to be taken into account in order to determine whether further processing for another purpose is compatible or not with the original purpose for processing (see also article 5(1)(b) GDPR). According to the draft guidelines, the compatibility test is not suited at all for further processing in the context of connected vehicles. However, the guidelines do not justify this ruling out of Article 6(4) GDPR, but only refers to the "data protection standard" of the ePrivacy Directive, which we assume refers to the requirement of consent. Although the standard of the ePrivacy Directive is informed consent, in our view this does not stand in the way of a compatibility test to be performed for the further processing based on a different legal ground. We therefore ask the EDPB to explain why the performance compatibility test should be excluded as an instrument to assess further processing.

- **Legal ground.** The guidelines do not refer to any of the legal grounds mentioned in Article 6 GDPR (e.g. performance of a contract or the legitimate interest of the controller) other than consent. The Article 29 Working Party (the EDPB predecessor), in its opinions on IoT (2014) and smart devices (2013), saw room for the applicability of other legal in the context of connected devices. If the EDPB no longer sees such room when it concerns personal data processing in the context of connected vehicles, a justification would be welcome. We would like the EDPB to elaborate on why the other grounds would not be suitable anymore in the context of connected vehicles.

ePrivacy Directive:
CLEPA believes that terminology introduced by the applicability of Article 5(3) ePrivacy Directive (e.g. consent requirement and exemptions therefrom) cannot be applied to connected vehicles.

Section 1.2 of the guidelines states that the ePrivacy Directive sets a specific standard applicable to all actors in the context of connected vehicles that wish to store information or access information stored in the terminal equipment of a subscriber or user in the European Economic Area. The section refers to the applicability of Article 5(3) ePrivacy Directive, which stipulates that the storing of information or the gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given their consent. We advise that the guidelines provide more insight on how the definition of "subscriber" and "user" must be interpreted in the context of connected vehicles, and clearly assess whether passengers are also to be considered as subscribers or, at least, users.

The guidelines conclude, without clear explanation, that all actors in the context of connected vehicles that wish to store information or access information stored in the terminal equipment of a subscriber or user must obtain a prior informed consent. The guidelines also refer to the exemptions from the

informed consent requirement. Informed consent requirement is not required under two exemptions detailed in paragraph 17 (for the sole purpose of carrying out transmission of a communication over an electronic communications network; when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service).

In our opinion, the following comments can be made to with respect to section 1.2 of the guidelines:

- **No examples of the technical features and technologies used.** We ask the EDPB to provide examples of the technical features and technologies used on the context of connected vehicles to clarify why, to whom, and under which circumstances Article 5(3) ePrivacy Directive applies.

- **Terminal equipment.** The guidelines do not explain why, in view of the definition of terminal equipment (given under Article 1(a) Directive 2008/63/CE), the connected car and in particular every device connected to it will always qualify as terminal equipment. It would be helpful to have a better understanding of the EDPB's assessment underlying this assumption. For now, it remains unclear which IoT devices fall in the scope of the guidelines. For example, police authorities may also gain direct access to vehicle data. In this respect, the guidelines would also benefit from elaboration on the meaning and limitations of the term "connected to it." Another example is an engineer using a tablet to get access to vehicle data to perform mechanical repairs, this data subsequently being sent via an app to computers of the garage exploiting the workshop for reporting purposes. Which devices are connected to the car and qualify as terminal equipment in this scenario? It would be practically impossible to implement a consent mechanism in case the computer of the garage would also qualify as terminal equipment of vehicle data.

- **Storage and access of information.** The draft guidelines currently lack a detailed description of the technical features and technologies used in the context of connected vehicles. In our view, they should assess:
    - How information is stored or accessed, and therefore to what extent Article 5(3) ePrivacy Directive applies; and
    - To what extent the features exclusively involve machine-to-machine communication, which is currently not automatically covered by Article 5(3). Moreover, according the second draft of the proposed ePrivacy Regulation, the Regulation should not apply if the transmission of machine-to-machine or IoT services is carried out via a private or closed network, such as a closed factory network. Can the EPDB explain, for example, whether communication between autonomous driving vehicles is exempted (machine-to-machine transmission within a closed network), or automated synchronisation of information between devices?

- **Article 5(3) ePrivacy Directive: the 'cookie-article.'** Historically, Article 5(3) primarily aims to cover cookies and related technologies in the internet/telecom sector, such as Java scripts and web-based threats (spyware, viruses…). The scope of Article 5(3) should therefore not be automatically and indiscriminately expanded to connected vehicles. We urge the EDPB to explain and differentiate the technical features and technologies relating to connected vehicles.

- **Addressees.** With respect to the addressees of Article 5(3) ePrivacy Directive, in most EU Member States the responsibility for complying with the informed consent obligation lies with

the person responsible for storing information or gaining access to information stored in the terminal equipment. However, this addressee is not necessarily the entity that is also responsible for providing the services in the context of connected cars. Although most consumers associate a connected car as one product with one service provider, which usually will be the car manufacturer, connected vehicles are in fact comprised of several services offered by several service providers. In view of the different actors, it would be extremely helpful if the guidelines could provide guidance on how the informed consent required under Article 5(3) can be obtained in such a diverse landscape of stakeholders. We urge the EDPB to also put forward possible solutions for the challenge of obtaining valid consent in this regard.

- **Exemptions.** The guidelines name the exemptions from Article 5(3) ePrivacy Directive but do not seems to address the applicability or relevance of the exemptions in the context of connected vehicles. We would welcome details on how the exemptions must be construed in the context of connected cars, to enable automotive suppliers to assess whether and to which extent they could benefit from these exemptions. For example:
    - With respect to the first exemption, the transmission of a communication over an electronic communications network merely aims at websites being able to have proper functionalities for users. The guidelines do not provide considerations on how this exemption could be relevant for connected vehicles.
    - With respect to the second exemption, the guidelines do not elaborate on whether and which services provided in the context of connected vehicles can be regarded as an information society service. An information society service is defined in Directive (EU) 2015/1535 and relates to the concept of any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of service. We recommend the EDPB to elaborate specifically on how this could be relevant in the context of connected vehicles and to provide specific examples in this respect, in particular addressing less clear-cut situations, for example when the user synchronises route information through a web application.

4) Cloud processing vs local processing

CLEPA agrees that in-vehicle processing has important advantages, and supports the EDPB's view that local processing of personal data can be a beneficial option with regards to privacy and personal data protection. However, the guidelines should also make clear that cloud processing is possible, in section 2.4.1.
The EPDB's approach should not stifle innovation and the development of user-centric cloud-based services. For example, drivers may benefit from receiving seamless and instant map, traffic, and other software updates. When cloud processing is used, it is possible to take into account GDPR and privacy-by-design principles to design a solution that protects personal data.

CLEPA, the European Association of Automotive Suppliers, represents over 3,000 companies supplying state-of-the-art components and innovative technologies for safe, smart and sustainable mobility.

CLEPA brings together over 120 global suppliers of car parts, systems, and modules and more than 20 national trade associations and European sector associations. CLEPA is the voice of the EU automotive supplier industry linking the sector to policy makers.

- The automotive sector accounts for 30% of R&D in the EU, making it the number one investor.
- European automotive suppliers invest over 25 billion euros yearly in research and development.
- Automotive suppliers register over 9,000 new patents each year.
- Automotive suppliers in Europe generate five million direct and indirect jobs.

CLEPA

Cours Saint-Michel 30G, 1040 Brussels

www.clepa.eu

Twitter @CLEPA_eu

For more information, please contact: info@clepa.be