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

Leaseurope

The Voice of Leasing and Automotive Rental in Europe

Leaseurope, the European federation representing the leasing and automotive rental industries, supports the EDPB's goal of clarifying the implications of the GDPR and the e-Privacy Directive on the use of personal data in connected vehicles and mobility applications. Nevertheless, we believe the Guidelines in their current form will lead to further confusion on how the GDPR and ePrivacy Directive should be interpreted in this context. Moreover, we feel the interpretation set out in the Guidelines is not proportionate or necessary to achieve the EDPB's aim of ensuring citizens personal data is afforded a high level of protection, as set out under the GDPR and ePrivacy Directive.

Lack of Proportionality

The 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 this personal data. For example, paragraph 176 would require car rental companies to delete data stored on the car's dashboard after every customer finishes using the vehicle. This data is entered by a customer on a purely voluntary basis and is 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).

In addition to the voluntary nature of the customer's decision to make this data available, customers also fully understand the implications of doing so. It is reasonable to assume that the average customer is aware of the fact that this data can remain in the dashboard subsequent to their rental period. This, coupled with the fact customers are able to delete any data they consider to be sensitive (to the extent that this is allowed by vehicle manufactures) renders the obligation on car rental companies to delete personal data after every rental disproportionate and overly burdensome, particularly in light of the operational challenges this would create (see section 3 on operational problems).

It is pertinent to note that personal information stored on a customer's device (such as contacts and phone numbers) which has been synced with a vehicle is protected by the vehicle's built in security features, requiring the synced device to be present in order to access the data stored on the dashboard. It is also important to highlight that renters will not be aware of the identity of the previous renter, so in the event that personal data *does* remain on the dashboard, it will not be possible for the average renter to link this information to an individual.

In addition to the problems posed by paragraph 176, the Guidance fails to take into account how the *type* of relationship the user has to a vehicle user may impact whether or not data can be regarded as personal. The Guidance often appears to take an ownership-centric approach, and generally fails to recognise how this general position may need to be adapted

in cases where a vehicle user is not also the owner or sole user. This is problematic because in a number of cases, data that would be considered personal in the context of an ownership model is not personal under a rental or leasing model. A good example of this is the wear and tear of a vehicle (as referenced in paragraph 3 of the Guidelines' introduction) under a rental contract. Although this would generally provide information about an individual's driving style, in the context of car rental (and particularly short term rental), the high turnover of customers means that it is extremely difficult to trace this type of damage (general wear and tear) back to any individual customer. As a result of this, it is highly questionable whether this type of data could be considered "personal".

Lack of Clarity and Consistency: The relationship and interpretation of the GDPR and ePrivacy Directive

In addition to the lack of proportionality, a key issue with the Guidelines in their current form is the lack of clarity on which rules car rental and leasing companies should adhere to, and how these relate to each other. Under the current Guidelines then, car rental and leasing companies would need to meet both the requirements of the ePrivacy Directive (which requires prior consent for the storing of information or the ability to access to information that is already stored) and the relevant provisions under GDPR (which requires any information being processed that meets this criteria to have a legal basis under Article 6 GDPR).This need for a "double basis" may lead to confusion on how data controllers should be managing personal data, and ultimately go against the EDPB's aim of affording high standards of protection to personal data.

As noted in the Guidance itself (Paragraph 49), the classic means of obtaining consent do not necessarily "translate" well in the context of a connected vehicle, risking the possibility of low quality consent becoming the norm. The consequences of this are likely to be similar to users' responses to online cookies, where the vast majority of consumers simply choose to "accept all cookies" by default[1]. In the case of a leased or rented vehicle, this problem may be magnified, since drivers will likely be less inclined to fully evaluate which data they wish to grant access to given the shorter term use of a leased or rented vehicle vi-a-vis one that they own. In the context of a connected vehicle then (and in particular a leased connected vehicle) the traditional approach to obtaining valid consent is likely to greatly diminish the user friendliness of a vehicle, with very limited -if any- additional benefits to the customer.

Another notable consideration in this context relates to the recent proposal put forward by the Croatian Presidency for a revision of the ePrivacy Directive. If adopted, this proposal would include "legitimate interest" as a legal basis for processing personal data, providing the fundamental rights of the end user are not compromised. In order to ensure consistency- and that the Guidelines do not conflict with potential changes to the future framework- the Guidelines should drafted in a way that aligns with the new proposal. One notable example of a situation where "legitimate interests" already over-ride the general provisions of the ePrivacy Directive is in the context of the eCall Directive, which allows emergency services the ability to access a user's geolocation in the event of an accident.

In addition to the aforementioned issues, another major problem with the Guidance in its current form is the arbitrary distinction made between the requirements for traditional car rental and leasing companies versus peer-to-peer rental. Car rental and leasing companies are required to comply with the requirements set out in the GDPR and the ePrivacy Directive,

[1] Utz, Degeling *et al*. "(Un)informed Consent: Studying GDPR Consent Notices in the Field" (October 2019)

whilst peer-to-peer rental companies, who purport to offer the same services and who's customers' personal data is used in the same way- are never explicitly referred to in the Guidance. This not only undermines the effectiveness of the GDPR and ePrivacy Directive, it also goes against the Commission's broader goal of legislating on activities as opposed to individual sectors, and ensuring legislation operates in the same way regardless of the channel/means of providing a service.

Operational Problems

A number of the requirements set out in the Guidelines would pose obstacles from an operational perspective. For example, the Guidance suggests that it is possible to cordon off technical and non-technical (personal) data, and that technicians responsible for repairing a car for example should only be granted access to technical data (paragraph 57). This is not feasible operationally; a vehicle's data management architecture does not -by default- make a distinction between personal and non-personal data.

In the context of rental and leasing in particular, the Guidelines also raise a number of specific problems. For example, in (shared) company cars it is important to be able to track who uses the car (and for what distance) for tax purposes. In this context, allowing a driver to unilaterally withdraw permission to track their distance travelled would have implications for the other drivers using that car. By way of example, if driver A and driver B use the same car, giving driver B the ability to delete all of the data on the vehicle would have implications for driver A. It may prevent driver A from being able to get an accurate reading of how much kilometres they have travelled for businesses purposes, which is important to ensure they are able to use this information for tax purposes.

As previously referenced (in the proportionality section) the requirements for leasing and rental companies to "wipe" the users data after every hire is disproportionate to the potential risks associated with this data being left on the vehicle, particularly given that a lesee or renter is able to delete this information if they wish. In addition to the lack of proportionality however, this requirement is also problematic from an operational perspective. Currently, a single button does not exist to wipe all data on all vehicles since OEMs are not required to include this functionality.

Moreover, it is not possible to carry out this "wiping" function remotely, so enforcing this requirement would work to stifle innovation in the rental and leasing sectors, since the free floating car sharing business model would no longer be feasible due to the practical problems associated with requiring rental and leasing companies to have a worker within a reasonable distance of all cars being rented at all times. The Guidelines' provisions on geolocation would also put this business model at risk, since the nature of the business requires this information to be available to the rental company at all times in order to manage the fleet.

Liability Issues

With regards to liability, it is important to note that in many instances the leasing and rental companies are simply not in a position to access, process or even be aware of the fact that data has been transferred/entered by a user, and can therefore not be held liable for failing to provide the necessary level of protection to a customer's personal data.

By way of example, customers may opt to download a vehicle manufacturer's app. The functionalities of these apps varies widely depending on the manufacturer and vehicle in question, with some allowing only basic functions, and others allowing for much more extensive capabilities (such as being able to open the vehicle using the app and being able to track the vehicles location). As a result of the fact that manufacturers have full control over who gains access to this data, leasing and rental companies have no means of knowing when a customer has downloaded this app, and no way of being able to protect other customers' data by requiring them to delete this app from their device. Consequently, it is feasible that a customer would be able to access a previous customer's information (such as their geolocation). This outlines the importance of ensuring leasing and rental companies are granted third party access to in-vehicle data. Leasing and rental companies want to be able to provide their customers with a secure, well maintained vehicle, and without this information their ability to do so is compromised.