Deloitte.

4 MAY 2020

Response to draft EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications

Introduction

Deloitte Risk Advisory is a leading global provider of cyber strategy consulting and cyber intelligence services. Deloitte's global network of member firms and related entities, active in more than 150 countries and territories, serves four out of five Fortune Global 500® companies.

We actively cooperates with automotive companies all over the world, providing experienced advice, among others, in Cyber Security, Research & development and GDPR compliance matters.

Given Deloitte Risk Advisory experience in the provision of advisory services to major automotive players, in our submission, we would like to highlight some legal and technical aspects of the draft Guidelines that we find would benefit from additional clarifications.

General considerations

Deloitte welcomes the European Data Protection Board's (EDPB) guidelines on processing personal data in the context of connected vehicles and mobility related applications.

The automotive industry is testifying a time of great change. New services can be enabled in connected vehicles and mobility related applications, from info mobility to safety or entertainment on-board. In addition, Advanced Driver Assistance Systems, Artificial Intelligence, Internet of Things, 5G and new technologies in general contribute to accelerating the transformation of vehicles and mobility.

While such transformation is only at its first stages, there is no doubt that the advent of connected vehicles and mobility related applications has already raised several data protection concerns, which will be potentially increased with the spread of autonomous vehicles.

Deloitte.

We firmly believe that the legislative framework applicable to connected vehicles and mobility related applications at the EU level should be clarified and standardized to the highest degree, for the benefit of the whole sector.

In this vein, we are very pleased that **the Guidelines make it finally clear that certain categories of data, even where not directly linked to a name, but to technical aspects and features of the vehicle, can be considered personal data, since they will relate to drivers or passengers**.

Indeed, establishing clear, consistent and uniform rules for manufacturers and vehicle equipment developers is essential to ensure the development of data-protection friendly connected solutions from the product design phase and throughout the complete development process.

Deloitte.

Table of Contents

Deloitte.

Lack of control and information asymmetry

Deloitte fully shares the EPDB concerns that **vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle**[1]. However, the Board emphasis on the right to be informed of passengers and subjects, others than the vehicle owner/ holder, might lead, in our opinion, to specific problems of implementation of the draft guidelines in practice.

Our considerations:

While we acknowledge that where drivers and passengers are somehow related to the vehicle's owner the provision of information might be easily ensured through the modalities suggested by the EDPB in the draft guidelines[2], in our opinion, they would **hardly be applicable in practice to drivers and passengers who are not related to the vehicle's owner**.

Our suggestions:

We do believe that car manufacturers and vehicle equipment developers would benefit from **further examples** by the Board that might help clarifying the specific context in which the information obligation could apply to subjects different from the vehicle owner/contract holder (i.e. users and passengers) in the context of connected vehicles and mobility related applications.

We also invite the EDPB to **clarify** in the final guidelines specific aspects such as the **time and the modalities for the provision of the information to users and passengers** (i.e. in case of second-hand, leased, rented or borrowed vehicles), especially where the contract with the vehicle's owner/ holder or consent applies as legal grounds for the processing.

We believe that this point is of high importance for car manufacturers and vehicle equipment developers, since the EDPB guidelines directly attributes to them the obligation to provide information to the data subjects.

Further considerations:

Today additional services provided to the Data Subject by vehicles, where the **Data Controller is different from the Vehicle manufacturer**, for instance

[1] See page [10] of the draft Guidelines, which states: "Information are usually provided to the owner on occasion of the signing of the contract while the car might process personal data of subjects others than the owner (i.e. users, passengers)…"

[2] See page [17] of the draft Guidelines, where the Board suggest that the information are provided to the data subjects in the contract for the provision of services, and or/in any written medium by using distinct documents or through the onboard computer.

smartphones mirroring services (used to mirror specific device features or apps the car's compatible infotainments), are a reality.

Given that **these services could be accessed by the vehicle's dashboard head unit**, it may not be clear to the Data Subject who actually acts as Data Controller for a specific processing.

In addition**,** the current wording of the draft Guidelines seems to suggest that **when new information are taken care of by a new data controller this latter shall provide data subjects with the required information when services that interact with connected vehicles are provided by them**[3].

In this regard, we believe that, given the speed demands associated with the execution and provision of mirroring services in the context of connected vehicles and mobility related applications, the risk of occurrence of a lack of information would be incredibly high.

Therefore, we suggest the Board to **provide in the final guidelines examples of adequate modalities for the provision of the information by new controllers,** preferably in the context of mirroring services and similar.

Quality of the users' consent

We are fully in line with the Board's position as for the **risk of obtaining a "low-quality consent"**[4] in the context of connected vehicles, since the users may not often be aware of the data processing carried out in their vehicle[5]. However, the **EDPB itself recognizes the practical difficulties associated with the fulfillment of this requirement**, acknowledging that classic mechanism used to obtain individual's consent may be difficult to apply in practice to drivers and passengers, especially where they are not directly related to the vehicle's owner / holder[6].

Our considerations:

In this regard, we believe that **the draft Guidelines' assertion that consent shall be obtained, separately from the "different participants"[7] would require a more granular examination**.

[3] Page [18] of the draft Guidelines
[4] Ibid.
[5] Ibid.
[6] Page [11] of the draft Guidelines
[7] In our understanding, the term would include not only the vehicle owner/holder but also other car users and passengers

Deloitte.

Our suggestions:

In particular, more context should be given in the final Guidelines to **clarify the adequate modalities for obtaining consent separately for drivers and passengers**, especially where the consent of the vehicle owner/holder is collected at the time of the conclusion of the contract[8].

Further considerations:

We also question whether the position taken by the EDPB is aligned with the provision of Recital 57 GDPR[9]. Indeed, while it is true that information concerning technical aspects and features of the vehicles should be considered as personal data, since they concerns the driver or the passenger, **in our opinion, information collected by a connected car might not always allow the controller to identify a natural person**.

This applies in particular to drivers and passengers, especially where they are not directly related to the vehicle owner/ holder (i.e. in case of second-hand, leased, rented or borrowed vehicles).

We are concerned that the necessity to obtain a valid consent from drivers and passengers might **potentially involve the acquisition of additional information** in order to identify the data subjects, **for the sole purpose of compliance** with the provision of the Regulation regarding consent.

Transmitting personal data to third parties

We believe that the EDPB statement that the **data subject's consent shall be systematically obtained before their data are transmitted to a commercial partner**, acting as a data controller[10], is in direct relation with the observation raised in the previous section.

Our considerations:

In our opinion, the **use of the term "data subjects"** in the draft Guidelines could be interpreted to include drivers and passengers, and might therefore lead to the specific **problems of implementation described above**, especially where drivers and passengers are not directly related to the vehicle

[8] The "Cases" of the draft Guidelines often states the necessity to collect the consent of the vehicle's owner at the time of conclusion of the contract (See pages [22] [27]).

[9] See Recital 57 GDPR, which states: "If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation".

[10] Page [20] of the draft Guidelines

owner/ holder (i.e. in case of second-hand, leased, rented or borrowed vehicles).

Rights of the data subjects

We appreciate the fact that the Guidelines provide specific orientations as for what concerns the handlings of the data subject's rights in the context of connected vehicles and mobility related applications. In particular, we believe that the **suggestion of implementing specific profile management systems**, centralizing every data settings for each data processing[11], is particularly helpful for vehicle and equipment manufacturers, who will be directly involved in the development of secure car applications, with due respect of the principle of privacy by design and by default.

Our considerations:

However, with regard to the EDPB assertion that: "*the sale of a connected vehicle and the ensuing change of ownership should trigger the deletion of any personal data"*, in our opinion, the draft Guidelines, while stating a specific obligation, are **not clearly identifying the subject responsible for its fulfillment**.

Our suggestion:

We believe that the current language in the Guidelines could be read to suggest that such obligation would be on the Data Controller (i.e. vehicle and equipment manufactures), however, we note that in many cases (i.e. purchase of a vehicle between private individuals), Controllers might find difficult to implement such requirement in practice.

Security of personal data

We fully agree with the Board's statement that the **"plurality of functionalities, services and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised"** [12]. In fact, within the scope of product digitization, the risk environment is changing and it is important to maintain the end user trust in the products and services, and especially in the protection of their personal data, while developing these new digital services.

[11] Page [19] of the draft Guidelines
[12] Page [11] of the draft Guidelines

Our considerations:

The services and related processing need to address the increasing personal data risk and ensure adequate protection to the customer personal data.

Considering the plurality of services that could be provided by the vehicles, and consequently of the processing, it is reasonable to assume that, if a specific analysis is not carried out by the vehicles manufactures, some related data protection risks will not be adequately considered and properly managed.

Our suggestions:

In this regard, we believe that the Board should place more emphasis in the final Guidelines on the necessity to implement a risk-based approach, to be followed by the manufacturer, so as to have a clear picture of Data Protection Risks of the vehicles. In brief, this would foresee a threat analysis to define a data protection vehicle reference model, aimed at identifying areas of risks in terms of data protection of a vehicle and the adoption of specific security controls to reduce the identified risks to an acceptable level.

Final considerations

To conclude our submission, we would like to add some further comments on the following grounds:

- Ground 1: Scope of application of the Guidelines and exclusion of processing of data enabling Cooperative Intelligent Transport Systems

As for the scope of the draft Guidelines, we acknowledge the Board's decision of excluding the processing of data **enabling Cooperative Intelligent Transport Systems (C-ITS)** from the application of the document, due to the very specific data protection implications in this context and the current discussions carried out at the European level[13].

However, considering that the development of cars is increasingly geared towards autonomous driving, especially with regard to freight transport, we expect in the short run the adoption of technologies capable of constantly communicating with the surrounding environment (V2V & V2I), eventually using block chain to allow for a faster transmission between the involved vehicles.

We firmly believe that where similar technologies are not developed with a specific focus on Data Protection, the risk for the data subjects would be to be constantly monitored by third parties (e.g. the provider of infrastructures

[13] Page [8] [9] of the draft Guidelines

services in V2I) that would always know the position and the movements of the data subjects.

While welcoming the EU discussions and efforts in its regards, we hope that the adoption of such technologies will be adequately regulated in the shortest possible time, to foresee the adoption of security by design in their early development and standardization.

- Ground 2: European level and international initiatives in the context of connected vehicles and mobility related applications

Section *1.1.1 European level and international initiatives* of the draft Guidelines seems not to explicitly mention the "**UN Proposal of Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems",** (also known as **UNECE WP.29 GRVA regulation**)" and the **ISO SAE 21434 "Standard on Road vehicles — Cybersecurity engineering"**[14].

Indeed, the UNECE WP.29 GRVA obliges in the near future - from 2022[15] exclusively for new models and from 2024[16] for all models in production (official date still to be defined) - to **implement a Cyber Security Management System (CSMS)** as a necessary requirement for cars' homologation. This also includes a successful certification of the management system and the specific vehicle types.

The **ISO SAE 21434** instead, in addition to various Cyber Security requirements, provides the necessity to identify relevant assets for the vehicles and possible "damage scenarios" including privacy-related impacts.

We believe that the inclusion of a reference to the aforementioned regulation and standards and to their potential interaction with the Guidelines should be considered in the final version, in order to ensure harmonization and avoid potential future contrasts on the subject.

[14] At the date of writing of this document in "Under development" Status

[15] As the document is still under development the data is subject to change

[16] Ibid.

Deloitte.

Closing remarks

We appreciate the opportunity to submit comments to the Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications and the continued effort of the EDPB to engage with stakeholders.

We remain available for any questions you may have.

Respectfully submitted,

Stefano Buschi

Partner Deloitte Risk Advisory

sbuschi@deloitte.it

Tommaso Stranieri

Partner Deloitte Risk Advisory

tstranieri@deloitte.it

Francesca Santoro

Manager Deloitte Risk Advisory

frsantoro@deloitte.it

Andrea Succi

Manager Deloitte Risk Advisory

asucci@deloitte.it