

# Guidelines



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

**Version 1.0**

**Adopted on 28 January 2020**

# Table of contents

- 1 INTRODUCTION ..... 3
  - 1.1 Related works..... 4
  - 1.2 Applicable law ..... 5
  - 1.3 Scope..... 6
  - 1.4 Definitions ..... 9
  - 1.5 Privacy and data protection risks..... 10
- 2 GENERAL RECOMMENDATIONS..... 12
  - 2.1 Categories of data ..... 12
  - 2.2 Purposes..... 14
  - 2.3 Relevance and data minimisation ..... 14
  - 2.4 Data protection by design and by default ..... 14
  - 2.5 Information ..... 17
  - 2.6 Rights of the data subject ..... 19
  - 2.7 Security and confidentiality ..... 19
  - 2.8 Transmitting personal data to third parties..... 20
  - 2.9 Transfer of personal data outside the EU/EEA ..... 20
  - 2.10 Use of in-vehicle Wi-Fi technologies..... 21
- 3 CASE STUDIES ..... 21
  - 3.1 Provision of a service by a third party..... 21
  - 3.2 eCall..... 25
  - 3.3 Accidentology studies ..... 27
  - 3.4 Tackle auto theft ..... 29
  - 3.5 Personal information stored on rental cars’ dashboard..... 30

## The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018<sup>1</sup>,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

### HAS ADOPTED THE FOLLOWING GUIDELINES

## 1 INTRODUCTION

1. Symbol of the 20th century economy, the automobile is one of the mass consumer products that has impacted society as a whole. Commonly associated with the notion of freedom, cars are often considered as more than just a mean of transportation. Indeed, they represent a private area in which people can enjoy a form of autonomy of decision, without encountering any external interferences. Today, as connected vehicles move into the mainstream, such a vision no longer corresponds to the reality. In-vehicle connectivity is rapidly expanding from luxury models and premium brands to high-volume midmarket models, and vehicles are becoming massive data hubs. Not only vehicles, but drivers and passengers are also becoming more and more connected. As a matter of fact, many models launched over the past few years on the market integrate sensors and connected onboard equipment, which may collect and record, among other things, the engine performance, the driving habits, the locations visited, and potentially even the driver’s eye movements, his or her pulse, or other biometric data for authentication or identification purposes.<sup>2</sup>
2. Such data processing is taking place in a complex ecosystem, which is not limited to the traditional players of the automotive industry, but is also shaped by the emergence of new players belonging to the digital economy. These new players may offer infotainment services such as online music, road condition and traffic information, or provide driving assistance systems and services, such as autopilot software, vehicle condition updates, usage-based insurance or dynamic mapping. Moreover, since vehicles are connected via electronic communication networks, road infrastructure managers and telecommunications operators involved in this process also play an important role with respect to the potential processing operations applied to the drivers’ and passengers’ personal data.
3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style

---

<sup>1</sup> References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

<sup>2</sup> Infographic “Data and the connected car” by the Future of Privacy Forum; [https://fpf.org/wp-content/uploads/2017/06/2017\\_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf](https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf)

or the distance covered, data relating to the wear and tear on vehicle parts or data collected by cameras may concern driver behavior as well as information about other people who could be inside or outside the vehicle.

4. In 2016, the Fédération Internationale de l'Automobile (FIA) ran a campaign across Europe called "My Car My Data" to get a sentiment on what Europeans think about connected cars.<sup>3</sup> While it showed the high interest of drivers for connectivity, it also highlighted the vigilance that must be exercised with regard to the use of the data produced by vehicles as well as the importance of complying with personal data protection legislation. Thus, the challenge is, for each stakeholder, to incorporate the "protection of personal data" dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.

### 1.1 Related works

5. Connected vehicles have become a substantial subject for regulators over the last decade, with a major increase in the last couple of years. Various works have thus been published at the national and international levels concerning the security and privacy of connected vehicles. Those regulations and initiatives aim at complementing the existing data protection and privacy frameworks with sector specific rules or providing guidance to professionals.

#### 1.1.1 European-level and international initiatives

6. From 31 March 2018 onward, a 112-based eCall in-vehicle system is mandatory on all new types of M1 and N1 vehicles (passenger cars and light duty vehicles).<sup>4,5</sup> In 2006, the Article 29 Working Party had already adopted a working document on data protection and privacy implications in eCall initiative.<sup>6</sup> In addition, as previously discussed, the Article 29 Working Party also adopted an opinion in October 2017 regarding the processing of personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).
7. In January 2017, the European Union Agency for Network and Information Security (ENISA) published a study focused on cyber security and resilience of smart cars listing the sensitive assets as well as the corresponding threats, risks, mitigation factors and possible security measures to implement.<sup>7</sup> In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles.<sup>8</sup> Finally, in April 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT), also adopted a working paper on connected vehicles.<sup>9</sup>

---

<sup>3</sup> Campaign "My Car My Data"; <http://www.mycarmydata.eu/>

<sup>4</sup> The interoperable EU-wide eCall; [https://ec.europa.eu/transport/themes/its/road/action\\_plan/ecall\\_en](https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en)

<sup>5</sup> Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service Text with EEA relevance; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585>

<sup>6</sup> Working document on data protection and privacy implications in eCall initiative;

[http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf)

<sup>7</sup> Cyber security and resilience of smart cars; <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>

<sup>8</sup> Resolution on data protection in automated and connected vehicles;

[https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles\\_en\\_1.pdf](https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf)

<sup>9</sup> Working paper on connected vehicles; <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>

### 1.1.2 National initiatives of European Data Protection Board (EDPB) members

8. In January 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) published a common declaration on the principles of data protection in connected and not-connected vehicles.<sup>10</sup> In August 2017, the UK Centre for Connected and Autonomous Vehicles (CCAV) released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector.<sup>11</sup> In October 2017, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released a compliance package for connected cars in order to provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data.<sup>12</sup>

## 1.2 Applicable law

9. The relevant EU legal framework is the General data protection regulation (2016/679). It applies in any case where data processing in the context of connected vehicles involves processing personal data of individuals.
10. Additionally to the GDPR, the “ePrivacy” directive (2002/58/EC, as revised by 2009/136/EC), **sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).**
11. Indeed, if most of the “ePrivacy” directive provisions (art. 6, art. 9, etc.) only applies to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.
12. Regarding the notion of “*terminal equipment*”, the definition is given by directive 2008/63/CE. Art. 1 (a) define the terminal equipment as an “*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment*”.
13. **As a result, the connected vehicle and every device connected to it shall be considered as a “terminal equipment” (just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy directive must apply where relevant.**
14. As recently outlined by the EDPB in its opinion 5/2019 on the interplay between the “ePrivacy” directive and the GDPR,<sup>13</sup> art. 5(3) ePrivacy directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the information stored in the end-user’s device

---

<sup>10</sup> Data protection aspects of using connected and non-connected vehicles;

[https://www.lda.bayern.de/media/dsk\\_joint\\_statement\\_vda.pdf](https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf)

<sup>11</sup> Principles of cyber security for connected and automated vehicles;

<https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>

<sup>12</sup> Compliance package for a responsible use of data in connected cars; <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>

<sup>13</sup> European Data Protection Board, [Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities](#), adopted on 12 March 2019, paragraph 40.

constitutes personal data, art. 5(3) ePrivacy directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information.<sup>14</sup> Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must additionally have a legal basis under art. 6 GDPR in order to be lawful.<sup>15</sup>

15. Since the controller will have to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations – when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy directive, the consent will normally also cover such processing operations. Consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the aforementioned processing operations. Indeed, when assessing compliance with art. 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.<sup>16</sup> Moreover, controllers must take into account the impact on data subjects’ rights when identifying the appropriate lawful basis in order to respect the principle of fairness.<sup>17</sup> The bottom line is that art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by art. 5(3) ePrivacy directive.
16. The EDPB recalls that the notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.
17. However, if consent is the principle, art. 5(3) ePrivacy directive allows the storing of information or the gaining of access to information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, if it satisfy one of the following criteria:
  - **Exemption 1:** for the sole purpose of carrying out the transmission of a communication over an electronic communications network ;
  - **Exemption 2:** 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.
18. In such cases, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal basis as provided by art. 6 GDPR.

### 1.3 Scope

19. 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: e.g., drivers, passengers, vehicle owners, renters, etc. More specifically, it deals with the personal data (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user’s smartphone) or (iii) collected within the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.
20. The connected vehicle definition has to be understood as a broad concept in this document. It can be defined as a vehicle equipped with many electronic control units (ECU) that are linked together via an

---

<sup>14</sup> Ibid, paragraph 40.

<sup>15</sup> Ibid, paragraph 41.

<sup>16</sup> Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraph 41.

<sup>17</sup> European Data Protection Board, [Guidelines 2/2019 on the processing of personal data under Article 6\(1\)\(b\) GDPR in the context of the provision of online services to data subjects](#), Version 2.0, 8 October 2019, paragraph 1.

in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle (for example, relying on the sole use of the smart phone) to assist drivers is included in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle *per se*. Applications for connected vehicles are multiple and diverse and can include<sup>18</sup>:

21. *Mobility management*: functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, by providing timely information about GPS navigation, potentially dangerous environmental conditions (e.g., icy roads), traffic congestion or road construction work, parking lot or garage assistance, optimised fuel consumption or road pricing.
22. *Vehicle management*: functions that are supposed to aid drivers in reducing operating costs and improving ease of use, such as notification of vehicle condition and service reminders, transfer of usage data (e.g., for vehicle repair services), customised “Pay As/How You Drive” insurances, remote operations (e.g., heating system) or profile configurations (e.g., seat position).
23. *Road safety*: functions that warn the driver of external hazards and internal responses, such as collision protection, hazard warnings, lane departure warnings, driver drowsiness detection, emergency call (eCall) or crash investigation “black-boxes” (event data recorder).
24. *Entertainment*: functions providing information to and involving the entertainment of the driver and passengers, such as smart phone interfaces (hands free phone calls, voice generated text messages), WLAN hot spots, music, video, Internet, social media, mobile office or “smart home” services.
25. *Driver assistance*: functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways,
26. *Well-being*: functions monitoring the driver's comfort, ability and fitness to drive such as fatigue detection or medical assistance.
27. Hence, vehicles can be natively connected or not and personal data can be collected through several means, including: (i) vehicle sensors, (ii) telematics boxes or (ii) mobile applications (e.g. accessed from a device belonging to a driver). In order to fall within the scope of this document, mobile applications need to be related to the environment of driving. For example, GPS navigation applications are indeed within the scope, while applications that suggest places of interest (restaurants, historic monument, etc.) to the user will not be covered by this document.
28. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver's complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle

---

<sup>18</sup> PwC Strategy 2014. “In the fast lane. The bright future of connected cars”;  
[https://www.strategyand.pwc.com/media/file/Strategyand\\_In-the-Fast-Lane.pdf](https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf)

maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

29. The connected vehicle ecosystem covers a wide spectrum of stakeholders. More precisely, it includes traditional actors of the automotive industry as well as emerging players from the digital industry.
30. Hence, these guidelines are directed towards vehicle manufacturers, equipment manufacturers and automotive suppliers, car repairers, automobile dealerships, vehicle service providers, rental and car sharing companies, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities as well as drivers, owners, renters and passengers. This is a non-exhaustive list.

### 1.3.1 Out of scope of this document

31. Employers providing company cars to members of their staff might want to monitor their employee's actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Data processing carried out by employers in this context raises specific considerations to the employment context, which might be regulated by labour laws at the national level that cannot be detailed in these guidelines.
32. Connected vehicles being radio-enabled systems, they are subject to passive tracking such as WiFi or Bluetooth tracking. In that sense they do not differ from other connected devices and fall in the scope of the ePrivacy directive which is currently being revised. This therefore excludes also large-scale tracking of WiFi equipped vehicles<sup>19</sup> by a dense network of bystanders who use common smartphone location services. These routinely report all visible WiFi networks to central servers. Since built-in WiFi can be considered a secondary vehicle identifier,<sup>20</sup> this risks a systematic ongoing collection of complete vehicle movement profiles in a third country.
33. Increasingly vehicles are equipped with image recording devices (e.g., car parking camera systems or dashcams). Since this deals with the issue of filming public places, which requires an assessment of the relevant legislative framework which is specific to each Member State, this data processing is out of scope.
34. The processing of data enabling Cooperative Intelligent Transport Systems (C-ITS) – as defined in the directive of the European Union 2010/40/EU<sup>21</sup> has been dealt with in a specific opinion by the Article 29 Working Party<sup>22</sup>. Through this opinion, the WP29 focused on specific use cases built for initial deployment and committed to assess at a later stage the new issues that will be undoubtedly raised when higher level of automation will be implemented. Since the data protection implications in the context of C-ITS are very specific (unprecedented amounts of location data, continuous broadcasting of personal data, exchange of data between vehicles and other road infrastructural facilities, etc.) and

---

<sup>19</sup> See <https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html> for details

<sup>20</sup> Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, pages 32 to 37.

<sup>21</sup> Directive on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040>

<sup>22</sup> WP29 - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS); [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610171](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171)



that it is still being discussed at the European level the processing of personal data in that context is out of scope.

35. Finally, this document does not aim to address all possible issues and questions raised by connected vehicles and can therefore not be considered as exhaustive.

#### 1.4 Definitions

36. The **processing** of personal data encompasses any operation that involves personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, etc.
37. The **data subject** is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle.
38. The **data controller** is the person who determines the purposes and means of processing that take place in connected vehicles. Data controllers can include service providers that process vehicle data to send the driver traffic-information, eco-driving messages or alerts regarding the functioning of the vehicle, insurance companies offering "*Pay As You Drive*" contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle's parts to improve its quality. Pursuant to art. 26 GDPR, two or more controllers can jointly determine the purposes and means of the processing and thus be considered as joint controllers. In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.
39. The **data processor** is any person who processes personal data for and on behalf of the data controller. The data processor collects and processes data on instruction from the data controller, without using those data for its own account. As an example, in a number of cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, e.g. art. 28 GDPR sets out data processors' obligations.
40. The **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. As an example, a commercial partner of the service provider that receives from the service provider personal data generated from the vehicle is a recipient of personal data. Whether they act as a new data controller or as a data processor, they shall comply with all the obligations imposed by the GDPR.
41. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. As an example, law enforcement authorities are authorised third parties when they request personal data as part of an investigation in accordance with European Union or Member State law.

## 1.5 Privacy and data protection risks

42. Article 29 Working Party has already expressed several concerns about Internet of Things (IoT) systems that can also apply to connected vehicles.<sup>23</sup> The issues relating to data security and control already stressed regarding IoT are even more sensitive in the context of connected vehicles, since it entails road safety concerns – and can impact the physical integrity of the driver – in an environment traditionally perceived as isolated and protected from external interferences.
43. Also, connected vehicles raises significant data protection and privacy concerns regarding the processing of location data as its increasingly intrusive nature can put a strain on the current possibilities to remain anonymous. The EDPB wants to place particular emphasis and raise stakeholders awareness to the fact that the use of location technologies requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data.

### 1.5.1 Lack of control and information asymmetry

44. Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle. The information may be given only to the vehicle owner, who may not be the driver, and may also not be provided in a timely fashion. Thus, there is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights. This point is of importance since, during their lifetime, vehicles may belong to more than one owner either because they are sold or because they are being leased rather than purchased. In addition, vehicles are increasingly being shared or rented, not just by companies, but also individuals, and the person whose data is collected may not be able to object to some data processing.<sup>24</sup>
45. Also, communication in the vehicle can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how the vehicle and its connected equipment interact, it is bound to become extraordinarily difficult for the user to control the flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.

### 1.5.2 Quality of the user's consent

46. The EDPB underlines that, when the data processing is based on consent, all elements of valid consent have to be met which means that consent shall be free, specific and informed and constitutes an unambiguous indication of the data subject's wishes as interpreted in EDPB guidelines on consent.<sup>25</sup> Data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given.
47. The same has to be applied when consent is required to comply with the “ePrivacy” directive, for example if there is a storing of information or the gaining of access to information already stored in the vehicle as required in certain cases by art. 5(3) of the “ePrivacy” directive. Indeed, as outlined above, consent in this context has to be interpreted in light of the GDPR.

---

<sup>23</sup> WP29 – Opinion 8/2014 on the Recent Developments on the Internet of Things;

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf)

<sup>24</sup> Privacy International – Connected Cars: What Happened to Our Data on Rental Cars;

[https://privacyinternational.org/sites/default/files/2017-12/cars\\_briefing.pdf](https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf)

<sup>25</sup> Article 29 Working Party – WP259 rev.01 - Guidelines on consent under Regulation 2016/679;

[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623051](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051) - endorsed by the EDPB

48. In many cases, the user may not be aware of the data processing carried out in his/her vehicle. Such lack of information constitutes a significant barrier to demonstrating valid consent under the GDPR, as the consent must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under the GDPR.
49. Classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, consent might also be difficult to obtain for drivers and passengers who are not related to the vehicle's owner in the case of second-hand, leased, rented or borrowed vehicles.

#### 1.5.3 Further processing of personal data

50. When data are collected on the basis of consent as required by art. 5(3) of the "ePrivacy" directive or on one of the exemptions of art. 5(3), it can only be further processed either if the controller 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 art. 23 (1) GDPR. The EDPB considers that further processing on the basis of a compatibility test according to art. 6(4) GDPR is not possible in these cases, since it would undermine the data protection standard of the "ePrivacy" directive.
51. The EDPB recalls that the initial consent will never legitimise further processing as consent need to be informed and specific to be valid.
52. For instance, telemetry data, which is collected during use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behaviour based insurance policies.
53. Furthermore, data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when the specific conditions in the law enforcement directive are fulfilled. In this case, such data will be considered as relating to criminal convictions and offences under the conditions laid down by art. 10 GDPR and any applicable national legislation. Manufacturers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled. The EDPB points out that processing of personal data for the sole purpose of fulfilling requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR. When law enforcement authorities are authorized by law, they could be third parties within the meaning of art. 4(10) GDPR, in this case manufacturers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each Member State.

#### 1.5.4 Excessive data collection

54. With the ever-increasing number of sensors being deployed in connected vehicles there is a very high risk of excessive data collection compared to what is necessary to achieve the purpose.
55. The development of new functionalities and more specifically those based on machine learning algorithms may require a large amount of data collected over a long period of time

#### 1.5.5 Security of personal data

56. 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. Unlike most Internet of Things devices, connected vehicles are critical systems where a security breach may endanger the life of its users and

people around. The importance of addressing the risk of hackers attempting to exploit connected vehicles' vulnerabilities is thus heightened.

57. In addition, personal data stored on vehicles and/or at external locations (e.g., in cloud computing infrastructures) may not be adequately secured against unauthorized access. For instance, during maintenance, a vehicle has to be handed to a technician who will require access to some of the vehicle's technical data. While the technician needs to have access to the technical data, there is a possibility that the technician could attempt to access all the data stored in the vehicle.

## 2 GENERAL RECOMMENDATIONS

58. In order to mitigate the risks for data subjects identified above, the following general recommendations should be followed by vehicle and equipment manufacturers, service providers or any other stakeholder who may act as data controller or data processor in relation to connected vehicles.

### 2.1 Categories of data

59. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). Certain data generated by connected vehicles may also warrant special attention given their sensitivity and/or potential impact on the rights and interests of data subjects. At present, the EDPB has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.

#### 2.1.1 Geolocation data

60. When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that geolocation data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver's centers of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller shall be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing. As an example, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data.
61. In general, collecting geolocation data is also subject to compliance with the following principles:
  - adequate configuration of the frequency of access to, and of the level of detail of, geolocation data collected relative to the purpose of processing. For example, a weather application should not be able to access the vehicle's geolocation every second, even with the consent of the data subject;
  - providing accurate information on the purpose of processing (e.g., is geolocation history stored? If so, what is its purpose?);

- when the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use, for example on the onboard computer ;
- activating geolocation only when the user launches a functionality that requires the vehicle’s location to be known, and not by default and continuously when the car is started;
- informing the user that geolocation has been activated, in particular by using icons (e.g., an arrow that moves across the screen);
- the option to deactivate geolocation at any time;
- defining a limited storage period;

### 2.1.2 Biometric data

62. In the context of connected vehicles, biometric data may be used, for among other things, to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver’s profile settings and preferences. When considering the use of biometric data, guaranteeing the data subject full control over his or her data involves, on the one hand, providing for the existence of a non-biometric alternative (e.g., using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory), and, on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal.
63. In the case of biometric data, it is important to ensure that the biometric authentication solution is sufficiently reliable, in particular by complying with the following principles:
- the adjustment of the biometric solution used (e.g., the rate of false positives and false negatives) is adapted to the security level of the required access control;
  - the biometric solution used is based on a sensor that is resistant to attacks (such as the use of a flat-printed print for fingerprint recognition);
  - the number of authentication attempts is limited;
  - the biometric template/model is stored in the vehicle, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art;
  - the raw data used to make up the biometric template and for user authentication are processed in real time without ever being stored, even locally.

### 2.1.3 Data revealing criminal offenses or other infractions

64. It is possible that personal data from connected vehicles could reveal the commitment of a criminal offence or other infraction (“offence-related data”) and therefore be subject to special restrictions. For instance, the instantaneous speed of a vehicle combined with precise geolocation data or data indicating that the vehicle crossed a white line could be considered offence-related data. As a result, processing of such data can only be carried out under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects as stated in art. 10 GDPR. The EDPB considers that instantaneous speed is, not on its own, offence-related data since it does not, by itself, reveal an offence given that speed restrictions vary by location. However, such data could nevertheless become offence-related data because of the purpose for which it is collected (e.g., for the purposes of investigating and prosecuting criminal offence), in which case the safeguards set out in art. 10 GDPR would apply.

65. In order to process data that relate to potential criminal offences, EDPB recommends to resort to the local processing of the data where the data subject have full control over the processing in question(see discussion on local processing above, in section 2.1). Indeed – except for some exceptions (see the case study on accidentology studies presented below in section 3.2) – external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures such as those described in section 2.7 must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data.

## 2.2 Purposes

66. Personal data may be processed for a wide variety of purposes in relation to connected vehicles, including driver safety, insurance, efficient transportation, entertainment or information services. In accordance with the GDPR, data controllers must ensure that their purposes are “specified, explicit and legitimate”, not further processed in a way incompatible with those purposes and that there is a valid legal basis for the processing as required in ar. 5 GDPR. Some concrete examples of purposes that may be pursued by data controllers operating in the context of connected vehicles are discussed in Part III of these guidelines, along with specific recommendations for each type of processing.

## 2.3 Relevance and data minimisation

67. To comply with the data minimization principles, vehicle and equipment manufacturers, service providers and other data controllers should pay special attention to the categories of data they need from a connected vehicle, as they shall only collect personal data that are relevant and necessary for the processing. For instance, location data are particularly intrusive and can reveal many life habits of the data subjects. Accordingly, industry participants shall be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing (see discussion on geolocation data above, in section 2.2).

## 2.4 Data protection by design and by default

68. Taking into account the volume and diversity of personal data produced by connected vehicles, the EDPB notes that data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by art. 25 GDPR. Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data. Specific guidance on how manufacturers and service providers can comply with data protection by design and by default could be beneficial for the industry.
69. Certain general practices, described below, can also help mitigate the risks to the rights and freedoms of natural persons associated with connected vehicles.

### 2.4.1 Local processing of personal data

70. In general, vehicle and equipment manufacturers, service providers and other data controllers should, wherever possible, use processes that do not involve personal data or transferring personal data outside of the vehicle (i.e., the data is processed internally). This scenario offers the advantage of guaranteeing to the user the sole and full control of his/her personal data and, as such, it presents, “by design”, less privacy risks especially by prohibiting any data processing by stakeholders without the data subject knowledge. It also enables the processing of sensitive data such as biometric data or data relating to criminal offenses or other infractions, as well as detailed location data which otherwise would be subject to stricter rules (see below). In the same vein, it presents fewer cybersecurity risks

and involves little latency, which makes it particularly suited to automated driving-assistance functions. Some examples of this type of solution could include:

- eco-driving applications that process data in the vehicle in order to display eco-driving advice in real time on the on-board screen;
- applications that involve a transfer of personal data to a device such as a smartphone under the user’s full control (via, for example, Bluetooth or Wi-Fi), and where the vehicle’s data are not transmitted to the application providers or the vehicle manufacturers; this would include, for instance, coupling of smartphones to use the car’s display, multimedia systems, microphone (or other sensors) for phone calls, etc., to the extent that the data collected remain under the control of the data subject and is exclusively used to provide the service he or she has requested;
- in-vehicle safety enhancing applications such as those that provide audible signals or vibrations of the steering wheel when a driver overtakes a car without indicating or straying over white lines or which provides alerts as to the state of the vehicle (e.g., an alert on the wear and tear affecting brake pads);
- applications for unlocking, starting, and/or activating certain vehicle commands using the driver’s biometric data that is stored within the vehicle (such as a face or voice models or fingerprint minutiae).

71. Applications such as the above involve processing carried out for the performance of purely personal activities by a natural person (i.e., without the transfer of personal data to a data controller or data processor). Therefore, in accordance with art. 2(2) GDPR, **these applications fall outside the scope of the GDPR.**
72. Local data processing should be considered by car manufacturers and service providers, whenever possible to mitigate the potential risks of cloud processing, as they are underlined in the opinion on Cloud Computing released by the Article 29 Working Party.<sup>26</sup>
73. However, if the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.). Hence, when they are acting as data controller or data processor, they must develop secure in-car application and with due respect to the principle of privacy by design and by default. In any case, according to Recital 78 GDPR, “When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations”. On the one hand, it will enhance the development of user-centric services and, on the other hand, it will facilitate and secure any further uses in the future which could fall back within the scope of the GDPR. More specifically, the EDPB recommends developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities.

---

<sup>26</sup> WP29 – Opinion 5/2012 on Cloud Computing; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf)

74. In general users should be able to control how their data are collected and processed in the vehicle:
- information regarding the processing must be provided in the driver’s language (manual, settings, etc.) ;
  - the EDPB recommends that only data strictly necessary for the vehicle functioning are processed by default. Data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned.;
  - data should not be transmitted to any third parties (i.e., the user has sole access to the data);
  - data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or member state law ;
  - data subjects should be able to delete permanently any personal data before the vehicles are put up for sale;
  - data subjects should, where feasible, have a direct access to the data generated by these applications.
75. Finally, while it may not always be possible to resort to local data processing for every use-case, “hybrid processing” can often be put in place. For instance, in the context of usage-based insurance, personal data regarding driving behaviour (such as the force exerted on the brake pedal, mileage driven, etc.) could either be processed inside the vehicle or by the telematics service provider on behalf of the insurance company (the data controller) to generate numerical scores that are transferred to the insurance company on a defined basis (e.g. monthly basis). In this way, the insurance company does not gain access to the raw behavioural data but only to the aggregate score that is the result of the processing. This ensures that principles of data minimization are satisfied by design. This also means that users must have the ability to exercise their right when data are stored by other parties, for example a user should have the ability to delete data stored in the systems of a car maintenance shop or dealership.

#### 2.4.2 Anonymization and pseudonymisation

76. If data must leave the vehicle, consideration should be given to anonymize them before being transmitted. The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. As a consequence, anonymization, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles.
77. As detailed in the opinion adopted in April 2014 by the Article 29 Working Party on anonymization techniques, various methods can be used – sometimes in combination – in order to reach data anonymization.<sup>27</sup>
78. Other techniques such as pseudonymisation can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing. Pseudonymisation consists of replacing directly identifying

---

<sup>27</sup> WP29 - Opinion 05/2014 on Anonymisation Techniques; [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)



personal data by a non-signifying pseudonym. This can be done by, for example, using a secret-key hash algorithm. Pseudonymisation, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of misuse. Pseudonymisation is reversible, unlike anonymization, and is considered as personal data subject to the GDPR.

#### 2.4.3 Data protection impact assessments

79. Given the scale and sensitivity of the personal data that can be generated *via* connected vehicles; it is likely that processing – particularly in situations where personal data are processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals. Where this is the case, industry participants will be required to perform a data protection impact assessment (DPIA) to identify and mitigate the risks as detailed in the art. 35 and 36 GDPR. Even in the cases where a DPIA is not required, it is a best practice to conduct one as early as possible in the design process. This will allow industry participants to factor the results of this analysis into their design choices prior to the roll-out of new technologies.

### 2.5 Information

80. Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller (e.g., the vehicle and equipment manufacturer or service provider), the purpose of processing, the data recipients, the period for which data will be stored, and the data subject's rights under the GDPR.
81. In addition, the vehicle and equipment manufacturer, service provider or other data controller shall also provide the data subject with the following information, in clear, simple, and easily-accessible terms:
- the contact details of the data protection officer;
  - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing ;
  - the explicit mention of the legitimate interests pursued by the data controller or by a third party, when such legitimate interests constitute the legal basis for processing;
  - the recipients or categories of recipients of the personal data, if any;
  - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  - the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
  - the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal where the processing is based on consent ;
  - where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and safeguards used to transfer them ;
  - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This could particularly be the case in relation to the provision of usage-based insurance to individuals ;
  - the right to lodge a complaint with a supervisory authority ;
  - information about further processing ;
  - In case of joint data controllership, clear and complete information about the responsibilities of each data controller.
82. In some cases, personal data is not collected directly from the individual concerned. For instance, a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service. When data have not been collected directly, the vehicle and equipment manufacturer, service provider or other data controller shall, in addition to the information mentioned above, also indicate the categories of personal data concerned, the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information must be provided by the controller within a reasonable period after obtaining the data, and **no later than the first of the following dates** in accordance with Art. 14 (3) GDPR: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.
83. New information may also need to be provided to data subjects when they are taken care of by new data controller, for instance if they cross borders. Roadside assistance that interacts with connected vehicles can be provided by different data controllers depending on which country or region the assistance is required in. New data controllers shall provide data subjects with the required information when data subjects cross borders and services that interact with connected vehicles are provided by new data controllers.
84. The information directed to the data subjects may be provided in layers<sup>28</sup>, i.e., by separating two levels of information: on the one hand, first-level information, which is the most important for the data subjects, and, on the other hand, information that presumably is of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing and a description of the data subject's rights, as well as any additional information on the processing which has the most impact on the data subject and processing which could surprise them. The EDPB recommends that, in the context of connected vehicles, the data subject to be made aware of all the recipients in the first layer of information. As stated in the WP29 guidelines on transparency, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers cannot provide the names of the recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.

---

<sup>28</sup> Article 29 Working Party - WP260 rev.01 - Guidelines on transparency under Regulation 2016/679. [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=622227](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227) - endorsed by the EDPB

85. The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the onboard computer.
86. Standardised icons could be used in addition to the information necessary, as required under art. 13 and 14 GDPR, to enhance transparency by potentially reducing the need for vast amounts of written information to be presented to a data subject. It should be visible in vehicles in order to provide, in relation to the planned processing, a good overview that is understandable, and clearly legible. The EDPB emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle. For example, when certain types of data are being collected, such as geolocation, the vehicles could have a clear signal on-board (such as a light inside the vehicle) to inform passengers about data collection.

## 2.6 Rights of the data subject

87. Vehicle and equipment manufacturers, service providers and other data controllers should facilitate data subjects' control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.
88. To facilitate settings modifications, a profile management system should be implemented inside the vehicle in order to store the preferences of known drivers and help them to change easily their privacy settings anytime. The profile management system in a vehicle should centralize every data settings for each data processing, especially to facilitate the access, deletion and removal of personal data from vehicle systems at the request of the data subject. 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.
89. The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes.

## 2.7 Security and confidentiality

90. Vehicle and equipment manufacturers, service providers and other data controllers shall put in place measures that guarantee the security and confidentiality of processed data and take all useful precautions to prevent control being taken by an unauthorised person. In particular, industry participants should consider adopting the following measures:
  - encrypting the communication channels by means of a state-of-the-art algorithm;
  - putting in place an encryption-key management system that is unique to each vehicle, not to each model;
  - when stored remotely, encrypting data by means of state-of-the-art algorithms;
  - regularly renewing encryption keys;
  - protecting encryptions keys from any disclosure;
  - authenticating data-receiving devices;
  - ensuring data integrity (e.g., by hashing);

- make access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);
91. Concerning more specifically vehicle manufacturers, the EDPB recommends the implementation of the following security measures:
- partitioning the vehicle’s vital functions from those always relying on telecommunication capacities (e.g., “infotainment”);
  - implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
  - for the vehicle’s vital functions, give priority as much as possible to using secure frequencies that are specifically dedicated to transportation;
  - setting up an alarm system in case of attack on the vehicle’s systems, with the possibility of operating in downgraded mode;
  - storing a log history of any access to the vehicle’s information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies.
92. These general recommendations shall be completed by specific requirements taking into account the characteristics and purpose of each data processing.

## 2.8 Transmitting personal data to third parties

93. In principle, only the data controller and the data subject have access to the data generated by a connected vehicle. However, the data controller may transmit personal data to a commercial partner (recipient), to the extent that such transmission is based on one of the legal basis stated in Art. 6 GDPR.
94. The vehicle manufacturer, service provider or other data controller can transmit personal data to a data processor selected to play a part in providing the service to the data subject, provided the data processor shall not use those data for its own purpose. Data controllers and data processors shall draw up a contract or other legal document specifying the obligations of each party and setting out the provisions of Art. 28 GDPR.
95. In view of the possible sensitivity of the vehicle-usage data (e.g., journeys made, driving style), the EDPB recommends that the data subject’s consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller (e.g., by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle). The commercial partner in turn becomes responsible for the data that it receives, and is subject to all the provisions of the GDPR.

## 2.9 Transfer of personal data outside the EU/EEA

96. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.
97. As a consequence, the data controller may transfer personal data to a recipient only to the extent that such transfer is in accordance with the requirements laid down in Chapter V GDPR.

## 2.10 Use of in-vehicle Wi-Fi technologies

98. Advances in cellular technology have made it possible to easily use the Internet on the road. While it is possible to get Wi-Fi connectivity in a vehicle through a smartphone hotspot or a dedicated device (OBD-II dongle, wireless modem or router, etc.), most manufacturers offer nowadays models that include a built-in cellular data connection and are also capable of creating Wi-Fi networks. Depending on the case, various aspects must be considered:
- The Wi-Fi connectivity is offered as a service by a road professional, such as a taxi driver for its customers. In this case, the professional or his/her company might be considered as an internet service provider (ISP), hence be subject to specific obligations and restrictions regarding the processing of his / her clients' personal data.
  - The Wi-Fi connectivity is put in place for the sole use of the driver (at the exclusion of and its passengers. In this case, the processing of personal data is considered to be purely personal or household activity.
99. In general, the proliferation of Internet connection interfaces via Wi-Fi poses greater risks to the privacy of individuals. Indeed, through their vehicles, users become continuous broadcasters, and can therefore be identified and tracked. In order to prevent tracking, easy to operate opt-out options ensuring the service set identifier (SSID) of the on-board Wi-Fi network is not collected must therefore be put in place by the vehicle and equipment manufacturers.

## 3 CASE STUDIES

100. This section addresses five specific examples of processing in the context of connected vehicles, which correspond to scenarios likely to be encountered by stakeholders in the sector. The examples cover data processing that requires calculating power which cannot be mobilised locally in the vehicle, and/or the sending of personal data to a third party to carry out further analysis or to provide further functionality remotely. For each type of processing, this document specifies the intended purposes, the categories of data collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information. In the case some of these fields are not described in the following, the general recommendations described in the previous part apply.
101. The examples chosen are non-exhaustive and are meant to be indicative of the variety of types of processing, legal bases, actors, etc. that might be engaged in the context of connected vehicles.

### 3.1 Provision of a service by a third party

102. Data subjects may contract with a service provider in order to obtain added-value services relating to their vehicle. For example, a data subject may enter into a *"Pay As You Drive"* insurance contract that offers reduced insurance premiums for good driving behaviour and which necessitates monitoring of driving habits by the insurance company. A data subject could also contract with a company that offers roadside assistance in the event of a breakdown and which entails the transmission of the vehicle's location to the company or with a service provider in order to receive messages or alerts relating to the vehicle's functioning (e.g., an alert on the state of brake wear, or a reminder of the technical-inspection date).

#### 3.1.1 Pay as you drive (PAYD) insurance

103. Pay as you drive is a type of usage-based insurance that tracks the driver's mileage and/or driving habits to differentiate and reward "safe" drivers by giving them lower premiums. The insurer will

require the driver to install a built-in telematics service that tracks the miles covered and the driving behaviour (braking pattern, rapid acceleration, etc.) of the policy holder. The information gathered by the telematic device will be used to assign the driver scores in order to analyse what risks he/she may pose to the insurance company.

104. The EDPB outlines that pay as you drive type of insurance should always be optional ; the policy holder must have the choice to subscribe to a non-usage-based insurance policy.

#### *3.1.1.1 Legal basis*

105. When the data is collected through a publicly available electronic communication service (for example *via* the SIM card contained in the telematics device), consent will be needed in order to gain access to information that is already stored in the vehicle as provided by art. 5(3) “ePrivacy” directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user. Consent could be collected at the time of the conclusion of the contract.

106. As regards the processing of personal data following the storage or access to the end-user’s terminal equipment, the insurance company can rely on art. 6(1)(b) GDPR in this specific context provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Insofar as the processing is objectively necessary for the performance of the contract with the data subject, the EDPB considers that reliance upon art. 6(1)(b) GDPR would not have the effect of lowering the additional protection provided by art. 5(3) of the “ePrivacy” Directive in this specific instance. That legal basis is materialised by the data subject signing a contract with the insurance company.

#### *3.1.1.2 Data collected*

107. There is two types of personal data to be considered:
- **commercial and transactional data:** data subject’s identifying information, transaction-related data, data relating to means of payment, etc. ;
  - **usage data:** personal data generated by the vehicle, driving habits, location, etc.
108. The EDPB recommends that, as far as possible, and given that there is a risk that the data collected via the telematics-box could be misused to create a precise profile of the driver’s movements, raw data regarding driving behaviour must be either processed:
- inside the vehicle in telematics boxes or in the user’s smartphone so that the insurer only accesses the results data (e.g., a score relating to driving habits), not detailed raw data (see section 2.1) ;
  - or by the telematics service provider on behalf of the controller (the insurance company) to generate numerical scores that are transferred to the insurance company on a defined basis. In this case, raw data and data directly relating to the identity of the driver must be separated. This means that the telematics service provider receives the real-time data, but does not know the names, licence plates, etc. of the policy holders. On the other hand, the insurer knows the names of policyholders, but only receives the scores and the total kilometres and not the raw data used to produce such scores.

109. Moreover, it has to be noted that if only the mileage is necessary for the performance of the contract, location data shall not be collected.

#### 3.1.1.3 Retention period

110. In the context of data processing taking place for the performance of a contract (i.e. provision of a service), it is important to distinguish between two types of data before defining their respective retention periods:

- **commercial and transactional data:** those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate medium: CD-ROM, etc.) or logically (by authorisation management) in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised ;
- **usage data:** usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw data. If it is necessary, raw data should be kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data should be kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member state law.

#### 3.1.1.4 Information and rights of data subjects

111. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, he or she must be informed of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. In this last case, the EDPB recommends to adopt a pedagogic approach to emphasize the difference between raw data and the score produced on this basis, stressing that the insurer will only collect the result of the score where appropriate.

112. Where data are not processed inside the vehicle but by a telematics provider on behalf of the controller (the insurance company), the information could usefully mention that, in this case, the provider will not have access to data directly relating to the identity of the driver (such as names, licence plates, etc.). Also, considering the importance of informing data subjects as to the consequences of processing of their personal data and the fact that data subjects should not be taken by surprise by the processing of their personal data, the EDPB recommends that data subject should be informed of the existence of profiling and the consequences of such profiling even if it does not involve any automated decision-making as referred to in art. 22 GDPR.

113. Regarding the right of data subjects, they shall be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since, raw data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends, *“that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”*.

114. The information can be provided when the contract is signed.

#### 3.1.1.5 Recipient:

115. The EDPB recommends that, as far as possible, the vehicle's usage data should be processed directly in telematics boxes, so that the insurer only accesses the results data (e.g. a score), not detailed raw data.
116. If a telematics service provider collects the data on behalf of the controller (the insurance company) to generate numerical scores, it does not need to know the identity of the driver (such as names, licence plates, etc.) of the policy holders.

#### 3.1.1.6 Security:

117. General recommendations apply. See section 2.7.

### 3.1.2 Renting and booking a parking space

118. The owner of a parking place may want to rent it. For this, he/she lists a spot and sets a price for it on a web application. Then, once the parking spot is listed, the application notifies the owner when a driver wants to book it. The driver can select a destination and check for available parking spots based on multiple criteria. After the approval of the owner, the transaction is confirmed and the service provider handles the payment transaction then uses navigation to drive to the location.

#### 3.1.2.1 Legal basis

119. When the data is collected through a publicly available electronic communication, art. 5(3) of the "ePrivacy" directive applies.
120. Because this is an information society service, art. 5(3) of the "ePrivacy" directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
121. For the processing of personal data and only for data necessary for the performance of the contract to which the data subject is party, art. 6(1)(b) GDPR will be the legal basis.

#### 3.1.2.2 Data collected

122. Data processed includes the driver contact details (name, email, telephone number, vehicle type (e.g. car, truck, motorcycle), license plate number, parking period, payment details (e.g. credit card info) as well as navigation data.

#### 3.1.2.3 Retention period

123. Data must be retained as long as it is necessary to fulfil the parking contract or otherwise as provided by Union or Member State law. After that data is either anonymized or deleted.

#### 3.1.2.4 Information and rights of data subjects

124. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way.
125. The data subject must be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since, the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends *"that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability"*.

#### 3.1.2.5 Recipient:

126. In principle, only the data controller and the data processor have access to the data.



### 3.1.2.6 Security:

127. General recommendations apply. See section 2.7

## 3.2 eCall

128. In the event of a serious accident in the European Union, the vehicle automatically triggers an eCall to 112, the EU-wide emergency number (see section 1.3 for further details) which allows an ambulance to be sent the place of the accident promptly according to regulation EU 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, and amending Directive 2007/46/EC.

129. Indeed, the eCall generator installed inside the vehicle, which enables transmission *via* a public mobile wireless communications network initiates an emergency call, which is either triggered automatically by vehicle sensors or manually by the vehicle occupants only in the event of an accident. In addition to activation of the audio channel, the second event triggered automatically as a result of an accident consists in generating the Minimum Set of Data (MSD) and sending it to the public safety answering point (PSAP).

### 3.2.1 Legal basis

130. Regarding the application of the “ePrivacy” directive, two provisions have to be considered:

- art. 9 regarding location data other than traffic data which only applies to electronic communication services. ;
- art. 5(3) for the gaining access to information stored in the generator installed inside the vehicle.

131. Despite the fact that, in principle, those provisions require the consent of the data subject, regulation EU 2015/758 of 29 April 2015 constitutes a legal obligation to which the data controller is subject (the data subject has no genuine or free choice and will be unable to refuse the processing of his/her data). Hence, regulation EU 2015/758 overrides the need of the driver’s consent for the processing of location data and the MSD.<sup>29</sup>

132. The legal basis of the processing of those data will be compliance with a legal obligation as provided for in art. 6(1)(c) GDPR (i.e., regulation EU 2015/758).

### 3.2.2 Data collected

133. Regulation EU 2015/578 provides that data sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2015 ‘Intelligent transport systems — eSafety — eCall minimum set of data (MSD)’ including:

- the indication if eCall has been manually or automatically triggered ;
- the vehicle type ;
- the vehicle identification number (VIN) ;
- the propulsion type of the vehicle ;

---

<sup>29</sup> It has to be noted that Article 8-1-f of the last version of the working document of the proposal for an “ePrivacy” regulation does provide a specific exemption for eCall as consent is not needed when “*it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number ‘112’ or a national emergency number, in accordance with Article 13(3).*”

- the timestamp of the initial data message generation within the current eCall incident event ;
- the last known vehicle latitude and longitude position determined at the latest moment possible before message generation ;
- the vehicle’s last known real direction of travel determined at the latest moment possible before message generation (only the last three locations of the vehicle).

### 3.2.3 Retention period

134. EU regulation 2015/758 of 29 April 2015 stipulates that data shall not be retained for longer than is needed for processing emergency situations. Those data shall be completely deleted when they are no longer needed for that purpose. Furthermore, in the internal memory of the eCall system, data shall be automatically and constantly deleted. Only the vehicle’s last three positions can be stored, insofar as it is strictly necessary to specify the current position of the vehicle and the direction of travel at the time of the event.

### 3.2.4 Information and rights of data subjects

135. Art. 6 of the EU regulation 2015/758 of 29 April 2015 stipulates that manufacturers shall provide clear and complete information on data processing done using the eCall system. This information shall be provided in the owner's manual separately for the 112-based eCall in-vehicle system and any third party service supported eCall systems prior to the use of the system. It includes:

- the reference to the legal basis for the processing;
- the fact that the 112-based eCall in-vehicle system is activated by default;
- the arrangements for data processing that the 112-based eCall in-vehicle system performs;
- the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Art. 5(2);
- the types of data collected and processed and the recipients of that data;
- the time limit for the retention of data in the 112-based eCall in-vehicle system;
- the fact that there is no constant tracking of the vehicle;
- the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests;
- any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a TPS eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with the GDPR. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.

136. Furthermore, the service provider shall also provide the data subjects with information in accordance with art. 13 GDPR in a transparent and understandable way. In particular, he or she must be informed of the purposes of the processing for which the personal data are intended as well as the fact that the processing of personal data is based on a legal obligation to which the controller is subject.

137. In addition, taking into account the nature of the processing, the information about the recipients or categories of recipients of the personal data must be clear and the data subjects should be informed

that the data are not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.

138. Regarding rights of data subjects, it has to be noted that since the processing is based on a legal obligation, the right to object and the right to portability will not apply.

#### 3.2.5 Recipient:

139. The data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
140. When it is triggered (either manually by vehicle occupants or automatically as soon as an in-vehicle sensor detects a serious collision), the eCall system establishes a voice connection with the relevant PSAP and the MSD is sent to the PSAP operator.
141. Furthermore, data transmitted via the 112-based eCall in-vehicle system and processed by the PSAPs can be transferred to the emergency service and service partners referred to in Decision No 585/2014/EU only in the event of incidents related to eCalls and under the conditions set out in that Decision and are used exclusively for the attainment of the objectives of that Decision. Data processed by the PSAPs through the 112-based eCall in-vehicle system are not transferred to any other third parties without the explicit prior consent of the data subject.

#### 3.2.6 Security

142. EU regulation 2015/758 stipulates the requirements to incorporate into the eCall system technologies that strengthen the protection of privacy, in order to offer users the appropriate level of protection of privacy, as well as the guarantees needed to prevent surveillance and abusive uses. In addition, manufacturers shall ensure that the eCall system based on the number 112, as well as any other system providing an eCall that is handled by third-party services or an added-value service, are so designed that it is impossible for personal data to be exchanged between those systems.
143. Regarding PSAPs, Member States shall ensure that personal data are protected against misuse, including unlawful access, alteration or loss, and that protocols concerning personal data storage, retention duration, processing and protection are established at the appropriate level and properly observed.

### 3.3 Accidentology studies

144. Data subjects may voluntarily agree to take part in accidentology studies aimed at better understanding the causes of road accidents and more generally scientific purposes.

#### 3.3.1 Legal basis

145. When the data are collected through a public electronic communication service, the data controller will have to collect the consent of the data subject **for the gaining of access to information that is already stored in the vehicle as provided by art. 5(3) of the “ePrivacy” directive**. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user.
146. Regarding the processing of personal data and taking into account the variety and amount of personal data needed for accidentology studies, prior consent of the data subject should be collected according to art. 6 GDPR. Such prior consent must be provided on a specific form, through which the data subject volunteers to take part to the study and have his or her personal data processed for that purpose.

Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g., ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to the processing being stopped. The data shall then be deleted from the active database, or anonymised.

147. Consent required by art. 5(3) of the “ePrivacy” directive and consent needed as a legal basis for the processing of data can be collected at the same time (for example by checking a box clearly indicating what the data subject is consenting to).

### 3.3.2 Data collected

148. The data controller shall only collect personal data that are strictly necessary for the processing.
149. There is two types of data to be considered:
- **data relating to participants and vehicles ;**
  - **technical data from vehicles** (instantaneous speed, etc.).
150. Scientific research linked to accidentology justifies the collection of the instantaneous speed, including by legal persons who do not administer a public service in the strict sense.
151. Indeed, as noted above, the EDPB considers that instantaneous speed collected in the context of an accidentology study is not offence-related data by destination (i.e., it is not being collected for the purpose of investigating or prosecuting an offence), which justifies its collection by legal persons who do not administer a public service in the strict sense.

### 3.3.3 Retention period

152. It is important to distinguish between two types of data. First, the data relating to participants and vehicles can be retained for the duration of the study. Second, the technical data from vehicles may not be retained for more than five years from the end date of the study. At the end of that period, the data shall be deleted or anonymised.

### 3.3.4 Information and rights of data subjects

153. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, in the case of collecting instantaneous speed, the data subjects shall be specifically informed of the data collection. Since the data processing is based on consent, the data subject must be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Moreover, because the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) GDPR (consent), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends, “*that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability*”. Consequently, the data controller must provide an easy way to withdraw his consent, freely and at any time, as well as develop tools to be able to answer data portability requests.
154. That information can be given on signing the form to agree to take part in the accidentology study.

### 3.3.5 Recipient

155. In principle, only the data controller and the data processor have access to the data.

### 3.3.6 Security

156. As noted above, the security measures put in place shall be adapted to the level of data sensitivity. For instance, if instantaneous speed (or any other data related to criminal convictions and offences) is collected as part of the accidentology study, the EDPB strongly recommends putting in place strong security measures, such as:

- implementing pseudonymisation measures (e.g., secret-key hashing of data like the surname/first name of the data subject and the serial number);
- storing data relating to instantaneous speed and to geolocation in separate databases (e.g., using a state-of-the-art encryption mechanism with distinct keys and approval mechanisms);
- and/or deleting geolocation data as soon as the reference event or sequence is qualified (e.g., the type of road, day/night), and the storage of directly-identifying data in a separate database that can only be accessed by a small number of people.

## 3.4 Tackle auto theft

157. Data subjects may wish, in the case of theft, to attempt to find their vehicle using geolocation. Using location data is limited to the strict needs of the investigation and to the case assessment by the competent legal authorities.

### 3.4.1 Legal basis

158. When the data is collected through a publicly available electronic communication service, art. 5(3) of the “ePrivacy” directive applies.

159. Because this is an information society service, art. 5(3) of the “ePrivacy” directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.

160. Regarding the processing of personal data the legal basis is the consent of the vehicle’s owner, or, if applicable, the performance of a contract (only for data necessary for the performance of the contract to which the vehicle’s owner is party).

161. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g., ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Freedom to give consent involves the option of withdrawing consent at any time, of which the data subject shall be expressly informed. Withdrawal of consent shall lead to the processing being stopped. The data shall then be deleted from the active database, anonymised, or archived.

### 3.4.2 Data collected

162. Location data can only be transmitted as of the declaration of theft, and cannot be collected continuously the rest of the time.

### 3.4.3 Retention period

163. Location data can only be retained for the period during which the case is assessed by the competent legal authorities, or until the end of a procedure to dispel doubt that does not end with confirmation of the theft of the vehicle.

#### 3.4.4 Information of the data subjects

164. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. More specifically, the EDPB recommends that the data controller emphasizes that there is no constant tracking of the vehicle and that location data can only be collected and transmitted as of the declaration of theft. Moreover, the controller must provide the data subject with information relating to the fact that only approved officers of the remote-surveillance platform and legally approved authorities have access to the data.
165. Regarding the rights of the data subjects, when the data processing is based on consent, the data subject must be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Besides, when the data collected in this context are provided by them (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) (consent) or art. 6.1.(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends, *“that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”*.
166. Consequently, the data controller must provide an easy way to withdraw his consent (only when consent is the legal basis), freely and at any time, as well as develop tools to be able to answer data portability requests.
167. The information can be provided when the contract is signed.

#### 3.4.5 Recipients

168. In the event of a theft declaration, location data can be passed on the (i) approved officers of the remote-surveillance platform, and (ii) to the legally approved authorities.

#### 3.4.6 Security

169. General recommendations apply. See section 2.7

### 3.5 Personal information stored on rental cars’ dashboard

170. When renting a vehicle, data subjects may want to use its in-car entertainment capacities, for instance to navigate to a given destination, to give a phone call or to play some music. A variety of technical means can be relied upon to do so and there is a risk that data relating to previous occupants of the vehicle are visible to subsequent users.

#### 3.5.1 Data collected

171. A variety of data can be processed in rental cars’ dashboard. Those data could be processed:
- when a data subject’s smartphone is paired with the rental car’s dashboard, for instance using Bluetooth or USB connections (phone identifiers, voice and data communications, etc.) ;
  - when the driver or the passenger use the rental cars’ dashboard (GPS navigation history, web browsing, and a growing range of applications).
172. Hence, the data generated can reveal personal information (web browsing data, personal contacts and schedules, choice of music, radio and other streamed audio or video content, etc.) and help to draw a precise profile of the data subject.<sup>30</sup>

---

<sup>30</sup> Privacy international, Connected Cars: What Happens To Our Data On Rental Cars?; [https://privacyinternational.org/sites/default/files/2017-12/cars\\_briefing.pdf](https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf)

173. Since rental companies have effective control over the processing, they should be regarded as the data controller of the information, which resides on the car's dashboard they rent. As such, they have the responsibility to ensure the confidentiality of the data and compliance with data protection requirements.

#### 3.5.2 Information of data subjects

174. To allow users to exercise effective control over their data, rental companies must provide clear and explicit information to customers in relation to what data that is likely to be processed locally, the purpose of the processing, and the option to, at all times, deactivate data collection and delete the data concerned. For example, if the car's dashboard is equipped with a "delete button", the rental companies must draw the attention of the customer on this functionality.

#### 3.5.3 Retention period

175. The EDPB recommends that manufacturers provide a simple functionality (such as a delete button) enabling data subjects to quickly and easily remove their personal data from the car's dashboard.
176. Rental companies shall define clear internal procedures to erase personal data stored on the car's dashboard before the vehicle can be rented again.

#### 3.5.4 Security

177. Rental companies shall ensure that the permissions setting on the rental car's dashboard is compliant with the principle of privacy by design and by default (having settings that prevents third parties from processing data generated by the car's dashboard unless they have the user's consent to enable third party access to that data for a specified purpose).