大成 DENTONS

European Data Protection Board

Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

(Version 1.0 – Adopted 28 January 2020)

(the "Guidelines")

Submission on behalf of **Avis Budget Group**

3 May 2020

1. Background

Avis Budget Group ("**ABG**") is a leading global provider of mobility solutions, operating three of the most recognised brands in the industry through Avis, Budget and Zipcar, the world's leading car-sharing network.

Dentons UK and Middle East LLP act on behalf of Avis Budget Group in making this submission.

2. Introduction and overview

Firstly, ABG would like to record its thanks to the EDPB for the additional direction provided in the Guidelines and to acknowledge the importance of ensuring personal data and the rights of individuals are protected, particularly in the context of new and developing technologies such as connected vehicles.

This is an area of rapidly developing technology and a consistent, Europe-wide approach to addressing the privacy issues such technology raises is welcomed.

Whilst it is our view that the Guidelines include some helpful clarifications and, we hope, will lead to improved consistency across many of ABG's markets, there are a number of concerns with the Guidelines as currently drafted. We are concerned that the Guidelines in their current form will lead to regulatory approaches and expectations that do not fully consider the varying data processing activities undertaken across the spectrum of connected vehicle use cases and mobility service business models.

In particular, our view is that the Guidelines are currently too focussed on data subjects' use of connected vehicles where the driver/user is the owner of the vehicle (the "owner-driver" scenario). In certain areas this results in an unduly restrictive interpretation of the requirements of GDPR and the ePrivacy Directive[1] when applied to connected vehicle technologies in some scenarios.

This, in turn, leads to significant operational challenges in ensuring compliance with GDPR and e-Privacy Directive for vehicle rental and car sharing operators in accordance with the expectations set out the Guidelines. This potentially leads to the imposition of requirements which are disproportionate to the potential risks in the context of a number of connected vehicle 'use cases'.

In this submission, we have set out areas of the Guidelines that we believe would benefit from further consideration in the context of vehicle rental/car sharing models. Where possible, to aid finalisation of the Guidelines, we have proposed alternative considerations and interpretations that we believe represent a more proportionate and/or fairer allocation of responsibilities to achieve the objectives of the law in this area.

Our submission focusses on the following considerations that we believe would be beneficial to incorporate into the final Guidelines:

[1] Directive on privacy and & electronic communications (2002/58/EC as revised by 2009/136/EC)

- a recognition that the current Guidelines focus on a user-owner approach to the interpretation of the relevant legal requirements and the solutions that are available to address them and that a difference between user-owner and other ownership scenarios is appropriate and reasonable;
- the interpretation of the interface between the GDPR and the ePrivacy Directive adopted in the Guidelines is unduly restrictive; and
- a number of the current recommendations in the Guidelines present 'real-world' operational challenges in vehicle rental and vehicle sharing scenarios.

3. Considerations and Recommendations

3.1 Ownership-centric approach

The Guidelines primarily consider the relevant data privacy issues – and recommended solutions – in the context of a user-owner scenario. As a result, the Guidelines fail to consider how general positions or interpretations of these issues need to be adapted in cases where a vehicle user is not also the owner of that vehicle.

In such scenarios, it is often the case that the intended purposes for the use of the data collected about the connected vehicle is not as anticipated in the Guidelines. For example, such data is often not used in the context of impacting an individual or to gain any insight or information about an individual under a rental or sharing model.

A specific example of this issue relates to data regarding the 'wear and tear' of a vehicle (as referenced in paragraph 3 of the Guidelines' introduction). Connected vehicles will often permit rental or car sharing operators to collect this type of information during users' rental or car share periods. Whilst this could be used to infer information about an individual's driving style when reviewed over an extended period for an individual user of the vehicle, this purpose is much less relevant in other scenarios. Instead, in a rental or car share context, where this data is collected it is generally for the purpose of maintaining the operator's vehicle fleet.

This demonstrates that the Guidelines' aim of protecting personal data is often set out in a way that does not consider the operational reality of the car rental/sharing model (particularly in light of the limited potential risks posed by use of personal data collected in many circumstances in this model).

It would be appropriate that the Guidelines are revised to accommodate that the user-owner model is not the only scenario in which connected vehicles operate and to recognise that, as such, data collected from connected cars should not necessarily be considered as intrusive or facilitating detailed insights into any particular individual.

It would also be appropriate to frame the recommendations included in the Guidelines as applicable only to the user-owner model where they are intended as such.

In addition, the approach in the Guidelines results in an assumption that all data collected from connected vehicles is "personal data". This may be true in many instances in a 'user-owner' scenario where the data clearly relates to a specific individual – the owner of the vehicle.

However, it would be more appropriate to consider that in scenarios where actors other than the user have an ownership interest in the vehicle – such as rental or car-share scenarios - some information should be considered as relating to the vehicle rather than an individual where the

relevant processing purpose is not intended to relate to, or affect, the individual. Nuance in the Guidelines to recognise that such data may not be "personal data" and/or that the various requirements could be interpreted accordingly would be welcome.

3.2 Relationship and interpretation of the GDPR and ePrivacy Directive

We also have concern with the approach the draft Guidelines adopt in relation to the application of Article 5(3) of the ePrivacy Directive (the "**ePrivacy Consent Rule**") and GDPR. We believe that this approach results in unintentionally disproportionate restrictions when applied in circumstances other than in a traditional 'user-owner' arrangement.

Under the Guidelines car rental/sharing companies such as ABG would need to meet both the requirements of the ePrivacy Consent Rule and the relevant provisions under GDPR (which includes requiring any personal data being processed to have a legal basis under Article 6 GDPR). While potentially manageable in an 'user-owner' arrangement the approach adopted in the Guidelines presents significant challenges under the car rental and sharing business models.

An example quoted in the Guidelines demonstrates these challenges - the collection of vehicle's technical data (e.g. data relating to the wear and tear on vehicle parts) when used for vehicle maintenance and fleet management purposes.

It is recognised that, where collected from a connected vehicle, it is possible this information: (i) is collected from "terminal equipment" (meaning, according to the Guidelines, the ePrivacy Consent Rule would apply); and (ii) could constitute personal data under GDPR in circumstances where that information can be linked to an identified or identifiable natural person (for example, where a VIN is retained within rental records).

However, this is information that is collected from "terminal equipment" belonging to the rental/car share company rather than the driver (or user). We believe that this is an important distinction to bear in mind when considering how to interpret these requirements. It is also an important distinction when comparing the application of these requirements to other common scenarios where the ePrivacy Consent Rule applies, such as in the context of personal mobile or computing devices.

ABG needs to maintain and service its fleet of vehicles – a task that can be a significant operational challenge when applied across a fleet of thousands of vehicles. It also has a duty of care to ensure its vehicles are safe and roadworthy for its customers. ABG has a legitimate business need to ensure it does this in as efficient a manner as technology permits. Doing so allows ABG to ensure safety standards across its fleet and limits unavailability of vehicles to allow it to offer a competitive service to its customers.

The technical data collected and used for this purpose – to the extent it is personal data - causes no real intrusion into an individual's privacy and provides little (if any) insight or information about that individual. Understanding that a vehicle has reached a relevant service milestone during a particular customer's rental does not provide significant insight into that customer.

However, the approach of the draft Guidelines could be understood to permit the individual renter or customer the ability to prevent this information being collected and used for this purpose without their consent. The exemptions to the ePrivacy Consent Rule would not obviously apply in such a scenario (and, in any event, the Guidelines imply that consent would be the appropriate legal basis under GDPR in this scenario).

This clearly demonstrates the disproportionate outcomes and limitations on legitimate uses of innovative technology that could apply to rental/car sharing enterprises as a result of the Guidelines in their current form.

We recognise that these requirements may be more appropriate – and have more achievable methods of compliance - in an user-owner scenario. However, the lack of consideration in the Guidelines of other scenarios, in particular the car rental/sharing scenario, results in an unintentionally restrictive application of the ePrivacy Directive and GDPR.

It should also be remembered that the primary focus of the ePrivacy Directive is to provide more specific protection for the security of electronic communications made by or for the benefit of *individuals* over telecommunications networks. The principle policy aim of Article 5(3) of the ePrivacy Directive, in particular, was to extend that protection to information held on individuals' devices.

With this in mind, we propose that the Guidelines provide for greater flexibility and an ability to rely on other interpretations of how to comply with the ePrivacy Directive and GDPR so that, for appropriate data uses, collection of the driver's consent is only one of the possible methods that could be deployed to achieve compliance.

This would be in line with the previously stated position of the Article 29 Working Party in the context of the ePrivacy Directive that it would be appropriate to consider "*other circumstances in which consent would not be required, because the processing would have little or no impact on the right of users to protection of their communication secrecy and private life*"[2].

In particular, we propose that the Guidelines are amended to recognise the following:

A. Greater flexibility of interpretation of the approaches to the ePrivacy Consent Rule in car rental/share operations

A number of the uses of connected vehicles in the car rental/sharing sector do not relate to any benefit or service specifically related to the individual driver. Instead, it is intended to relate to, and support services received and used by, the car rental/sharing company. Maintenance and fleet management is one example of this.

The driver has not directly requested, and does not get any direct benefit from, the connectivity services forming part of the operation of the connected car in those contexts. Instead, they rely on ABG (and other rental or vehicle sharing operators) to manage this as part of their services. It is therefore not appropriate that the driver's consent should be required.

Therefore, the Guidelines should clarify that, in such cases, the ePrivacy Directive was not intended or designed to prevent the collection of information in these circumstances. Instead, it is intended to protect the collection of information from an individual's personal "terminal equipment" in circumstances where the user is both the owner and user.

---

[2] WP 29, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) (Adopted 19 July 2016)

This interpretation is supported by the drafting of Article 5(3) and its supporting definitions. In particular, the ePrivacy Directive requires consent when gaining access to information already stored in the "terminal equipment of a subscriber or a user" (emphasis added).

In these cases the driver is not "using a publically available electronic communications service" – it is the rental/car sharing company that is *using* the services. As such, the vehicle is not the "terminal equipment of ... a user". So it should therefore not be considered a scenario where user's consent is required.

And it may not be appropriate to consider the rental or car share company a "subscriber" in some such circumstances. This is because in some arrangements the relevant connectivity services associated with connected vehicle technology is obtained as part of a "packaged service" received from the vehicle OEMs (who, in turn, contract directly with the relevant telecommunications service provider).

So it should be recognised that the ePrivacy Consent Rule may not apply on the basis that the vehicle is the "terminal equipment" of neither "a subscriber or a user".

Alternatively, the Guidelines could accommodate compliance with the ePrivacy Directive in another way.

Article 5(3) permits the consent to be given by the "subscriber or user" (emphasis added). The Guidelines could recognise that, in relevant circumstances, it would be reasonable that a rental/car sharing operator can give the necessary consent(s) rather than the driver/user. This is an approach that has been recognised in guidance issued by Supervisory Authorities in other contexts relating to the ePrivacy Directive[3].

This could be combined with clarification that the connectivity service provided via vehicle OEMs (as opposed to a direct relationship with telecommunications providers) is in effect a "publicly available electronic communications service" to which the rental/car sharing company has contracted[4].

Given the above approaches to this issue that are available within the framework of the existing law, it is our view that the current consent-based model required in the Guidelines is too restrictive to apply to all connected vehicle use cases and should be adjusted accordingly.

---

[3] The UK's ICO has issued guidance that indicates that – in appropriate circumstances – it would be appropriate for an employer (as the subscriber) to give consent on behalf of an employee for the use of cookies on the employee's device. (https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules6)

[4] Without this clarification the definitional technicalities could be problematic as the car rental/sharing company would otherwise not be a "subscriber" as is required under the definitions. However, it is our view that this is a reasonable interpretation as, in general, these "packaged services" (including connectivity services) are available to the general public via the vehicle OEMs when buying private vehicles.

B. Applicability of ePrivacy Directive exemptions

While exemptions are included in Article 5(3) ePrivacy Directive for 'information society services' explicitly requested by users there are challenges in relying on this in the context of car rental/car sharing services.

This is a challenge arising due to the law, and its interpretation, failing to keep pace with the way in which technology is used to improve delivery of some traditional services. The so-called "market disruptors".

The intention of these exemptions is to permit processing where necessary to provide services/perform contractual obligations that are requested by a user without needing to rely on an additional consent that is, in effect, implicit within the request for the services.

As such, it is our view that it would be appropriate that the Guidelines – and the interpretation of these exemptions adopted by the EDPB – recognise that a similar approach can be applied in the context of technology-enabled business models where this supports relevant service provision (albeit that it may not be sufficiently ancillary to itself qualify as an "information society service").

This would help address the challenges that the current definition of "information society services" presents, including the approach that has been adopted in the Guidelines in the pay-as-you-drive use case which indicates that a consent is required in addition to reliance on the performance of a contract.

3.3 Operational Challenges

A number of the requirements set out in the Guidelines would pose significant challenges for vehicle rental and car sharing operators, including ABG, from an operational perspective.

Whilst ABG recognises that protecting individual's data requires responsible organisations to take appropriate measures, we have set out below four examples in the Guidelines that create disproportionate operational challenges.

A. Personal information stored on rental cars' dashboard (Section 3.5 Guidelines)

ABG notes a number of other submissions made in response to the Guidelines that have addressed this issue. It is supportive of the comments and views expressed in those submissions.

In addition, ABG would suggest that the Guidelines should be updated to incorporate the following points:

a. **Data subjects have control and provide personal data voluntarily**: Fundamentally, users have control over this data. All data stored on the car's dashboard by a customer is shared by the customer on a voluntary basis. None of the ABG fleet requires the input of this data to make use of the relevant vehicle. Customers are free to enter destinations in the GPS and/or connect their mobile device(s) with the car and therefore the customer has control over providing this data.

   Current arrangements put the user in control of the deletion and removal of this information from the vehicle dashboard. Instead of relying on a third party, such as a vehicle rental or car share operator, vehicle users have a self-service ability to delete

personal data from the dashboard of a connected vehicle. This gives the user, rather than a third party, direct control over their personal data.

There is a good level of understanding amongst ABG's customers about the functionality of dashboard features and the need for data to be deleted to protect any information from being visible following their rental period.

b. **Household exemption and identifying relevant controllers**: Customers are utilising the dashboard for their own personal uses. ABG does not access the dashboard of its vehicles to extract data during rental periods.

   Therefore, in the majority of circumstances, use of the dashboard will fall outside of the scope of GDPR under the personal/household exemption. This approach has previously been endorsed by the CNIL[5]. This should be recognised in the Guidelines.

   In addition, it should also be recognised that given the lack of control that rental companies have over the collection of this type of data it is not necessarily clear that they should be considered as 'data controllers' in respect of it.

c. **Nature of personal data and uses**: Data collected through the rental cars' dashboard is not likely to be intrusive into the privacy of any specific individual (and is very unlikely to include special category personal data). As discussed in more detail in the section below regarding Geolocation Data, given the limited duration of most rentals/car share periods this use is not likely to reveal patterns of behaviour or life habits in respect of the large majority of ABG customers.

   In addition, subsequent renters are highly unlikely to know the identity of the previous renters. Therefore, they will not be able to link the majority of any data left on the vehicle's dashboard to identifiable individual(s). So, for the large majority of any data that may continue to reside on a dashboard post-rental, the information does not pose significant risk. This data is not extracted from the dashboard by ABG for any purpose.

   In addition, in the large majority of instances much information stored on the customer's device (such as contacts and phone numbers) are not retrievable without the customer's device being present in the vehicle at the same time. So this naturally limits data that may be viewed by future renters.

   For all these reasons, there are practical limitations on the potential intrusion into the privacy of any individual renter that such information can cause. And, as explained below, there are operational challenges with the expectation that rental businesses can delete this information across a fleet.

d. **Practical challenges with data deletion**: It is ABG's view that the expectation that car rental companies will delete user data after each rental is disproportionate from an operational perspective. This is particularly true because of the nature of this information and the control that the renters themselves have over the data.

---

[5] Compliance Package: Connected Vehicles and Personal Data (October 2017) (https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf)

It is important that the EDPB are aware that, currently, a single button does not exist to delete all data on all connected vehicles. Vehicle manufactures are not required to include this functionality and it is not currently possible for other parties to carry out this deletion function remotely.

The method for deletion of data from a vehicle dashboard varies by make and model (and in some instances, between "trims") and can involve a number of steps to be taken to delete data. Whilst deletion by a user is feasible (requiring deletion from a single vehicle dashboard), this makes deletion at scale across an entire rental fleet after every rental/car share, operationally challenging.

The policy approach adopted by EDPB in the Guidelines would place a significant operational and financial burden on ABG (and other rental and car share operators).

Given the nature of the information and level of risk posed to users, a more reasonable expectation of such operators would be facilitating Customers' own deletion of any data e.g. providing a service message to prompt users prior to the end of a rental.

B. Tackling auto theft (Section 3.4 Guidelines)

ABG works very hard at protecting its business against auto theft across the globe. This is a real issue that ABG, along with many other rental and vehicle-share operators, need to address against often very sophisticated criminal organisations.

The Guidelines limiting collection of location data to the time of "the declaration of theft" and not continuously causes ABG a real-world challenge. In many cases, by the time theft is suspected, sophisticated and organised criminals will already have taken steps to disable or remove any location tracking device in the vehicle. In other words, at this point it is too late. This removes an ability for ABG to protect its assets

We therefore request the EDPB amend this case study (and in particular para 162 of the Guidelines) to accommodate scenarios where it may be reasonable and proportionate to collect location data prior to suspected theft provided such collection is subject to appropriate safeguards (such as technical and organisational measures in place to ensure limited access only once theft suspected and to ensure purpose limitation; appropriate retention/deletion etc).

C. Geolocation information

ABG recognises the sensitivity that applies regarding the collection and use of geolocation information.

However, we propose the following additional considerations are accommodated in the Guidelines to recognise that different concerns / approaches may be applicable in a rental or car share scenario:

a. The Guidelines identify geolocation information as a higher risk data collection activity. This is understandable in the context of a user-owner scenario or where information about a single driver is collected over a material period of time. However, the Guidelines should acknowledge that there are circumstances where it is unlikely/more difficult to determine life habits of individuals from geolocation data collected via a connected car e.g. short term holiday rentals. Therefore, geolocation information should not always "automatically" be considered high risk data and appropriate safeguards and measures could be adopted as appropriate.

b. Recognition that certain recommendations included in the Guidelines regarding geolocation data are not directly applicable where the purpose of processing are not intended for the purpose of connecting such data to the individual, but rather the connection is incidental to the processing activity or otherwise has minimal or no impact on individual (e.g., fleet utilization; locating a reported lost or stolen vehicle or identifying when they are entering high-risk locations such as ports etc; fuel and mileage; check out/in; etc.). It is these types of processes that are the most common uses of geolocation information by rental / car-share operators such as ABG. In such circumstances, adequate safeguards to prevent other uses of the geolocation data should be sufficient.

c. In addition, a blanket approach that limits the continuous collection of geolocation information may significantly impact on certain functionality that is intended for the benefit of the customer such as roadside assistance or accident reporting. A more nuanced approach to this recommendation should be adopted in the Guidelines.

D. Reliance on OEMs

ABG notes that the Guidelines include a number of technical measures that would assist privacy in connected vehicles and welcomes these suggestions.

However, as a vehicle rental and car share operator it does not have the direct ability to implement many of these technical features. We believe the Guidelines would benefit from clarity as to which actor is best placed to address these concerns.

In particular, many of the recommended privacy-enhancing measures are properly within the control of the vehicle OEMs and any specific requirements that the EDPB wishes to make of such OEMs in respect of connected vehicle technologies should be clearly directed as such.

From the perspective of ABG, these specifically include:

a. **Control/deletion of data** – ABG does not have the ability to install a 'privacy button' or similar technology in their connected vehicle fleet and cannot easily provide the ability for such controls to allow the deletion of driver's information (e.g. in-vehicle profile management systems).

b. **Transparency** – Notifications/transparency when geolocation is being tracked are controlled by dashboard functionality. ABG cannot determine what is displayed to drivers through the control panel when this functionality is active.

c. **Deletion of dashboard data** – OEMs control the process for deletion of data from the dashboard. As noted above, this process varies by make/model and involves differing mechanics and steps.

4. Conclusion

As stated above, ABG welcomes the increased clarity and guidance provided in the Guidelines but trusts that the above has clearly set out some the challenges and concerns that arise from the current draft.

We would encourage the EDPB to consider these observations and recommendations in the next draft of the Guidelines and would welcome the opportunity to engage further with the EDPB on these issues.

Dentons UK and Middle East LLP

3 May 2020